D3.1. State of the Art

FUSE-IT

Editors: Son Han, Shohreh Ahvar, Noël Crespi, Reza Farahbakhsh, Bahram Alinia (IMT-TSP)

Contributors: CCS, CEA-LIST, Evoleo, ICAM, iMINDS, IMT-TSP, ISEP/GCAD, SOGETI, Thales Services, ULR

Reviewer: Hélia POUYLLAU (Thales RT)

Draft history		
V.0.1.0	15 Dec 2014	Initial Version (Reviewed by Thales RT)
V.1.0.0	30 Jan 2015	Release 1 - Revisions needed: - 3.1.4. Physical Detection and Anti-intrusion Sensors [Thales Services - Introduction] - 3.3.3. Network Operation Centers (NOC) [CCS - Solutions & Products] - 3.4.3. Security Operation Centers (SOC) [CCS – Figure 3.4.4, Situation awareness, limitation of SIEM and/or ad-hoc orchestrator] - 4.1.3. Internet of Things Alliances [SOGETI, technical details]
V.1.0.1	30 May 2015	- Revisions needed as in V.1.0.0 - Added Smart Grid and Smart Grid Standards (ISEP/GECAD) - Updated 4.1.3 Internet of Things Alliances (SOGETI)
V. Final	22 June 2015	- Updated 3.1.1 Smart Energy sensors, 3.2.2 Building Automation & SCADA (ICAM) - Updated 4.1.3 Internet of Things Alliances (SOGETI)
V.Update	8 August 2015	- Added 4.4 Security Standards (IMT) - Updated 4.2.1 Building Automation Standards (IMT) - Added 3.4.1 Smart meters and cyber security (Thales Services) - Added 3.1.3 Heterogeneous traffic data , 3.1.4 Opportunistic spectrum access sensors and 3.4.3 Attacks and threats in IoT (ULR)

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Overview

Fuse-IT will address the need of a sustainable, reliable, user-friendly, efficient, safe and secure Building Management System (BMS) in the context of Smart Critical Sites. It is the sole initiative addressing Sustainability and Security & Safety challenges from a site management perspective. It will benefit to both challenges by solving the dilemma between efficiency and security in intelligent buildings. A BMS is defined here as a computer based system that controls and monitors the building facilities such as ventilation, lighting, power systems, fire detection and security. A Smart Site is a facility or infrastructure implementing intelligent building and energy control & monitoring technologies such as micro-grids, smart sensors or communicating devices. A micro-grid is intended here as a local electrical system that includes multiple loads and distributed energy resources that can be operated in parallel with the broader utility grid or as an electrical island. A Critical Site is a facility or infrastructure which has to meet higher grade safety and security requirements, whether this is for national/business-strategic or public health and safety reasons.

The trend towards global competition and supranational regulation forces nations to flow down more and more environmental, economical, national-critical and safety-critical requirements on key public and private actors. These actors need to upgrade their facilities and assets accordingly. In the context of a Smart Critical site, a Site Manager and a Security Manager may face incompatible objectives and constraints. A Site Manager would likely focus on manageability, automation, energy efficiency, sustainability and global cost of building operation. A Security Manager would more likely focus on anti-intrusion at physical and logical level, relying on dedicated equipments and segregated networks, whatever the infrastructure, staff & power required.

From a technological point of view, however, with ICT enhancing all legacy building equipment and automation, a number of synergies emerge which may help solving this dilemma. Through connection to enterprise network and the internet, building energy and automation systems become more flexible, powerful and upgradable. They also get exposed to new threats, a reason why, from its original focus on information networks, cyber-security has moved towards a more comprehensive scope involving security of cyber-physical systems. A striking rationale for that is that attacks on cyber-physical systems do not only harm national / business strategic information security. They can ramp up into industrial, environmental or public health and safety catastrophe.

A way to success is to stimulate cross-domain innovation between activities which are traditionally very segmented. Advanced data processing and analysis is the key capability required to meet all challenges above. Therefore, the main achievement of Fuse-IT shall be the development of a Core Building Data Processing & Analysis module. It will process data reported by Secured share Sensors, Effectors and Devices strongly interconnected through Trusted federated Energy & Information Networks. It will display the building & security status based on common Key Performance Indicators (KPIs). At user-level, a Smart unified Building Management Interface will enable daily monitoring and controlling with a “view of god” on buildings, while a Full Security Management Interface will enable supervision of both physical and logical security throughout the premises and the enterprise network.

The result of Fuse-IT will be a Smart Secured Building System, incorporating the above described modules. They will be marketable as standalone components or fully integrated system in order to address either existing or new Smart Critical Sites. A service offering will also be set up to enable trusted building management and/or security management operation under rental price. Besides lower investment cost, this enables expertise federation and full benefit from big data analytics advantage.

1.2 FUSE-IT Components

From a technical point of view, some key technology bricks involved in Smart Critical Building management are to be considered (see Figure 3.1.1-1): Building Management System (BMS), Network Operation Center (NOC), Security Operation Center (CCTV), Closed-Circuit Television (EMS), Energy Monitoring System (HAVC), Heating, Ventilation, and Air Conditioning (HVAC), and Facility Management System (FMS). They are classified into two categories including Building management system and network management center.

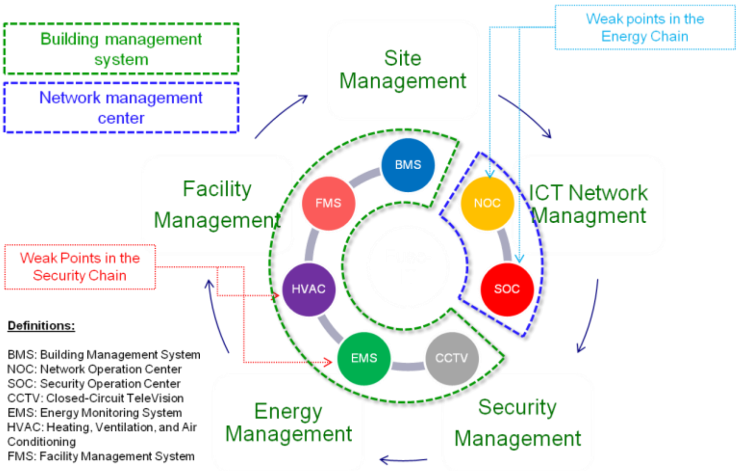

Building management system
Network management center
Weak points in the Energy Chain
Site Management
Facility Management
ICT Network Managment
Weak Points in the Security Chain
BMS
FMS
NOC
HVAC
SOC
EMS
CCTV
Energy Management
Security Management
Definitions:
BMS: Building Management System
NOC: Network Operation Center
SOC: Security Operation Center
CCTV: Closed-Circuit TeleVision
EMS: Energy Monitoring System
HVAC: Heating, Ventilation, and Air Conditioning
FMS: Facility Management System

Figure 3.1.1-1 Technology bricks – legacy systems

Based on the legacy technology bricks, FUSE-IT Smart Building System will include five module as shown in Figure 3.1.1-2 to exhibit its value chain. On sensors and networks layers (M1+M2), Fuse-IT will mainly look for synergies among emerging technologies in contactless sensing, low energy actuation, device geolocation, wireless communication, network virtualization and light cryptography. On the core data processing & analysis layer (M3), Fuse-IT will focus on developing advanced data processing, fusion, correlation and analysis capabilities based on a common information model and a set of Key Performance Indicators (KPIs). On management interface layer (M4+M5), two modules will be developed in order to fit ergonomic expectations and be easily marketable by BMS and Security integrators. A panel of tailored businessviews will be accessible within each module. In addition to this, a full view merging M4 & M5 will also be enabled for authorized users.

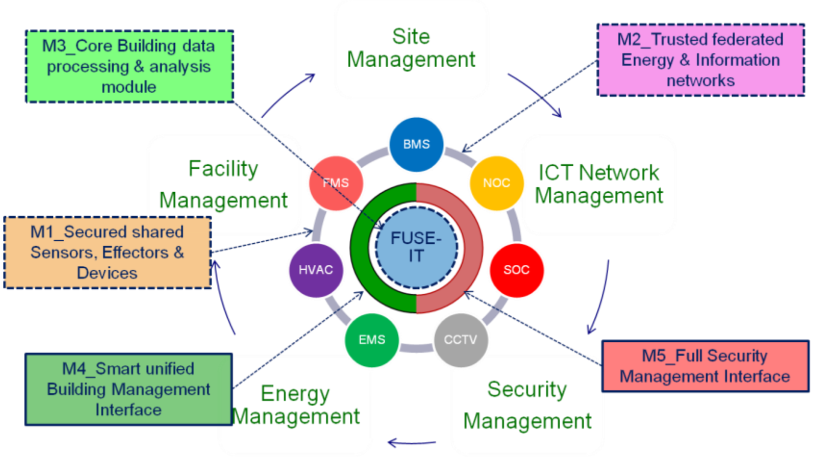

M3_Core Building data processing & analysis module
Site Management
M2_Trusted federated Energy & Information networks
BMS
Facility Management
FMS
NOC
ICT Network Management
M1_Secured shared Sensors, Effectors & Devices
FUSE-IT
HVAC
SOC
EMS
CCTV
M4_Smart unified Building Management Interface
Energy Management
Security Management
M5_Full Security Management Interface

Figure 3.1.1-2 Overview on Fuse-IT Building System

2 Related Projects

2.1 ITEA2 – ViCoMo

The ITEA 2 project ViCoMo (Visual Context Modeling) conducted from 2009 to 2012 is the successor of CANTANTA, which focused on behavior and interaction analysis, and its predecessor CANDELA (single event detection). The general goal of ViCoMo project is to find the context of events captured by cameras or image sensors, and model the context such that reliable reasoning about an event can be established. The technology that has been developed contributes to improving healthcare, security and safety, and the public infrastructure in society in general.

Three main innovations were demonstrated in this project: multi-camera and dynamic analysis, 3D environment modeling and the successful integration of new marketing concepts and emerging technologies. Two scenarios demonstrated this context: a port terminal and a shopping mall. In the port scenario, the context modeling techniques improved the monitoring and tracking of cargo throughout the harbor while visualization of the 3D modeling improved the logistic operations and control.

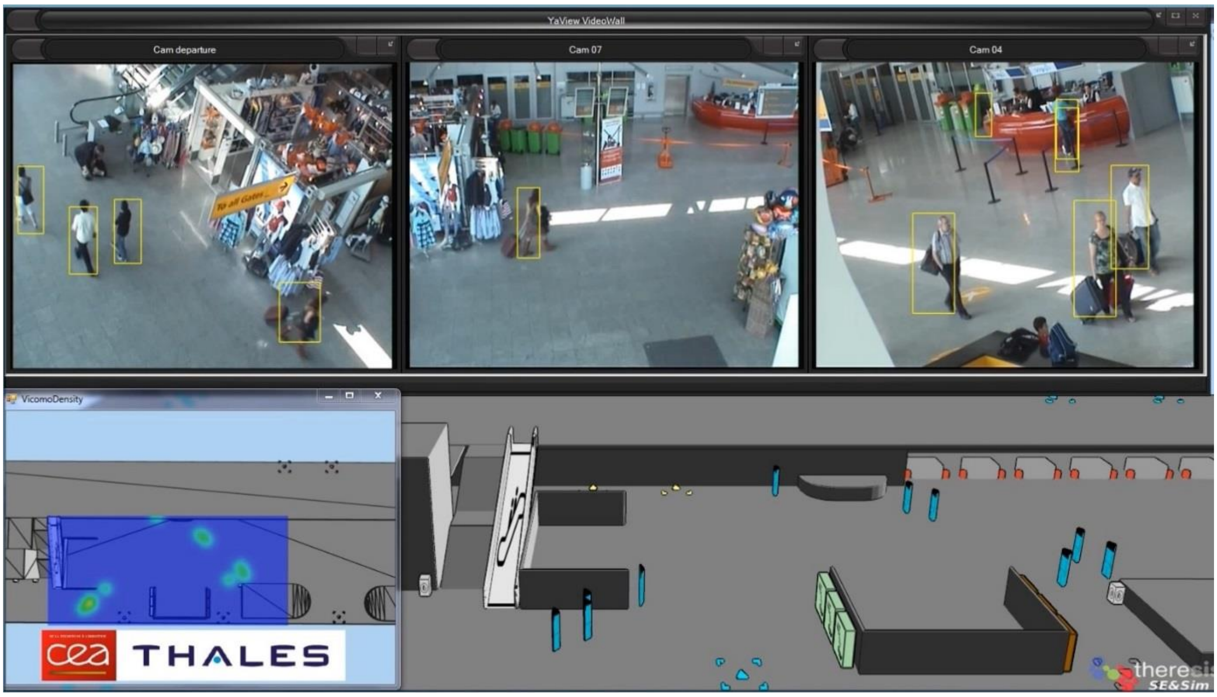


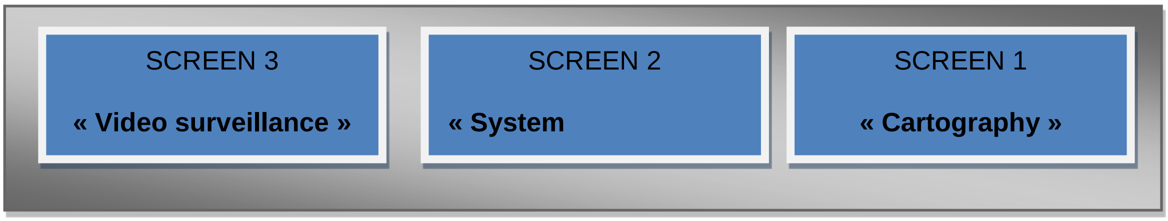
Figure 3.1.1-1 ViCoMo site security supervision system

The technology used for multi-camera analysis, the similarity of the concepts for modeling the context and the surveillance applications were used to build a site security supervision system. In terms of observation for surveillance, 3D information and context enabled more faithful reasoning to be achieved for a high-level of semantics while situational awareness was enhanced by combining all camera views into a single visual presentation. In respect of 3D modeling of the real-world environment, full automatic infrastructure recognition in geo-referenced images along with autonomous simulation from video inputs enabled to deduce the person density in the scene. As for observation of human behavior for system control, this was given a boost through the use of 3D modeling of context.

2.2 FUI3 – MOBISIC

The MOBISIC (Mobile Security System of Critical Infrasctrucures) project aims to define and develop temporary security capacity for occasional needs for critical infrastructures security. A temporary increase of security needs can result from the increase of the risk which is itself the consequence of the activation of an important level of vigilance of local or national security plan. Occasional security needs can result from protection of sites that became sensitive or vulnerable due to temporary events such as sporting or political event. It can also result from the support for the intervention for emergency on a site or an infrastructure that underwent an accidental sinister or an attack. The system capabilities enable operational gains for site security or rescue operations.

The aim of MOBISIC supervision control station is to display the situation in a synthetic, quickly understandable form. The control station ergonomics was developed in collaboration with end users. Moreover, the control station must enable to manage various sensors for each intervention or for the same intervention. Indeed, for each alarm raised, a frame is displayed. This frame displays precise data linked to this alarm and its metadata. The supervision control station enables also to monitor the mapping of the situation.



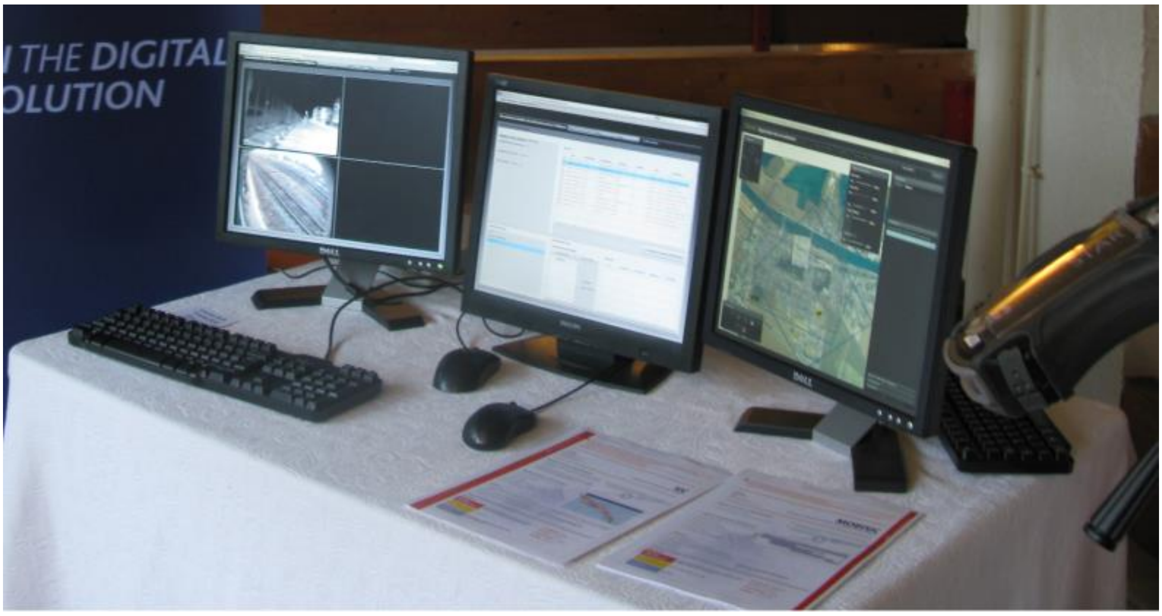


Figure 3.1.1-1 MOBISIC supervision control station

2.3 EU FP7 - SECUR-ED

The SECUR-ED (SECured URban transportation – European Demonstration) project is a demonstration project with an objective to provide a set of tools to improve urban transport security. SECUR-ED based its vision of a future-proof interoperability framework on design patterns which are successfully used in other industries. These include the following elements:

- A reusable Service-Oriented Architecture (SOA);
- An Event-Based Architecture for data exchange between various security components and decoupling the components from each other;
- Reuse of well-established and proven standards which reduce the non-recurring cost of software integration;
- Building modular components with web services;
- Supporting discoverable components to reduce the configuration effort and improve the reusability;
- Building on an IP network (cabled or wireless) which is dimensioned to support consistently the video surveillance systems necessary to assess, confirm and investigate security incidents.

To support the general requirement for future-proof interoperability and modularity of the public transport systems, SECUR-ED demonstrations confirmed that the sole implementation of the video-surveillance (also called CCTV) industry standards is not enough. Implementation of such generic standards is further complicated by the regulatory need for stability and trustworthiness as well as privacy protection imposed on security video systems.

Several video analytics solutions have reached intrinsically a reasonable level of maturity, such as intrusion detection, video tracking, crowd assessment and face recognition. Implementing such analytics in a real public transport environment proves to be more complex than in controlled environments. The main difficulty is to define precisely for each camera what to detect and what not to detect; to be very concrete, a system supposed to detect suspicious left objects will be quickly rejected by the operators if there is an alarm each time an empty paper bag is left in on the floor.

The public transport security concept comprises three interrelated elements: security organization which includes interfaces with internal and external bodies, security risk management plan which is the assimilation of a structured, comprehensive security risk management process, and security risk mitigation safeguards which include operational arrangements, procedures, technological communication and information management systems, physical protection means, incident response and business continuity planning. As a result, PTOs need to adopt a comprehensive and holistic approach to security as an integral part of the service they provide to their passengers.

2.4 Other Projects

Another valuable background for the project State of the Art is the outcome from previous research projects, which may be in a process of integration into new standards and solutions. The following table Table 2-1 presents a (non-exhaustive) list of projects of interest to FUSE-IT.

Table 2-1 Project Legacy

Project Name	Technical Focus	Relation to FUSE-IT/Limitations
BEAMS FP7 2011-14 (Buildings Energy Advanced Management System)	Development of an advanced, integrated management system which enables energy efficiency in buildings and special infrastructures from a holistic perspective (i.e. considering the indoors areas, the public spaces around the facility and the interaction of the overall compound with the grid and	The domain of BACS is not addressed, nor the possibility of M2M exchange, as in the case of DLC (Direct Load Control) or EV monitoring for large building and complex industrial facilities. The data model does not cover the main components in a facility management vision such as with Load, Meter, Generator and Storage in a formally approach nor the relationship within the

Project Name	Technical Focus	Relation to FUSE-IT/Limitations
	urban network outside it).	different actors within the value chain. The communication interface is limited.
HESMOS FP7 2010-13 (Holistic Energy Efficiency Simulation and Lifecycle Management Of Public Use Facilities.)	Provide advanced simulation capabilities. Integrate a Virtual Laboratory. Close the gap between Building Information Modelling (BIM) and Building Automation Systems (BAS).	The project addresses topics that can be of interest for the approach of modeling and simulation of BIM and BAS. The domain of BACS is not addressed, nor the possibility of M2M exchange, as in the case of DLC (Direct Load Control) or EV monitoring.
CyMPERIA FP7 2013-16 (Enhancement of Cyber Security by Merging with Physical Security)	CyMPERIA is an innovative prescriptive, proactive risk based, and high-performance framework designed to serve the operational needs of organizations which must protect their critical assets from cyber threats and crimes which are increasingly correlated with physical threats.	The project shall stimulate cross domain synergies between physical security and cyber security. It does not address the other site management topics in focus of FUSE-IT (energy, facility…)
Smart Build FP7 2012-15	Implementing smart ICT concepts for energy efficiency in public buildings	The domain of public buildings may be of interest for Fuse-IT partners on different point of views, technical and regulatory framework. The domain of BACS is not addressed, nor the possibility of M2M exchange, as in the case of DLC (Direct Load Control) or EV monitoring.
IMPONET ITEA2 2010-13 (Intelligent Monitoring of Power Networks)	The project aims at ensuring reliable, consistent and efficient electrical power distribution for industry, services and consumers	The project addresses flexibility issues related to the implementation of smart grids, interoperability issues, remote management and dear real-time monitoring. It is focused on energy efficiency and does not address the other building management Activities (Security, Facility, …)
BaaS FP7 2012-05-01 to 2015-04-30 (Building as a service)	The BaaS system aims to optimize energy performance in the application domain of "nonresidential buildings, in operational stage.	The project approach thanks to its technology focus on wired and wireless communication is relevant for Fuse-IT. The domain of BACS is not addressed, nor the possibility of M2M exchange, as in the case of DLC (Direct Load Control) or EV monitoring. Security seems not be taken into account nor critical buildings.
SPORTE2 FP7 2010-14	SPORTE2 aims to manage and optimize the triple dimensions of energy flows (generation, grid exchange, and consumption) by	The use case may be of interest to Fuse-IT. It includes Energy and Facility activity domains as well as public safety & security issues. The domain of BACS

Project Name	Technical Focus	Relation to FUSE-IT/Limitations
(Intelligent Management System for European Sport and Recreation Buildings)	developing a new scalable and modular BMS based on smart metering, integrated control, optimal decision making, and multi-facility management.	is not addressed, nor the possibility of M2M exchange, as in the case of DLC (Direct Load Control) or EV monitoring.
ENERFICIENCY ITEA2 2012-2014 (User Led Energy Efficiency Management)	A whole new market in energy management Open software platform to underpin new energy-management services	It is focused on energy management and excludes all other Building Management topics. The domain of BACS is not addressed, nor the possibility of M2M exchange, as in the case of DLC (Direct Load Control) or EV monitoring.
NEMONEMO_CODED ITEA2 2009-13 (Networked Monitoring & Control, Diagnostic for Electrical Distribution)	Improving power distribution efficiency The first step towards a Smart Grid implementation	The specific focus on Smart Grid may be of interest to Fuse-IT. The domain of BACS is not addressed, nor the possibility of M2M exchange, as in the case of DLC (Direct Load Control) or EV monitoring.
TOISE ENIAC 2011-2013 (Trusted Computing for European Embedded Systems)	The objective of TOISE is to define, develop and validate trust hardware and firmware mechanisms applicable both to lightweight embedded devices and as security anchors within related embedded platforms.	TOISE is a technology oriented project in the field of semi-conductors which finds applications in Smart Grids, electricity network, home appliance, environmental or infrastructure sensor networks. It is not implementation driven like FUSE-IT and there is no particular focus on site management applications.
SEAS ITEA2 Feb 2014 - Dec 2016 (Smart Energy Aware Systems)	The objective of the SEAS project is to enable energy, ICT and automation systems to collaborate at consumption sites, and to introduce dynamic and refined ICT-based solutions to control, monitor and estimate energy consumption.	Main results of this project will be: - Knowledge Model - Information Exchange Platform FUSE - IT and SEAS are strengthening collaboration to share the knowledge model and ontologies. Although, SEAS is not concerned with the management of Critical Buildings according to the four layers established by FUSE-IT.

2.5 Conclusion

This section provides a review on projects related to FUSE-IT as well as their limitations which FUSE-IT shall address. These projects are relevant to FUSE-IT on different aspects of critical site management system by considering few of its aspects; CyMPERIA addresses the security, IMPONET deals with energy, while FUSE-IT covers different critical site management topics simultaneously includes energy, facility, security. Also, details of each aspect of critical site management system in projects should be considered. Although, projects like BEAMS and HESMOS, Smart Build provide higher efficiency in the use of energy , they still have a lack of BACS domain and the possibility of M2M exchange, as in the case of DLC (Direct Load Control) or EV monitoring for large building and complex industrial facilities. In this regard, FUSE-IT tries to centralize control of a building's heating, ventilation, air conditioning, lighting and other systems and enable real-time remote monitoring, commissioning and control of entire portfolios of buildings through M2M exchange and extend communication interfaces. The data model is the next issue which is considered by details in FUSE-IT covering also the main components in a facility management vision such as with Load, Meter, Generator and Storage in a formally approach.

3 Related Technological Development

3.1 Smart Sensors

3.1.1 Smart Energy Sensors

3.1.1.1 Introduction

The intelligent building is defined as an energy-efficient building, integrating the intelligent management (by data mining) of consumer equipment building, equipment producers and storage equipment, such as electric vehicles.

Energy efficiency also depends on building construction techniques, insulation for example. The concept of intelligent building is the integration of energy management solutions in homes and business buildings, especially to achieve positive energy buildings. Many solutions exist and are complementary:

- Improved insulation of buildings: it is the most effective method to avoid heat waste and eliminates the need for heating outside the cold periods (many materials : glass wool, hemp and straw) ;
- New energy generation techniques: the building allows easy integration of renewable energies. The roof can accommodate photovoltaic panels that offset or exceed energy expenditure of residents or solar thermal collectors that heat water for heating and sanitary;
- The development and strengthening of ventilation systems to avoid losing the benefit of the insulation by opening a window both in periods of extreme cold or high heat (dual flow ventilation or Canadian well) ;
- Heating and air conditioning systems more virtuous (wood stove, heat pump, geothermal) and other systems to better regulate the temperature (thermostat, efficient boilers, etc.);
- A more thoughtful choice on the building location in terms of location and orientation field to make the most of the insulation, openings and photovoltaic panels ;
- The development of home automation, energy consumption equipment sober and energy management.

This last point will be considered in this part, particularly the smart energy sensors.

3.1.1.2 How to make smarter a power grid?

In order to make smarter a power grid, it is necessary to deploy a technology of precise measure to analyze, treat, sort out and distribute the data, outside the electrical infrastructure. The sensors which allow to measure the electric parameters (current, tension, phase shift and frequency) are the link between the physical world and the intelligent systems.

What is therefore the ideal sensor? To ensure fine control of energy, it must also be intelligent, which means non-intrusive (no service interruption or jeopardizing the integrity of the installation), compact, requiring no maintenance or recalibration remotely programmable, and have low heat dissipation (no additional loss) and the ability to accurately measure small currents as well as strong, AC and DC. The ideal sensor is basically a versatile device that performs several functions at once (measurement and protection, and measurement and data storage, for example), which allows real-time monitoring and exchange of data and information.

Different types of Sensors will enable the optimization of consumption and buildings flows for Better energy efficiency. For this, It must integrate the sensors in places thoughtful and strategic order to get relevant information such as the actual use of the building, the occupation of the different parts, thermal flow exchanges but bright also between the different parts.

The technological evolution of sensors now allow all these strategic deployment. Indeed, the evolution of Microelectronics permits major enhancements such as the miniaturization of the different components, reducing costs and allowing integration functions always smarter.

All these progresses have helped conducting easily to deployable sensors, and especially without touching the building envelope. Indeed, information transmissions from the sensor measurements are wireless with telecommunications bricks very low consumption and which are easily integrable easily. All these improvements were able to afford to insert the power supply in the sensor. Thye also can recover energy with the light (photovoltaic panels) or mechanical (by recovering the intrinsic vibration of the building, for example, using accelerometers).

In general, smart sensors will be used to collect data that can be correlated to build its own energy optimization scenarios based on five components:

- Measurement: taking into account all the factors influencing energy consumption.
- Identification: a detection of behavioral dysfunction is performed, electrical malfunctions (reactive power current peaks, brownouts) or process dysfunction.
- Analysis: a study of the performance of an installation is performed with an identification of influencing factors;
- Evaluation: a performance analysis under a performance benchmark is conducted;
- Communication: configuration and automatic output reports are made to encourage the involvement of all in the energy saving strategy.

The following section will give a non-exhaustive list of smart sensors to achieve energy savings.

3.1.1.3 Smart energy sensors

The various smart sensors have different areas of applications such as storage, instrumentation and control, measurement, protection, lighting managements or temperature. We can notice:

The current sensors: Commonly based on Hall effect technology, these current sensors will allow to give a precise value of the current (ac or dc depending on the technology) consumed by the system. These measures will help to:

- Optimization of storage: for example, these sensors optimize the lifetime of batteries connected to solar panels. These batteries have a minimum state of charge to respect and current measurement will allow estimating the best charge rate and thus being able to use the battery with a longer lifetime. Similarly, the sensor will, if the charging rate becomes critical to help the network to recharge the battery (principle of microgrid).
- Reduction in electricity bill and process improvement.

- Make diagnosis or continuous monitoring of a system in order to improve performance and service continuity and ensure the protection of building and people.

Power Meter: Several companies offer boxes to monitor in real time and record data specific power consumed by the building or facility. The current sensors previously mentioned coupled with power meters can measure active and reactive power of the installation and can be connected to a human-machine interface (on the internet, on smartphones, etc...) with a follow-up, a review of consumption. We can even, for some applications, act on other ordered sensors (smart switches for example), which will unload the networks using for example PV storage batteries.

Lighting sensors: Lighting accounts for over a third of energy consumption in buildings (in France or united Kigdom) as shown in Figure 3.1.1-1.

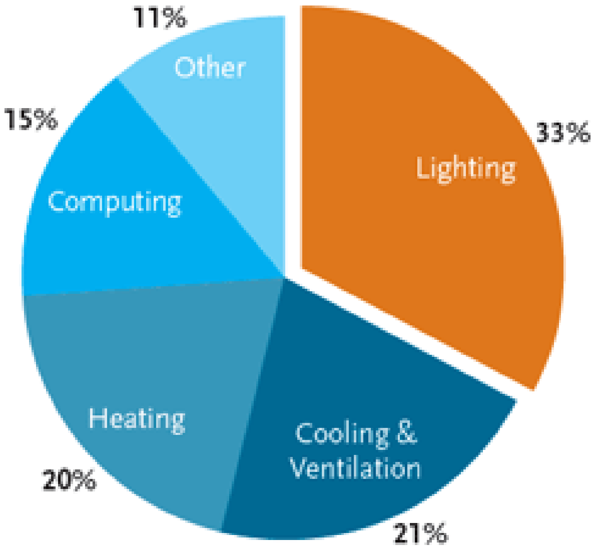


Figure 3.1.1-1 Repartition of energy consumption in buildings

In order to reduce power consumption, multiple sensors can be used:

- Batteryless wireless switches control lighting and shading
- Batteryless outdoor light sensors automatically match lighting to daylight
- Occupancy sensor (see paragraph 3.1.4) adjusts temperature and turns off lights when a room is not in use.
- Sensors which adjusting the brightness in the room depending on the light outside.

Smart Thermostats

The smart thermostats use occupancy sensors to save energy by automatically turning off the HVAC when occupants are sleeping or away.

3.1.1.4 Systems normalization

Given the diversity of systems, equipment and means of communication developed to improve comfort and management of power consumption in the building, it became necessary to work on the standardization of equipment in order to cross the systems and devices without difficulty and allow interactions. The remote control is a good example of the tool that multiplies and that only works with the device with which it is provided. It's the same principle for many wireless smart sensors.

CENELEC, the European Committee for Electrotechnical Standardization, has set up a technical committee, the "Technical Committee" 205 (TC 205), on the issue of "Home & Building Electronic

Systems". After publishing technical reports on field network standards (BatiBUS, EIBUS, EHS, etc.), the TC 205 focuses on other topics: certification, inspection of facilities, gateways to telecom, communication radiofrequency or infrared. A standard installation and wiring home automation and building automation systems is being finalized.

The BatiBUS, EIBUS and EHS systems had being merged to create KNX system at the end of the 90s. This standardized system allows to enable the communication between the equipment of different actors (sensors, controllers and effectors) and contrary to others protocol systems, KNX is not a master/slave protocol. More standardized systems exist, similar to KNX, which permit to connect several types of equipment with data exchanges. They are more developed in part 3.2.2.

3.1.2 Physical Detection and Anti-intrusion Sensors

The technologies presented in this section are part of the state of the art about detection and anti-intrusion sensors in the context of Fuse-IT project. Security of premises and perimeter protection are the aim of these sensors.

3.1.2.1 Radar

Radar (RAdio Detection And Ranging) uses electromagnetic waves to secure extended areas. This system emits a powerful signal through an antenna. The reflected signal is then analyzed to detect and to determine the speed of the target thanks to the Doppler shift. Some radars also localize the detected object. Indeed, there are different types of radar. The most used are:

- Continuous-wave radar. The radar emits continuously from one antenna and receives on another antenna. It only measures the speed of the object.
- Pulse-Doppler radar [RAD]. The radar emits an impulsion and waits that the reflected signal comes back. It measures the speed and localizes the object.

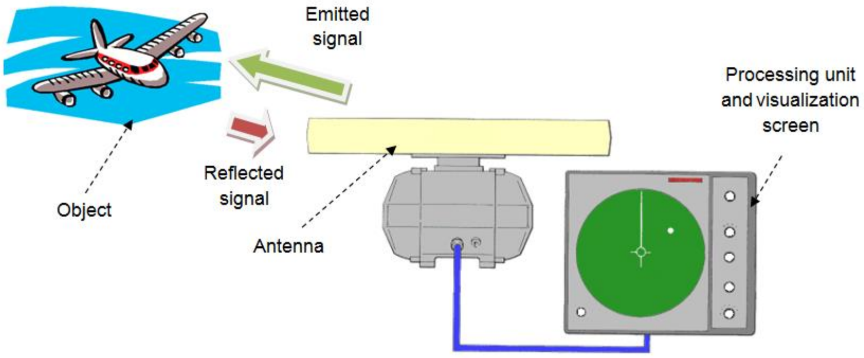


Figure 3.1.2-1 Operation scheme of the Pulse-Doppler radar

This technology offers a wide range of applications to survey extended areas with a high level of security (aerial surveillance, ground surveillance, building surveillance, etc). The radar range can be from a few meters to thousands of kilometers according to the chosen model. Mobile system also exists. Nevertheless, the cost of such a system is still very high and the implementation can be very complex [RAPID].

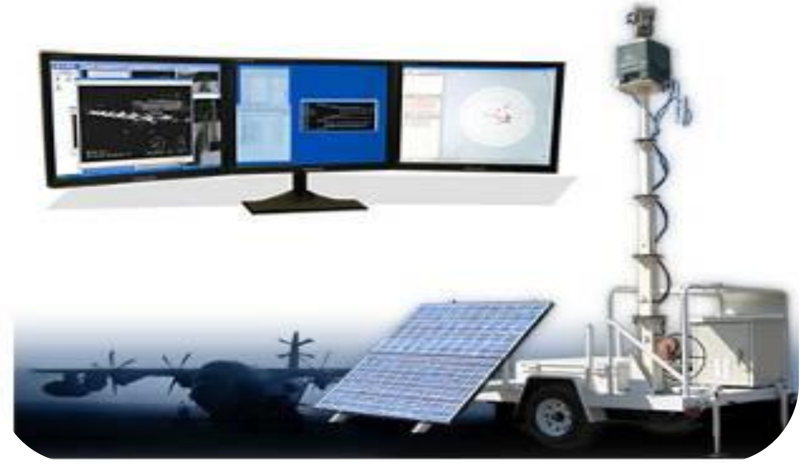


Figure 3.1.2-2 Example of mobile radar

3.1.2.2 Volumetric Detectors

Volumetric detectors can detect every movement inside a volume. Solutions, compatible with indoor and outdoor applications, use three types of detection:

- Passive infrared sensors
- Active microwave sensors
- Active infrared sensors

The range of these sensors can reach several hundred meters [HGH].

3.1.2.2.1 Passive Infrared (PIR)

Every object emits a thermal radiation in the infrared wavelengths. The Passive Infrared volumetric detector [PIS] detects the temperature variations during a movement in the area that it covers. The "passivity" of the system refers to the fact that the devices do not generate any energy for detection purposes.

3.1.2.2.2 Millimeter Wave (MW)

These sensors detect motion through the principle of Doppler radar. It gathers in the same antenna the functions of emission and reception of the microwave. The emitted signal is reflected by its environment, received by the antenna and analyzed by the processing unit. A movement inside the covered area modifies the signal and its analysis can trigger intrusion alarms.

3.1.2.2.3 Laser Scanner (LS)

The Laser Scanner detects and localizes objects. A very short luminous impulse is emitted by a laser diode. Then, the system measures the time between emission and reception which is directly proportional to the distance sensor-object. Thanks to the rotating mirror polygons, the Laser Scanner emits successive "shots" in order to scan a wide angle of about 180°.

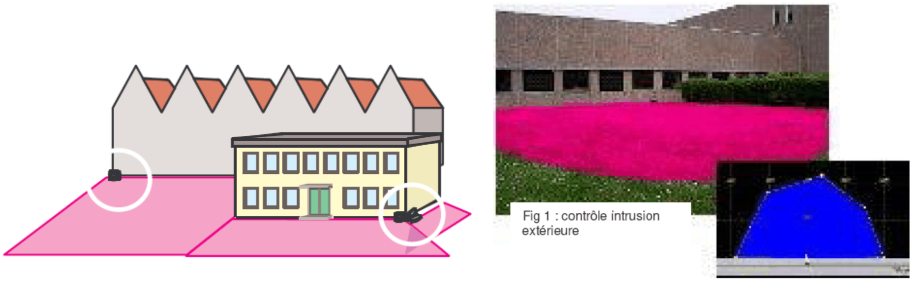


Figure 3.1.2-3 Implementation example of Laser Scanner

3.1.2.2.4 Bi-technology (PIR and MW)

The bi-technology sensor associates a Passive Infrared sensor and a millimeter ware sensor. The comparison of PIR data and MW data enables to discriminate false alarms from those generated by an intrusion [PIR_BI].

3.1.2.3 Video sensors

Video sensors propose automatic solutions of video surveillance. The types of video sensor in a security system can be various from visible cameras to IR cameras [VID]. The triggering thanks to video-based detection of an event enables the system to keep only pertinent images. A video sensor can detect several kinds of event such as:

- Movement detection
- Presence detection
- Break-in detection
- Abnormal behavior detection

Video sensors versatility makes easier their use in various operational scenarios (volumetric surveillance, perimeter surveillance, etc).

Figure 3.1.2-4 Face detection

Moreover, numerous mobile solutions exist in the market (drone, embedded camera, etc). However, these sensors are very sensitive to luminosity and contrast variation. As a consequence, theses systems generated a lot of false alarms. Outdoor systems use for instance video filter to diminish parasite images.

On the other hand, the digitalization of images has enabled numerous treatment algorithms to be applied to the video streams. Some of these algorithms can be carried out by dedicated processors within the camera itself. We then speak of smart cameras [IVSS]. The main advantage of this is to overcome the losses in quality due to compression or to transmission problems. The images are therefore processed with their full dynamic range, before they are degraded by compression and transmission. This opens the way to new possibilities, such as only transmitting the relevant information deduced from the video analysis. In this case, the architecture of the system is said to be “distributed”.

3.1.2.4 Perimeter sensors

These systems detect the break-in of a material or immaterial barrier by a person. Perimeter sensors can secure a perimeter of about 400 meters.

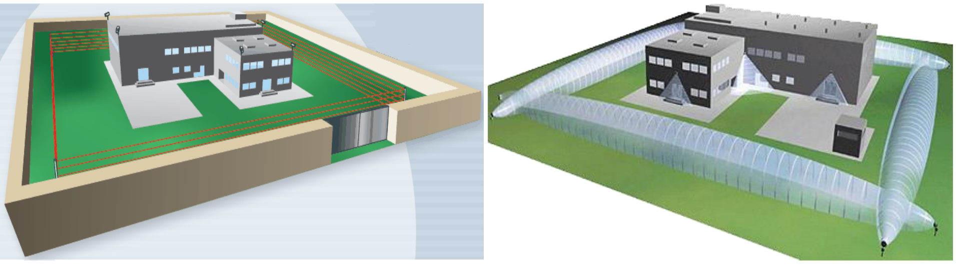
3.1.2.4.1 Infrared Barrier

An Infrared Barrier is constituted of transmitters generating infrared light beams and of receivers which detect the cut-off of beams.

This technology is tested and ensures a high level of security. On the other hand, the implementation of these modular systems is relatively easy.

3.1.2.4.2 Microwave Barrier

A Microwave Barrier is constituted of a transmitter generating an directed electromagnetic field and a receiver which detect the changes in this electromagnetic field when a person cut off the surveyed perimeter. The wide range of the covered area enables these systems to have a great detection rate. The range can reach 8 meters wide and high.



(a) Infrared barriers

(b) Microwave barriers

Figure 3.1.2-5 Example of implementation: (a) infrared barriers, (b) microwave barriers

3.1.2.4.3 Impact Detector

This technology detects vibrations caused by a person when he tries to breach or escalade the surveyed perimeter. The processing unit sends an impulsion on the cable and analyzes the reflected signal thanks to a digital signal processing algorithm in order to detect and localize the intrusion point. The precision of the localization is about 3 meters [EXEN].

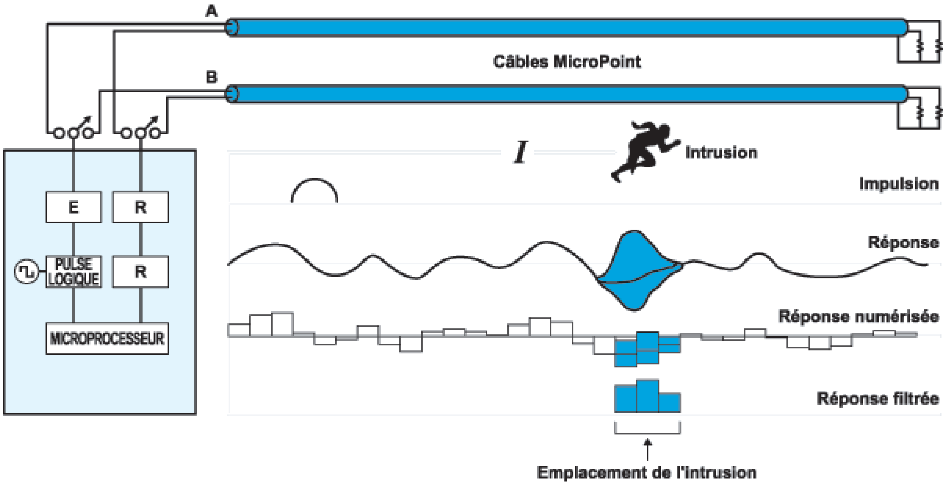


Figure 3.1.2-6 Detection scheme of an impact detector

3.1.3 Heterogeneous traffic data

To achieve the efficient energy management and the safe operation of the electrical equipments within the smart buildings, sensors must be able to control diverse set of applications. Sensed data have different QoS requirements which depend on the traffic that the application generates. In [OPT1, 2, 3, 4], the authors classify and prioritize different types into many classes.

In general Smart Building application characteristics and its traffic requirements are attributed in terms of:

- **Data rate**: closely related to how fast the data is transmitted
- **Reliability**: the communication node should always be reliable for continuity of communication
- **Latency:** can be described as the delay of the data transmitted between the different components

The most important applications are:

- **Advanced metering (AMI)**: allow two way communications between the smart meter and utility system. The smart meter periodically transmits data to the utility system. It measures energy consumption for billing and statistical purposes. The utility system also forecast price signal to the smart meter. Hence, due to the AMI application, the customer can view his real time consumption information in addition to the real time pricing.

- **Demand-Response (DR)**: controls the energy demand and loads of customer. The goals of the DR application are to achieve the balance between electrical energy supply and demand, maximize the use of the electricity generated by the bulk power transmission system the customer represents the key of success of the application. Hence data generated must be transmitted in near real time in order to satisfy the user and minimize his waiting time for an alternative energy sources.

- **Distributed Energy Resources (DER)**: sensors are deployed to control the distributed generation and storage systems in order to coordinate between them and increase the participation of the renewable energy resources into energy consumption.

Fast and reliable data transfer is a key requirement for the DER in order to achieve a complete vision of the available electric resources to be used at different time of the day.

- **Emergency-Response (ER)**: sensors are deployed to control malicious actions on the electric grid. Data generated may not tolerate any latency. For the other applications latency is not critical.

All these diverse communication requirements must be meeting and sensor nodes must be prioritized in addition to the traffic generated if the sensor generates different types of traffic.

The following sub-section introduces sensors with opportunistic spectrum access capability.

3.1.4 Opportunistic spectrum access sensors

Traditionally sensor nodes operate in unlicensed frequency bands which become more and more overcrowded because of the number of the emerging technologies using these frequency bands. Satisfying smart building communication needs is very difficult by the use of these traditional sensors. To this end deploying sensors with cognitive radio capability can enhance the network performance by dynamic spectrum access. In this case smart building sensors are called secondary user. They operate in licensed bands in the absence of primary user signal and they must vacate frequency bands if a primary user reappears.
To have the ability to interact with the environment and adapt to any changes, several cognitive functions have been added to the secondary user sensors:

- **Spectrum sensing function**: sensors are able to monitor spectrum bands in any given time and detect the available spectrum holes.

- **Mobility function**: if a signal of a primary transmission is detected, sensor can change its operating frequency band and continues its transmission without interruption.

Several literature work consider the use of the cognitive radio technology for smart building and smart grid communication network as promising candidate. It allows a better user of spectrum which is a limited resource in unlicensed spectrum bands. Moreover cognitive radio technology increases the interoperability among heterogeneous communication network.

There are different approaches which have been carried out in the field of cognitive radio deployment for smart grid applications [OPT3, 4, 5, 6].
In what follows, we introduce the two most important ones.

- In [OPT3], the use of the cognitive radio technology to improve the wireless communication QoS in the harsh smart grid environment is proposed. The authors presented a distributed control algorithm for data delivery requirements. Data traffic is classified into different priorities to deal with each traffic class according to its QoS demands. Simulation shows that the proposed framework achieves the required QoS.

- In [OPT4] a priority-based traffic scheduling approach was proposed to improve the performance of Cognitive Radio communication infrastructure to support real-time communication in a smart grid. The heterogeneous traffic types in Smart Grid are classified and prioritized for traffic scheduling in order to obtain the optimal resource utilization.

3.2 Smart Networks

3.2.1 Smart Grids and Micro-Grids

With growing environmental concerns, the European Union (EU) has adopted ambitious targets, for 2020, to:

- 20% increase in the share of Renewable Sources of Energy (RES) in the energy mix.
- 20% decrease in the CO2 emissions of EU countries compared to 1990.
- 20% increase in energy efficiency.

These political objectives will change the energy use and the management of the electricity system. In the past 10 years in France, we have had an increase of 15% of the electric consumption and an increase of 33% of the maximal annual peak intensity, see Figure 3.2.1-1. This is the result of demographic growth, the use of electrical heating and the increasing utilization of electronic devices.

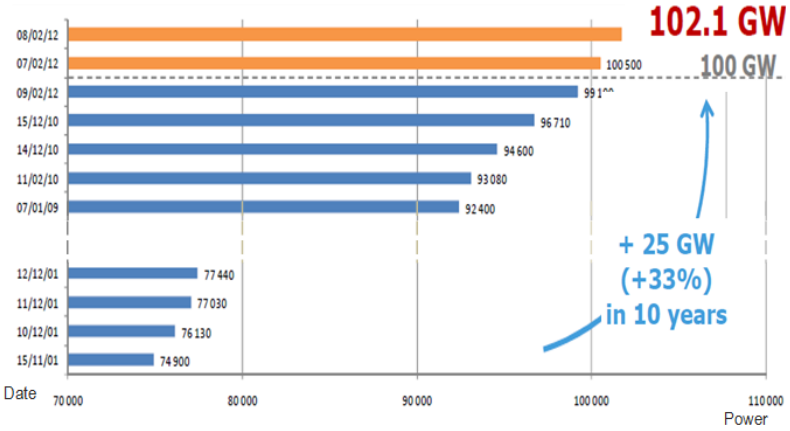


Figure 3.2.1-1 Rise of the peak intensity in the last decade in France

On the one hand, consumers, such as Electrical Vehicles for example, develop and increase the consumption of electricity already on the rise and complicate the control of electrical networks. Moreover, the electricity consumption depends on the seasons and fluctuates during the day. Energy consumption is higher in winter than in summer and there are two daily peaks for domestic consumers. On the other hand, the development of decentralized production leads to more production sites and to injecting energy in the distribution network which was initially designed for a flow of power from the producers like power plants to the consumers.

The smart grid fits in this context. In fact it is an electric network with computer technology and controllers that can control and communicate with infrastructure. It manages a power flow in both ways taking into account decentralized production.

The integration of new information technologies and communication networks will take into account the actions of various actors in the grid, while ensuring a more efficient power delivery, which is also economically viable and safe.

The electrical system will be better controlled and more flexible to handle constraints such as the intermittency of Renewable Energy (RnE) and the development of building automation. These constraints will also have the effect of changing the current system where the balance is provided in real time by adjusting production to consumption, into a system where the adjustment will be more by the demand, making the consumer a real actor. The grid becomes a system where all the actors interact.

3.2.1.1 The development of Renewable Energy

Over the past five years, the number of photovoltaic and wind energy producers has increased. There should be approximately one million by the year 2020 [GRID]. A part of the production of RnE is intermittent and not controllable while electric networks were originally designed to deliver electricity produced centrally, from production to consumption. Intermittency means that they have both non-controllable variability and are partially unpredictable. The injection of this Renewable Energy production involves the two-way operation of electric networks. The development of decentralized RnE (wind, solar...) connected to electric grids will therefore profoundly alter the exploitation of the electrical system. In the near future, networks will not only distribute produced electricity, but it will also have to deal with all decentralized productions. At the same time, power grids must still meet the objectives of ensuring the security, stability, reliability, and quality of service. The integration of RnE in the grid implies disturbances in the grid. The PV installations have the following consequences on the networks: local variation of voltage, voltage unbalance, fast variation of power, harmonics, etc.

In case of high production and light load there is overvoltage; furthermore, in case of light production and heavy load there is under voltage, so the intermittent nature of PV production implies voltage variations. Therefore, if voltage exceeds the limits, the inverters are disconnected.

Moreover, the grid influence on PV system operations includes: voltage variation on network, harmonics and voltage dips. In this context, smart grids appear as one of the possible solutions to integrate RnE while meeting the objectives for the grid. They will manage the electrical system and make it reactive to deal with distributed and unpredictable energy. The aims are to diminish the impacts and maximize the services.

3.2.1.2 Electrical System Upgrade

Management of electrical networks, centralized and unidirectional from production to consumption, becomes bidirectional, see Figure 3.2.1-2. This will lead to a change in the way we design and manage the network. This adaptation of the electrical system must go through the integration of new information technologies and communication networks.

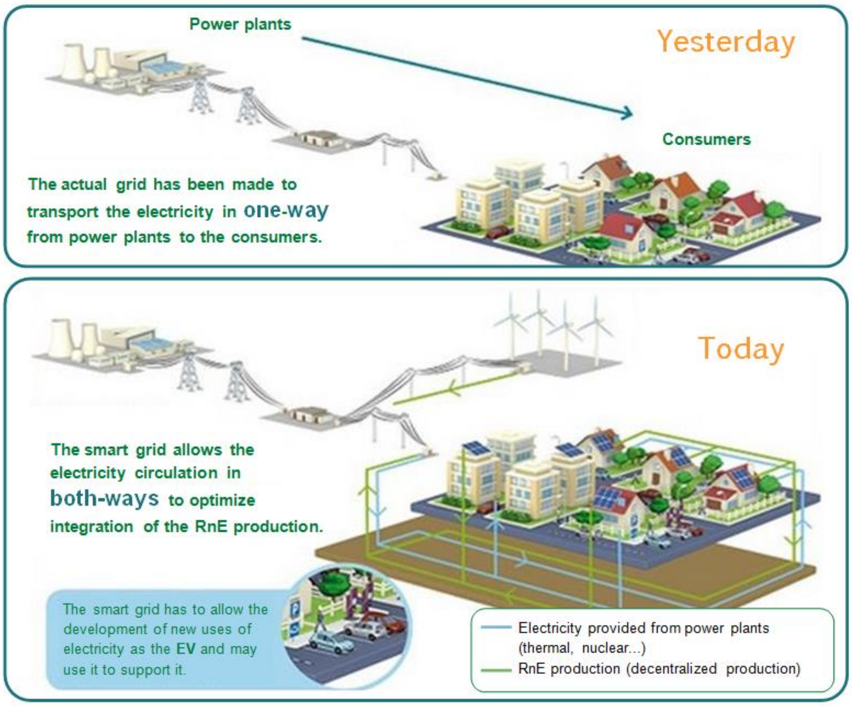

Power plants
Yesterday
Consumers
The actual grid has been made to transport the electricity in one-way from power plants to the consumers.
Today
The smart grid allows the electricity circulation in both-ways to optimize integration of the RnE production.
The smart grid has to allow the development of new uses of electricity as the EV and may use it to support it.
Electricity provided from power plants (thermal, nuclear...)
RnE production (decentralized production)

Figure 3.2.1-2 The evolution of the electricity circulation [CRE]

The smart grids actors are interconnected because they incorporate information and communication technology. This communication takes into account the actions of the various actors in the electricity system, including consumers. The aim is to ensure a balance between supply and demand at all times with responsiveness and reliability.

The smart grid architecture can be divided into three parts:

- The infrastructure to carry electricity (lines, transformers, etc.).
- The communication architecture based on different media and communication technologies (fiber, GPRS, PLC, etc…), for collecting data from sensors installed on electrical networks.
- The applications and services, such as systems for remote troubleshooting or prices acceptance using information in real time.

Table 3-1 Electric grid vs smart grid features

Actual electric grid features	Smart grid features
Analogue	Numerical
Unidirectional	Bidirectional
Centralized production	Decentralized production
Communicating on one part of the grid	Communicating on whole the grid
Manage the electrical system balance by the production	Manage the electrical system balance by the consumption

Actual electric grid features	Smart grid features
Consumer	Consum’actor

In the smart management, there are many possibilities and many application levels. For example, at the building level, the smart management is to control and handle the production and the consumption of a building. It can produce power and use it, the buildings become producers and not just consumers. It relieves the main grid by diminishing its consumption and facilitates load management from the grid point of view.

To ensure the reliability of the previous scenario, we need to develop an algorithm which estimates the building’s energy consumption knowing the weather forecast and usage information. The service can inform and advise the consumer of the possible actions improving energy efficiency or minimizing the cost of energy.

Numerous scenarios can be developed to handle the electric network in an intelligent manner. The responsibility of the consumer becomes more and more significant.

As the consumer can also be a producer of electricity (solar panels…), the grid must therefore take into account the flow of electricity in two directions: to collect electricity generated on one side and to distribute it to consumers on the other.

In a context where the commitments made at the environmental level requires users able to better manage their energy consumption. The development of smart grids technologies will go along with the change in consumption patterns of households, businesses and industries.

In this perspective, one of the main projects of the electricity networks of the future is to ensure that all users know how to manage their real-time energy consumption, through a system of information collection. This system must be able to turn on or off some domestic appliances, depending on the state of the electrical system. The consumers may also be encouraged to island their houses totally or partially using their own productions during peak consumption.

The main goal of smart grid is to assist in balancing the power generation and the power consumption using sensors, communications and monitoring. Therefore, one can say that the Smart Grid concept covers different areas, depending on the approach. More broadly, the following items are identified:

- Smart Metering. The first approach to the Smart Grid concept occurred for more than a decade ago and only intended, in fact, the telemetering. To reach this goal, the Automatic Meter Reading (AMR) technology was developed and implemented. It had the advantage of replacing the manual, expensive and inefficient readings, also avoiding the use of estimated measures, which do not give customers accurate information about their consumption, which is considered today, important in order to induce changes behavior related to energy consumption. The next generation of metering equipment, corresponded to the Automatic Meter Management (AMM) technology that besides the telemetering, allowed turning on and off the power supply and also modify the maximum power available to the consumer. The AMM technology enables also monitoring failures and power quality.
- Information and communication technologies (ICT). The Smart Grid is the integration of electrical and communication infrastructures with advanced process automation and information technologies within the existing electrical network. It is a huge challenge to motorize in real time the network Grid and all the devices connected to it. The ICT are crucial for the success and implementation of the Smart Grid concept. There are several

communication technologies that could support Smart Grid communication in the distribution system, ranging from optical fiber, to power line carrier (PLC), to wireless technologies. Indeed, the wireless communication is a broad topic ranging from WiFi IEEE 802.11 to IEEE 802.15.4 and so-called LTE "Long Term Evolution" [ESU2]. The communication highlights the progresses that have been achieved in implementing the energy markets as well as their trends and developments. An important issue is the attention on Data Privacy related to the deployment of Smart Grids. It is important to assure safety in all established communications. It is justified the implementation of appropriate measures of information protection, preventing access by unauthorized third parties. Greater risk may come from an attack by "hackers" to Smart Grid, which would allow, for instance, turn off the supply to a certain customer. This may reach huge consequences when related to critical buildings such as those related to health services, governmental and military services, etc. It becomes therefore important to assure the reduction of the Smart Grids vulnerabilities. Physical infrastructures installations (e.g. optical fiber cable) are welcome to mitigate access by unauthorized third parties, however actually the market solutions are mainly based on wireless solutions.

- Resources Management. Distributed energy resources can be defined as smaller power sources that can be aggregated to provide power necessary to meet regular demand. In this context, renewable technologies and storage can support the transition to a Smarter Grid. Deploying DER in a widespread, efficient and cost-effective manner requires complex integration with the existing electricity Grid. Research can identify and solve the challenges of integration, facilitating a smoother transition for the electricity industry and their customers into the next age of electricity infrastructure. The DERs have mechanisms that identify disturbances in the national Grid and provide real-time system isolation in emergency conditions implementation brings new challenges to the network Grids. Typically, the power systems were designed to ensure the flow of energy produced in large power plants, through a high-voltage transmission system. Energy flows were unidirectional, from generation to consumption. Micro generation changed this scenario by introducing reverse flows in the power networks. The consumer is now also producer passing from passive consumer to Smart system agent. The management of all this resources is needed, in the context of the Smart Grid, as well in the scope of the functioning of the electricity markets.
- Reliability. It is expected that the reliability of the power Grid will be increasing, preventing and avoiding power outages as well as non-technical losses. The first one is concerned to the demand increasing, which may causes an increased risk of power outages; the second relates the deployment of Smart meters that prevent fraud and allow the two ends (suppliers and consumers) to have more autonomy to manage their supply / consumption in real-time.
- Self-healing. The IEEE Smart Grid expertise [available online http:// http://SmartGrid.ieee.org/] define a self-healing infrastructure as "*a self-healing Grid that uses digital components and real-time secure communications technologies installed throughout to monitor its electrical characteristics at all times and constantly tune itself so it operates at an optimum state. It has the intelligence to constantly look for potential problems caused by storms, catastrophes, human error or even sabotage. It will react to real or potential abnormalities within a fraction of a second, just as a military fighter jet reconfigures itself to stay aloft after it is damaged. The self-healing Grid isolates problems immediately as they occur, before they cascade into major blackouts, and reorganizes the Grid and reroutes energy transmissions so services continue for all customers while the problem is physically repaired by line crews*". A self-healing Smarter Grid can provide a number of benefits that lead to a more stable and efficient system. Basically, its primary functions include: real-time monitoring and reaction (which allows the system to constantly tune itself to an optimal state); anticipation (which enables the system to automatically look for problems that could trigger larger disturbances); and rapid isolation (which allows the system to isolate parts of the network that experience failure from the rest of the system, to avoid the spread of disruption and enable a more rapid restoration).

As a result of these functions, a self-healing Smart Grid system is able to reduce power outages and minimize their length when they do occur. The Smart Grid is able to detect abnormal signals, make adaptive reconfigurations and isolate disturbances, eliminating or minimizing electrical disturbances during storms or other catastrophes.

- Power quality. Assuming the increase of the precision and coverage of power monitoring and control throughout the power Grid, delivered quality will come into sharper focus and control. It will become possible to provide distinct levels of power quality and at different costs.
- Active consumers' participation. Initially, demand response has been related to the participation by consumers in the operation of the power system, requiring that every consumer has the proper communication system (device) to perform monitoring and issue pricing signals for their power bidding. However, this can be extended to include consumers' participations by generating and selling their own power. In these cases, the consumer is called a "*prosumer*", as in one who may both consume and produce electric power [ESU3].
- Cyber security. All the information should be protected against malicious attacks that are likely to exploit the Grid´s communication network. In these cases the power Grid should operate in a fault-tolerant manner. In fact, this notion can also be adopted for natural disasters, and in both some parts of the power Grid can be disconnected avoiding outages occurrence.

Smart Grid delivery should not be based on only enabling solutions but on integrating solutions that address business and operating concerns and deliver meaningful, measurable, and sustainable benefits to the consumers, the utility, the economy and the environment. Some benefits of the Smart Grid are pointed in [ESU1,2]. The main idea is that the Smart Grid provides enterprise-wide solutions that deliver far-reaching benefits for both utilities and consumers.

For consumers the benefits of Smart Grids are:

- Reduce outage frequency and duration;
- Improve power quality;
- Empower consumers to reduce energy costs;
- Improved communications with utility.

For operational efficiency of the network Grid and distributed generation, can be identified the following benefits:

- Integrate distributed generation;
- Optimize network design;
- Enable remote monitoring and diagnostics;
- Improve asset and resource utilization.

For energy efficiency point of view, there are great benefits and are justified by the following reasons:

- Reduce system and line losses;
- Enable Demand-Side Management offering;
- Improve load and VAr management;
- Comply with state energy efficiency policies.

One cannot underestimate the effects of "*Green Agenda*" that several countries have assumed. Thus, the governmental and environmental benefits of the Smart Grid implementation are:

- Reduce greenhouse gas (GHG) emission via demand-side management and "*peak shaving*";
- Integration of renewable energy resources;
- Comply with carbon/GHG legislation;
- Enable wide adoption of EV's.

The Smart Grids uses innovative products and services, jointly with monitoring, control, communications and intelligent self-regeneration technologies in order to facilitate the connection and operation of generators of all sizes and technology, allow consumers to participate actively on the optimization of system operation, provide consumers with more information and more options for choice of the supply company, reduce significantly the environmental impact of the global system of electricity supply, maintain or even improve existing levels of reliability, quality and security of supply system, maintain and improve existing services efficiently and finally, encourage the integration of markets to an European Market.

Figure Figure 3.2.1-3 The Smart Grid characteristics and requirements [6], adapted from [ESU6], depicts the integration of the Smart Grid with the current state-of-the-art technologies in power, communication and information that envisages bringing a more intelligent and environmentally sensitive network to the existing system. It is showed a series of essential attributes for the Smart Grid that are interconnected in a very close relationship as cause-effect among one another. Each of them should be well considered for the progressive strategies and designs in both power and communications fields to support the Smart Grid development [ESU6].

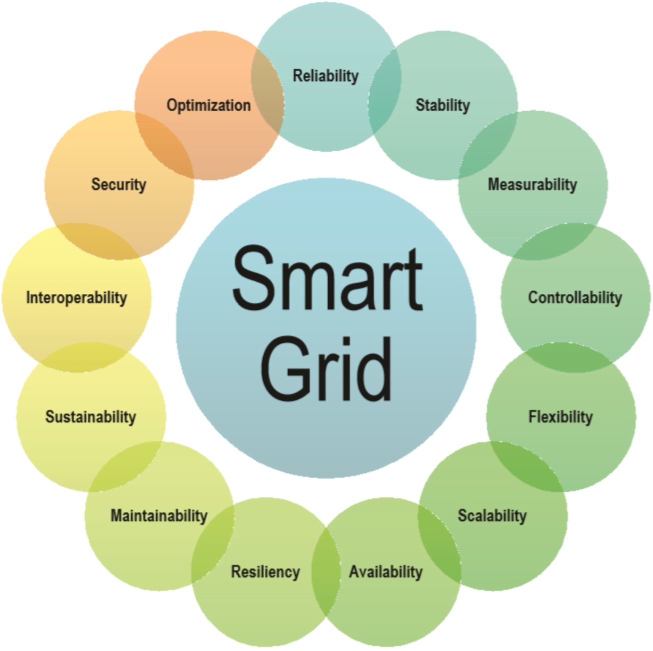


Figure 3.2.1-3 The Smart Grid characteristics and requirements [6]

All Smart Grid initiatives will need to integrate with the “Legacy Systems”. Therefore, in order to overcome the “legacy” hurdle, are created standards. In fact, without standards, there is the potential for technologies developed or implemented with sizable public and private investments to become obsolete prematurely or to be implemented without measures necessary to ensure security.

3.2.1.3 Microgrid

Clearly, the concept of a microgrid can be applied to buildings. Nowadays microgrids are proposed in the context of critical infrastructures, such as hospitals and airports, university campus, military systems and communal networks. A microgrid is intended here (critical infrastructures) as a local electrical system that includes multiple loads and distributed energy resources that can be operated in parallel with the broader utility grid or an electrical island. A building management system can be a facility or infrastructure which has to meet higher grade safety and security requirements, whether this is for national/business-strategic or public health and safety reasons.

In fact, in an increasingly constrained context with severe requirements of quality, safety and environment respect, a building-integrated photovoltaic involves advanced local energy management rather than PV power permanent grid injection [MIC16]. A local energy management can be proposed with consideration of different grid tariffs scenarios, grid injection limit, storage capacity, load and PV power shedding if necessary.

The concept of having many small-scale energy sources or micro-sources, dispersed over a grid has gained a considerable interest over the last years. Many distributed generation (DG) technologies such as micro-turbines and fuel cell are quite well known and being developed all across the world. However, there is another technology that has become feasible only in last few years and is being developed to improve voltage control as well as the power quality. It is microgrid technology.

The intensive growing of DG imposes new methodologies in power systems operation. Several approaches were proposed in recent years, namely the active networks concept, the microgrids, the virtual power players and smart grids. Although there are no consensual concepts for each approach, several developments were proposed and are being applied.

In fact, the implementation of active distribution networks requires the implementation of new concepts and microgrids have become a means to integrate and control distributed generation resources into the grid, being at the same time viewed as a “building block” of smart grids [MIC1].

The concept started in the early 2000 and one of the first definitions of a Microgrid has been proposed by Bob Lasseter in 2001 [MIC2] and was defined as a cluster of micro-sources, storage systems and loads which presents itself to the grid as a single entity that can respond to central control signals. This cluster is connected to the main grid trough an interface point that separates them from an electrical point of view and connects them economically. On the inside, is the microgrid operator that determines the conditions and the quality of service while the exterior is controlled by other entities, e.g. other microgrid or the main grid.

In 2002 the Consortium for Electric Reliability Technology Solutions (CERTS) published a white paper on the Lasseter microgrid concept and all their understanding of the application and managing of a microgrid. In this paper the need of power electronic based micro sources is reinforced as a means to provide the required flexibility to insure operation as a single aggregated system, allowing the microgrid to present itself to the bulk power system as a single controlled unit that meets local needs for reliability and security [MIC3].

In the same year, 2002, Venkataramanan and Illiandala propose the microgrid as a way of maintaining the supply of high quality loads when a fault occurs in the main grid or when the quality of the supplied power is not enough to answer the needs of the loads [MIC4].

A recent definition can be found [MIC1]: “Microgrids are low voltage (LV) distributed systems with distributed energy resources (fuel cells, photovoltaic’s, wind turbines, micro-turbines, etc.), controllable loads, and storage devices (flywheels, energy capacitors and batteries) being electrically connected to the power delivery system at a point of common coupling, thus appearing as a controllable single subsystem to the utility grid. They can be operated in a non-autonomous way, if interconnected to the main grid, or in an autonomous way, if disconnected from the main grid. The operation of the micro sources in the network can provide distinct benefits to the overall system performance, if managed and coordinated efficiently.” [MIC1]. It can be seen as a group of interconnected loads and DER with clearly defined electrical boundaries that acts as a single controllable entity with respect to the grid and can connect and disconnect from the grid to enable it to operate in both grid connected or island mode, as represented in figure 2, adapted from [MIC5]. Within the main grid, a microgrid can be considered as a controlled entity which can be operated as a single aggregated load or generator and, given attractive remuneration, as a small source of power or as ancillary services supporting the power network.

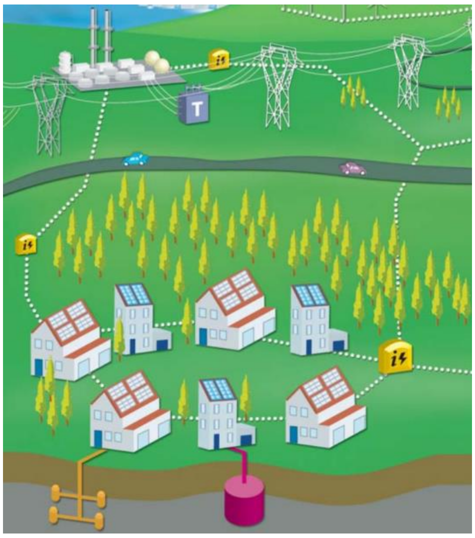


Figure 3.2.1-4 Example of Microgrid system [MIC5]

The power grid sees the microgrid as a single controllable entity behaving as a group of aggregated loads and generation sources [MIC6]. Lower net operating cost encourages interconnected microgrids to cooperate with each other [MIC7]. Establishing an effective coordination mechanism between microgrids and the main distribution system is a critical challenge in the short-term operation of integrated microgrids. The challenges associated with the design, control and operation of microgrids are enormous.

It is important to distinguish microgrid from smart grid. One can say that a microgrid is a small-scale power grid that can operate isolated or connected to the main electrical grid. A smart grid is a modernized electrical grid that uses ICT to gather and act on information, such as information about suppliers and consumers behaviour (in an automated fashion) to improve the efficiency, reliability, economics, and sustainability of the production and distribution of electricity over a wide area.

Figure 3 illustrates the microgrid concept, inserted in the context of a smart grid. Ensuring a stable operation and security requirements during faults and various network disturbances are, thus, some of the main advantages of microgrids.

Worth noting that buildings can also be considered as a microgrid since they include multiple loads and DERs that can be operated in parallel with the utility grid.

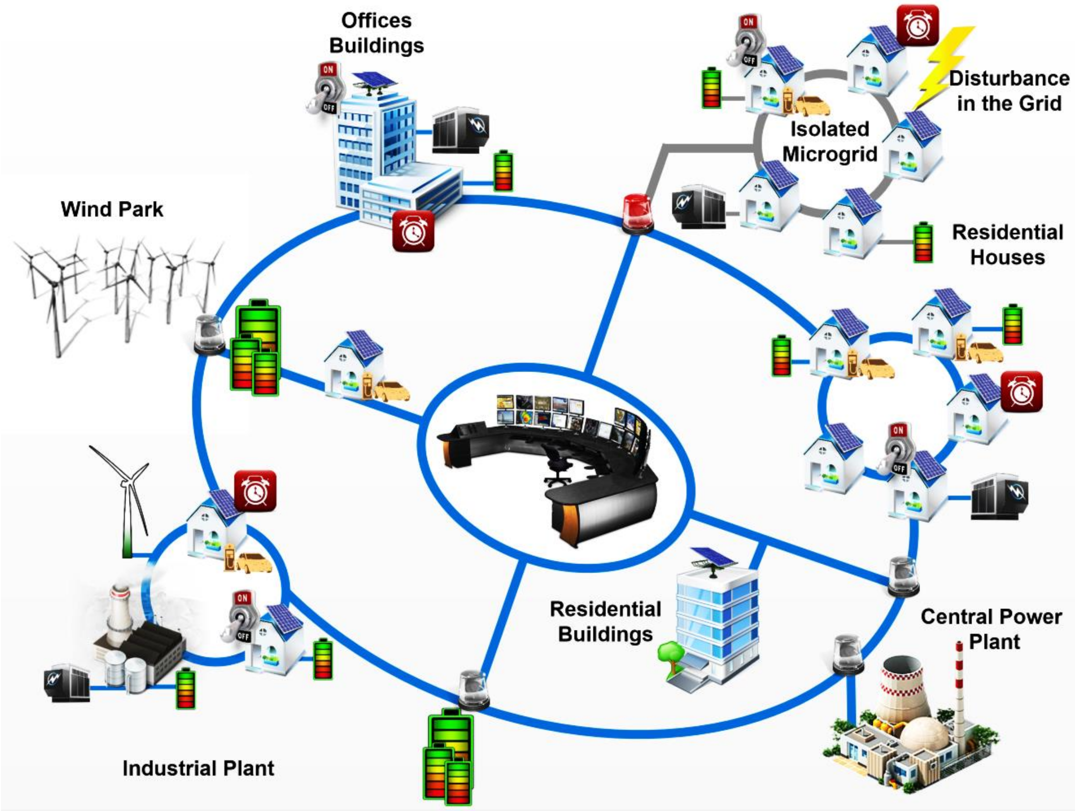


Figure 3.2.1-5 Smart Grid and Microgrid operation

The operation of system can be shared between central and distributed generators. The control of distributed generators could be aggregated to form microgrids or “virtual” power plants to enable their integration both in the physical system and in the electricity market.

Often microgrids can be intended as “back-up power” to the main power grid during periods of heavy electricity demand. Indeed, microgrids involve multiple energy sources as a way of incorporating renewable power. Other purposes include reducing costs and enhancing reliability.

Virtual utilities can adopt the structure of the Internet-like model and its information and trading capability, rather than any hardware. Power can be purchased and delivered to agreed points or nodes. Its source, whether a conventional generator, renewable energy source or from energy storage is determined by the supplier. The system can be enabled by modern information technology, advanced power electronic components and efficient storage.

To enable the implementation of the microgrid concepts, assuring the change of the electricity supply structure towards progressively more distributed generation, renewable energy source and “active grids”, it is required that a wide number of factor should be addressed [MIC5]:

- Improvements of security standards, in the context of critical infrastructures;
- Integration of both central and distributed generation;
- Integration of innovative technologies into existing grids;
- Harmonisation of equipment standards to allow “plug-and-play”;
- Increased funding for large research incentives, including public and private sharing;
- Impact of neighbouring electricity systems on the European network;
- Higher education and skills issues. With regards to education and skills, it is already evident that an insufficient number of well-trained engineers are being produced in the power

engineering field. In order to develop, operate and maintain future networks, cross-functional, intra-disciplinary educational strategies must be adopted.

Microgrids can offer important advantages to both consumer and utility. For customers, the Microgrids can provide both thermal and electricity needs, and in addition enhance local reliability, reduce emissions, improve power quality by supporting voltage and reducing voltage dips, and potentially lower costs of energy supply. For utilities, the implementation of distributed energy sources can potentially reduce the demand for distribution and transmission facilities.

In the European Union (EU), the promotion and deployment of DERs are expected to benefit energy consumers, the European energy system, and the environment through optimization of the value chain from energy suppliers to end users. Microgrids are considered a basic feature of future active distribution networks, able to take full advantage of DERs, if coordinated and operated efficiently. They have been studied in a number of researches, development, and demonstration (RD&D) projects, and they form a key component in the Strategic Research Agenda for Europe's Electricity Networks of the Future, available at http://ec.europa.eu/research/energy/pdf/smartgrids_agenda_en.pdf [MIC8].

Important European projects have been conducted in order increase the penetration of microgeneration in electrical network through the exploitation and extension of the Microgrids concept. At the EU international level, major research efforts have been devoted exclusively to microgrids [MIC9]. Within the 5th Framework Programme (1998–2002), the "Microgrids: Large Scale Integration of Micro-Generation to Low Voltage Grids", ENK5-CT-2002-00610 (www.microgrids.eu), was funded at €4.5 million. The Consortium, led by the National Technical University of Athens (NTUA), included 14 partners from seven EU countries, including utilities such as EDF (France), PPC (Greece), and EDP (Portugal); manufacturers, such as EmForce, SMA, GERMANOS, and URENCO [MIC8]. In the scope of Microgrids projects, the main objectives of the RD&D were to:

- Study the operation of microgrids to increase penetration of renewable and other DERs while reducing carbon emissions;
- Study the operation of microgrids in parallel with the grid and islanded, as may follow faults;
- Define and develop control strategies to ensure efficient, reliable, and economic operation and management of microgrids;
- Define appropriate protection and grounding policies to assure safety, fault detection, separation, and islanded operation;
- Identify and develop the required telecommunication infrastructures and protocols;
- Determine the economic benefits of microgrid operation and propose systematic methods to quantify them;
- Simulate and demonstrate microgrid operation on laboratory scales.
- For a wide deployment of Microgrids the main guidelines are as follows:
- Investigation of new micro source, storage and load controllers to provide efficient operation of Microgrids Transition from interconnected to islanded operation provides challenging frequency control problems. Close coupling of active-reactive power in low voltage (LV) networks complicates voltage control.
- Development of alternative control strategies (centralised versus decentralised). Several levels of decentralization can be applied, ranging from a fully decentralized approach to a hierarchical control.
- Alternative Network designs Inverter dominated Microgrids are not necessarily subject to the same frequency limitations, as traditional power systems. The advantages of operation at variable frequencies including DC operated Microgrids should be investigated together with the application of modern protection philosophies and modern solid state interfaces and other devices.

- Technical and commercial integration of Multi-Microgrids Integration of multiple Microgrids into the operation of a de-carbonised power system, perhaps with millions of active participants, requires radically new control and management structures and practices to make possible the interface with the upstream DMS and the operation of co-ordinated, but de-centralised markets for energy and services.
- Impact on power system operation. The distinct advantages of Microgrids on power system operation, regarding increase of reliability, reduction of losses, environmental benefits, etc. have been quantified at regional, national and EU level.
- Impact on the development of electricity network infrastructures. Large penetration of Microgrids will have a massive impact on the future operation and development of electricity networks. Microgrids must become a key part of the overall network reinforcement and replacement strategy of the aging EU electricity infrastructure. New tools and simulation approaches are needed to address this objective and to quantify the benefits of Microgrids.

Following Microgrids FP5 project, the “Advanced Architectures and Control Concepts for More Microgrids”, an European Project Supported by the European Commission within the Sixth Framework Program (2002-2006), SES6-019864 (www.microgrids.eu) improved concepts and pilot sites. The consortium, led by the National Technical University of Athens (NTUA) and having as Coordinator Nikos Hatziargyriou, comprises manufacturers, including Siemens, ABB, SMA, ZIV, I-Power, Anco, Germanos and EmForce; power utilities from Denmark, Germany, Portugal, the Netherlands and Poland; and research teams from Greece, the United Kingdom, France, Spain, Portugal, and Germany [MIC8]. This project involved the investigation of alternative microgenerator control strategies and alternative network designs, development of new tools for multi-microgrids management operation (involving Distribution Management System architectures and new software adaptation) and standardization of technical and commercial protocols.

On the Portuguese field tests, EDP Distribuição (EDP) analysed the behaviour of a microturbine installed in the Ílhavo Municipal Swimming-Pool (MSP) [MIC8-9], supplying the local load in islanding mode and exporting power in grid connected mode. The interaction between this microturbine and a Diesel gen-set was also analysed in islanding mode. The main objective was to demonstrate the feasibility of transferring microturbine and MSP loads from grid connected to islanding mode under various operating conditions. This includes transferring in several load and generation regimens and the necessary load control. Field tests demonstrated the feasibility of transitions between grid connected and islanding modes.

CONTINUON’s MV/LV facility project [MIC8-9] operates a holiday-park with more than 200 cottages. A great number of these cottages are equipped with Photovoltaic (PV) generators, coupled to the grid by means of inverters. The total amount of installed PV-power is 315 kW. The cottages are connected to a MV/LV transformer using four LV-feeders. The load of these cottages is during daytime low compared with the PV-power. So in daytime most of the PV-power is injected in the MV-grid. In the evening (and night) of course some support from the MV-grid is needed. During the several seasons the load and generation profiles will be different.

In Mannheim-Wallstadt [MIC8], Germany, a Pilot installation is implemented on residential area in order to integrate DG, active distribution grid and microgrid operation. Several PV systems were implemented and connected to the LV grid.

The F.Y.R.O.M - Kozuf Microgrid Project [MIC8-9], Greece, intended to cover the electricity needs of a small sheepfold, located near the new ski-centre on Kozuf Mountain. The sheepfold owners, who are also involved in the ski-centre investment, have envisaged utilization of renewable energy sources for electricity supply for the sheepfold. Within the ski-centre project, there is also a Waste Water Treatment Project that will allow treatment of the ski centre municipal wastewater. Further on, the idea was to construct a pilot plant for biogas production which will accept the surplus sludge from the municipal waste water treatment plant, the biomass from the sheepfold as well as the waste water from a small diary production line which exists at the sheepfold. The plant will be constructed underground and located close to the sheepfold. The produced biogas will be used for electricity production, while the fermented waste will be composted and will be used as an organic fertilizer.

LABEIN main site in Derio (Spain) aims at the increase of penetration of microgeneration in electrical networks through the exploitation and extension of the Microgrids concept, involving the investigation of alternative microgenerator control strategies and alternative network designs, development of new tools for multi-microgrids management operation (involving Distribution Management System architectures and new software adaptation) and standardisation of technical and commercial protocols [MIC8-9].

In [MIC10] it is possible to find critical literature review of various Microgrids architectures, and also the benefits of grid-connected or isolated microgrid with storage are properly identified. In Table 1 we can see that the majority of microgrids testbeds have implemented central controller systems and only few of them have autonomous or agent-based ones.

Table 3-2 Existing examples of Microgrids in Europe [MIC9]

Location	Power supply	DC source	Energy storage	Microgrid controller	PQ control	Communication
Bronsberg, Netherlands	AC	PV	Battery	Central	None	GSM [MIC11]
Am Steinweg, Germany	AC	CHP, PV	Battery	Agent based	∗PoMS	TCP/IP [MIC12]
CESI RICERCA DER, Italy	DC	PV, wind, diesel, CHP	Battery	Central	Flywheel	Combination of LAN Ethernet, wireless and power line [MIC13]
Bornholm, Denmark	AC	Diesel, wind	None	Autonomous	None	Optical fiber network [MIC11]
Kythnos, Greece	AC	PV, diesel	Battery	Central	None	Power line [MIC11]
CAT, Wales, UK	AC	Hydro, wind, PV	Battery	Central	None	Not discussed [MIC15]

∗PoMS – Power flow and power quality management system.

The microgrid team at Berkeley Lab, California (http://building-microgrid.lbl.gov/), studies customer adoption patterns of grid technology and distributed energy resources (DER) optimization in microgrids and buildings. Since 2000, the team has been developing the Distributed Energy Resources Customer Adoption Model (DER-CAM). DER-CAM is a tool that outputs microgrid investment and dispatch results that minimize costs or emissions. This shows how a building can be as a microgrid and not only part of a microgrid.

In scope of [MIC1] three major messages are identified regarding on what really consists a Microgrid:

1. Microgrid is an integration platform for supply-side (microgeneration), storage units and demand resources (controllable loads) located in a local distribution grid;
2. A Microgrid should be capable of handling both normal state (grid-connected) and emergency state (islanded) operation.
3. The difference between a Microgrid and a passive grid penetrated by microsources lies manly in terms of management and coordination of available resources.

In short, the microgrid concept highlights three essential features that are, local controllable loads, local micro-generation and intelligent control.

In the scope of the microgrids operation the IEEE Standards Coordinating Committee supported the development of the IEEE P1547.4 Guide for Design, Operation, and Integration of Distributed Resource (DR) island systems with Electric Power Systems. This guide provides alternative approaches and good practices for the design, operation, and integration of distributed resource island systems with electric power systems (EPS). This includes the ability to separate from and reconnect to part of the area EPS while providing power to the islanded local EPSs. This guide includes the distributed resources, interconnection systems, and participating electric power systems. This document intends to be used by EPS designers, operators, system integrators, and equipment manufacturers and also intends to provide an introduction, overview and address engineering concerns of DR island systems.

3.2.1.4 Building as a Microgrid

The increasing use of distributed generation, namely from renewable energy sources, brought several challenges to buildings system operation. The large amount of energy consumption at buildings can be saved through optimized energy management and operation without, necessarily, changing the building structure and the hardware configuration of the energy supply system.

Microgrids mostly operates interconnected to the utility grid, but also can turn into an islanded mode, in case of external faults. In fact, microgrid technology provides a huge opportunity and desirable infrastructure for improving the efficiency of energy usage in buildings. The main key to improve building energy efficiency is to coordinate and optimize the operation of the several energy sources and loads [MIC17].

Along last year’s many efforts have been made to improve building energy efficiency. One important target was concerned to improve building materials and structures in order to save energy consumption (caulk windows, double glazing, better wall and flooring materials, etc.), improving the efficiency of Heating, Ventilation and Air Conditioning (HVAC) systems by natural ventilation integrating the information of outdoor environment, increasing the utilization ratio of sunlight improving the efficiency of the lighting system and also by using more efficient lamps, such as lamps based on LED technology. The integration of renewable energy resources and distributed storage systems can really contribute to save energy significantly.

One of the main question that needs to be address is the operation of the building infrastructure in order to coordinate the several energy infrastructures and loads to aim the safety of energy supply while satisfying occupant comfort requirements.

A typical microgrid for buildings integrates the operation of electrical and thermal energy supply and demand. The supply may include energy sources from distribution grid, autonomous power generators such as fuel cells, combined heat and power (CHP) systems, renewable energy resources such as photovoltaic panels and wind power generation, energy storage devices, such as batteries and water tanks, and also electrical vehicles that may consume or inject electricity to the power grid. The typical electrical loads include those for HVAC, lighting, elevators, information technology, data centers, a range of household appliances, etc.

The focus to improve operation efficiency of building energy consumption is, in fact, to coordinate and optimize the operation of various energy sources and loads. Therefore, it can be seen as a scheduling problem, which the main goal is to take advantages from the integration of distributed generation, electricity market prices and demand response programs without depreciating the users comfort levels.

The scheduling of all these resources is subject to large random and uncertainties fluctuations. Moreover, the electricity generation from renewable sources depends on atmospheric conditions that have a high level of uncertainty and variability. The lighting demand, elevators usage, and others loads directly related to dynamic occupant movements and human behaviours are also subject to significant uncertainties and high uncertainties in both supply and demand may cause major difficulties in scheduling and control problem.

The building energy operation and management, maintaining the occupants comfort requirements, makes the building operation as a microgrid a problem extremely challenging.

3.2.2 Building Automation and SCADA

3.2.2.1 Building Automation

Building Automation Systems (BAS) are centralized, interlinked, networks of hardware and software, which monitor and control the environment in commercial, industrial, and institutional facilities. While managing various building systems, the automation system ensures the operational performance of the facility as well as the comfort and safety of building occupants. Typically, such control systems are installed in new buildings or as part of a renovation where they replace an outdated control system.

Generally, building automation begins with control of mechanical, electrical, and plumbing (MEP) systems. For instance, the heating, ventilation, and air-conditioning (HVAC) system is almost always controlled, including control of its various pieces of equipment such as, for generic examples, air handling units, roof-top units, fan coil units, heat pump units. Lighting control is, likewise, essential for optimizing building performance. Other systems that are often controlled and/or brought under a complete automation system include: power monitoring, security, close circuit video, card and keypad access, fire alarm system, elevators/escalators, plumbing and water monitoring.

Most of the automation system is behind the scenes as hardware devices mounted to equipment or hidden under the floor or in the ceiling. Some personalized control can be made available through thermostat-like devices. From a central management perspective, the BAS resides as software on an operator workstation (computer) or is available as a web page. Various types of "controllers" manage equipment and portions of the network.

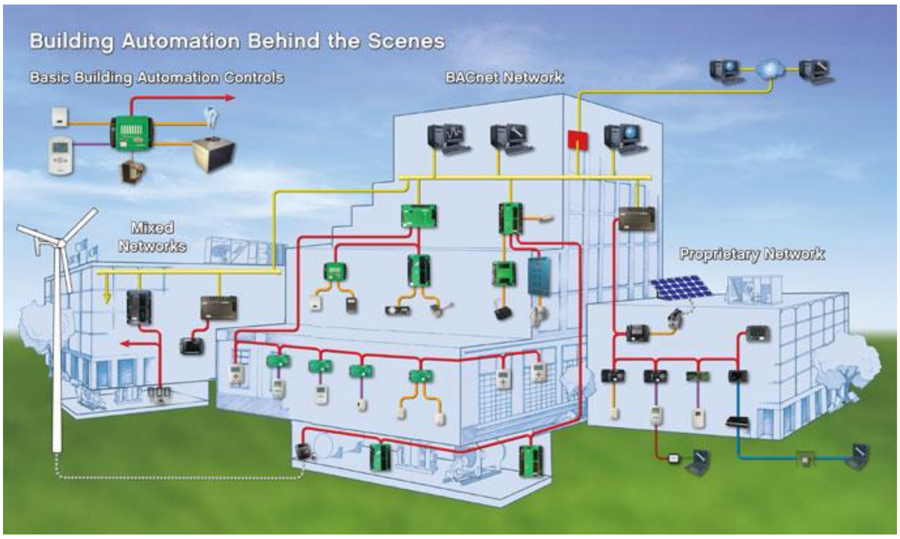

Building Automation Behind the Scenes
Basic Building Automation Controls
BACnet Network
Mixed Networks
Proprietary Network

Figure 3.2.2-1 A generalized view of a building automation system

3.2.2.2 BAS architecture

Building automation system contains three main levels (Management, Automation and Field levels) distinctly separated as represented in the following pyramid (cf Figure 3.2.2-2) [BAS1].

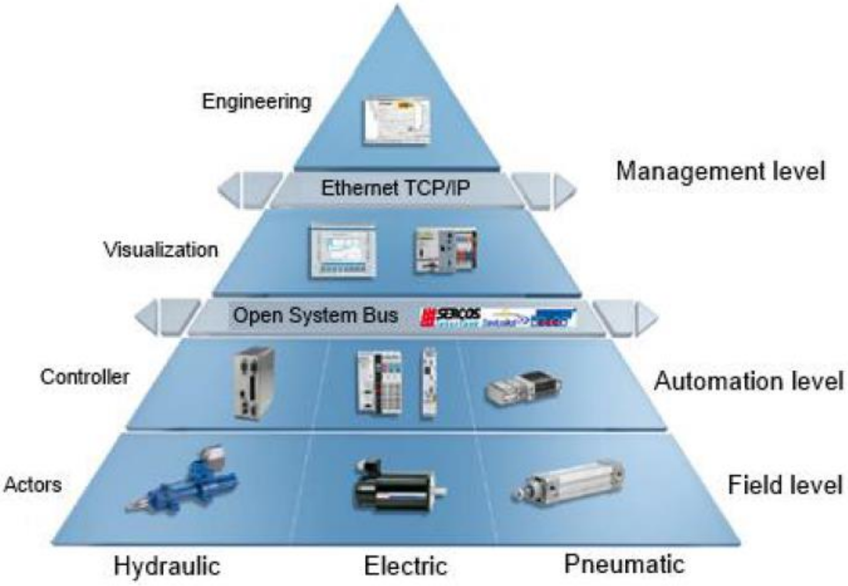


Figure 3.2.2-2 - Automation architecture. (source :Rexroth, Bosh Group).

The communication between different levels are made by different communication media and known protocols such as Ethernet (TCP/IP) or various open system buses. All these communication protocols allow to all the equipment such as heating, cooling, ventilation, lights, etc.. to communicate between each level.

Some systems topology have been developed for building automation by, for example, Siemens or Kieback&Peter shown in figures Figure 3.2.2-3 and Figure 3.2.2-4. Because of the standardized open system buses, the system topologies made by different manufacturers may vary but look very alike.

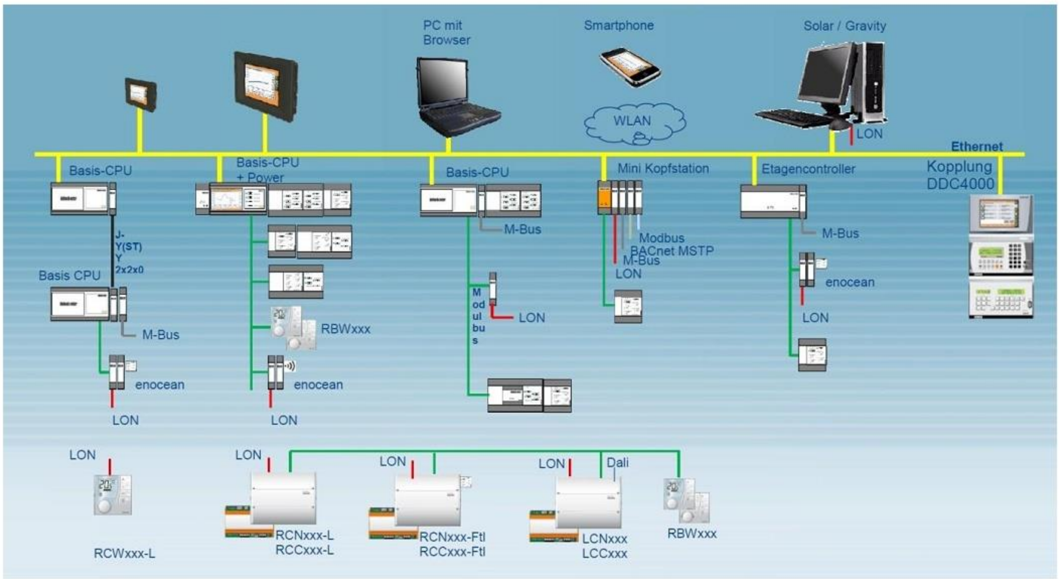


Figure 3.2.2-3 - System topology within the Kieback&Peter Company (source Kieback&Peter GmbH & Co. KG)

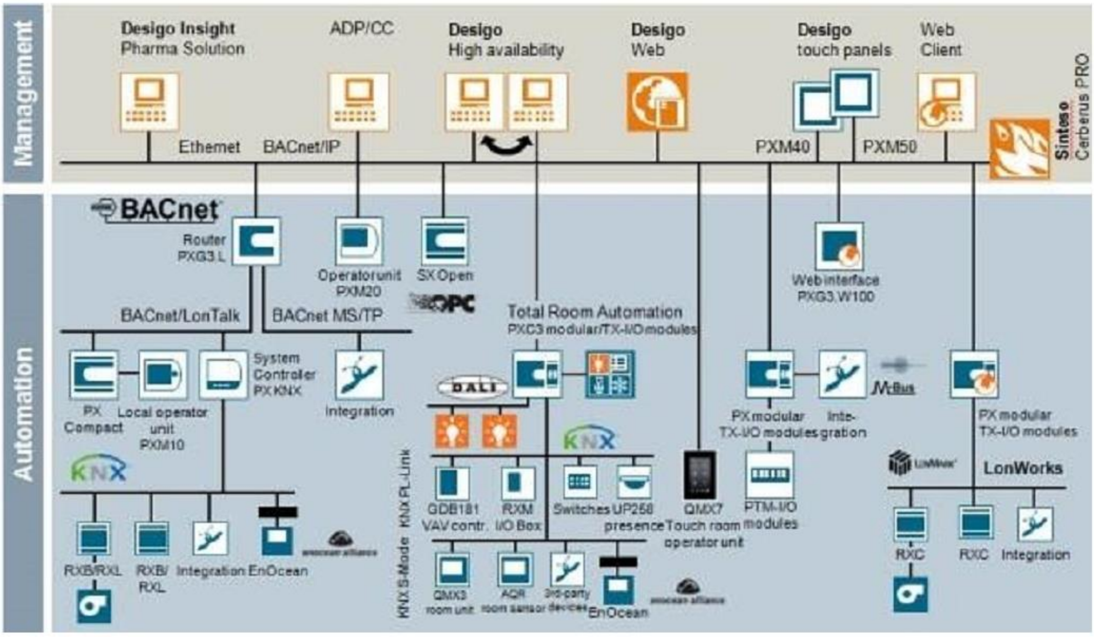


Figure 3.2.2-4 - System topology of DESIGO BAS from Siemens (source SOA BaaS)

One of the standardized open system bus, BACnet, will be described next below.

3.2.2.3 BAS example: BACnet

BACnet is the acronym for “Building Automation and Control networking protocol”. It is a communications protocol for building automation and control networks. BACnet was designed to allow communication of building automation and control systems for applications such as heating, ventilating, and air-conditioning control, lighting control, access control, and fire detection systems and their associated equipment. It is one of the standards for building automation. The goal of such a system is to integrate equipment from different sellers. To realize this task, BACnet takes place at several levels as described on the Figure 3.2.2-5 here below.

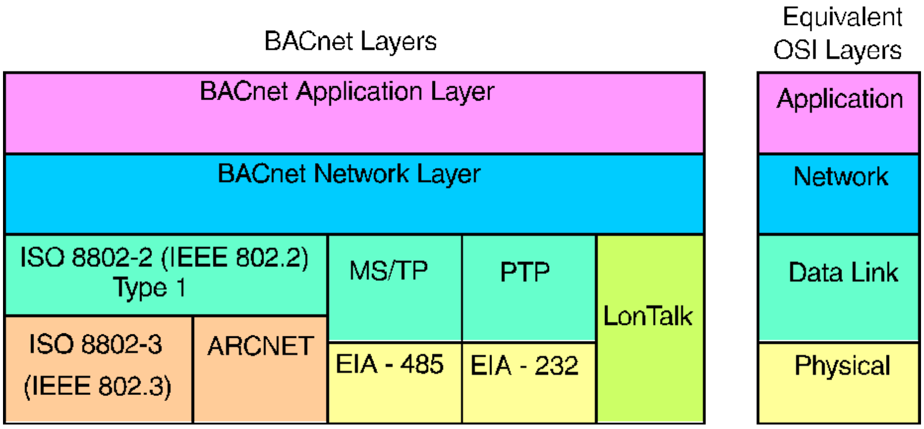


Figure 3.2.2-5 - BACnet architecture. Steven T. Bushby - Automation in Construction

BACnet interact with four layers based on the OSI (Open System Interconnection) model:

- Application
- Network
- Data link
- Physical

The BACnet protocol provides mechanisms for computerized building automation devices to exchange information, regardless of the particular building service they perform. Proper communication between building automation devices is critical for maximizing building energy efficiency, indoor air quality, and other aspects of "green" buildings.

BACnet became ISO 16484-5 in 2003. ISO 16484 defines a general conceptual framework of BAS. There is a need for standards enabling open systems in the sense of systems “which can be repaired, modified, and extended by everybody with the necessary basic qualification without having to rely on the original manufacturer”. Consequently, corresponding standards were developed, like KNX, LONworks, SCS and have already achieved considerable significance in the world-wide market. They, however, concentrate on field communication issues, while the integral automation and management functions still rely on proprietary solutions. Additionally, standards for specific functional domains are currently being developed, e.g. the IEC standard DALI (Digital Addressable Lighting Interface).

In front of that background, newest trends in BAS raise an urgent need for enhanced inter-working between different functional domains. This would enable open, flexible and integral high-level automation functions and overcome the limitations of the current heavyweight gateway architectures. Moreover, new trends in data communication for distributed building automation arise from the adoption of new IP-based device communication technology (IPv6, 6LoWPAN), of wireless communication (Wifi, IEEE 802.15.4, ZigBee, 6LowPAN), and from the development of BAS-oriented application layer communication protocols (e.g. Web Services, BACnet/WS, oBIX, CoAP, Sensor Observation Service).

3.2.2.4 SCADA

Supervisory Control and Data Acquisition (SCADA) is a computer system for gathering and analyzing real time data. SCADA systems are used to monitor and control a plant or equipment in industries such as telecommunications, water and waste control, energy, oil and gas refining and transportation. A SCADA system gathers information, such as where a leak on a pipeline has occurred, transfers the information back to a central site, alerting the home station that the leak has occurred, carrying out necessary analysis and control, such as determining if the leak is critical, and displaying the information in a logical and organized fashion. SCADA systems can be relatively simple, such as one that monitors environmental conditions of a small office building, or incredibly complex, such as a system that monitors all the activity in a nuclear power plant or the activity of a municipal water system. SCADA systems were first used in the 1960s.

For Building Automation, the SCADA system allows to manage, control and supervise equipment. It is composed of monitoring software, a Programmable Logic Controller (PLC), a measure equipment, and control drivers.

For a smart management, optimization algorithms will be implemented in the SCADA system. The objectives for building automation are:

- Minimize intentional load disconnection (load shedding or else) while keeping consumer preferences (set formerly)
- Adjust consumption, by reducing or increasing consumption depending on the actual context (hour, weather forecasts, energy price, etc.)
- Automatic energy management, optimal respect of set point, taking into account the whole sensors included in the building
- Possibility for the consumer to manage loads manually (subject to discussion depending on the liberty degrees willed
- Consumer/SCADA interaction

3.3 Management Systems

3.3.1 Energy monitoring

3.3.1.1 Purpose and Advantages

There is an increasing demand for continuous access to power and with the less disturbance possible (power quality). Today’s power environments increases the requirement for continuous and reliable monitoring of the power consumed. Each disturbance that occurs reduces the quality of delivery and power and thereby gives an increased cost. Also, electrical equipment tend to be built up of electronics that not only create disturbances on the power and transmission network but are also more sensitive to poorer power quality [EMT1].

In a common house context an energy interruption may lead to higher costs and some lack of comfort but nothing critical as long as the failure only last some hours. However, in industrial and critical buildings the impact is considerably higher. For instance, a power failure in health care facilities may have severe consequences. Therefore is of most importance to monitor the energy to understand the energy usage and to improve the energy availability considering the facilities priorities and requirements.

The main energy monitoring advantages can be considered, by category:

Environmental: helps to understand better how energy is used within a facility to improve efficiency and minimize waste and reducing energy consumption.

Reliability: Assessment of data from the monitoring system can reveal existing or imminent issues within the facility.

Maintenance: Data trends can help forecast and notify when discrete equipment parameters may be exceeded, allowing to plan ahead instead of facing unpredicted shutdowns.

Safety: Monitoring systems typically allow controlling every action remotely minimizing the need for people to enter in potentially hazardous electrical environments.

Financial: More than avoiding unnecessary system startups and reducing the maintenance effort, monitoring systems help to validate billings [EMT2].

3.3.1.2 Monitoring System Components

Energy monitoring systems are usually composed by 3 essential elements:

- Monitoring devices strategically placed though the facility to monitor.
- Software to store, manage, display and build reports based on the acquired information.
- Communications interfaces between the software and the devices.

Devices: The devices may vary a lot in functionality and price according and should be select according to the facility needs. In the actual market devices the most common available features goes from the basic measurements like voltage, current, real and reactive power, power factor and energy usage to the most complex measurements as disturbance detection and location, harmonic distortion analysis, flicker detection, anti-aliasing, automated alarms among others. The monitoring philosophy can also be either local or remote.

There are also 2 common strategies to setup the monitor hardware devices:

- One is to install the most featured monitor devices at the main electrical switchgear and less featured devices further into the electrical system. This approach is usually taken in order to understand the quality of the energy provided by the electric utility while also grasping basic electrical characteristics within your facility.
- The other strategy is to install monitor devices that correspond with their application throughout the facility. Sensitive consumers rely on this more expensive approach to understand both their energy usage and the quality of their energy throughout their facility. Monitoring large loads may allow you to identify energy savings opportunities while simultaneously identifying electrical parameters that could damage the load or affect the product. It should be apparent that more monitoring points will provide a better model of the electrical system [EMT2].

Software: The software required in the energy monitoring systems is usually part of a Building Management System software. The basic features of the energy monitoring software are:

- Receive and Store Data: The software must be able to communicate with the monitoring devices and request their data either in real of delayed. For this, the software must have the ability to use each device protocol, which should be a standard.
- Display Data: The software should enable the user to access the acquired data in a user-friendly and easy to understand layout.
- Create Reports: Based on the stored data, the user should be able to create reports.

Below are some examples of some software which consider these features:

PowerLogic® ION EEM

ION EEM is a unifying application that complements and extends the benefits of existing energy-related data resources. These can include power monitoring and control systems, metering systems, substation automation and SCADA systems, EMS systems, building and process automation systems, utility billing systems, weather services, spot-market energy pricing feeds, and enterprise business applications. Data is automatically acquired, cleansed and warehoused. Personalized, browser-based dashboards and innovative visualization and modeling tools help you accurately monitor, validate, predict and ultimately control all energy-related expenses and risks to reliability [EMT3].

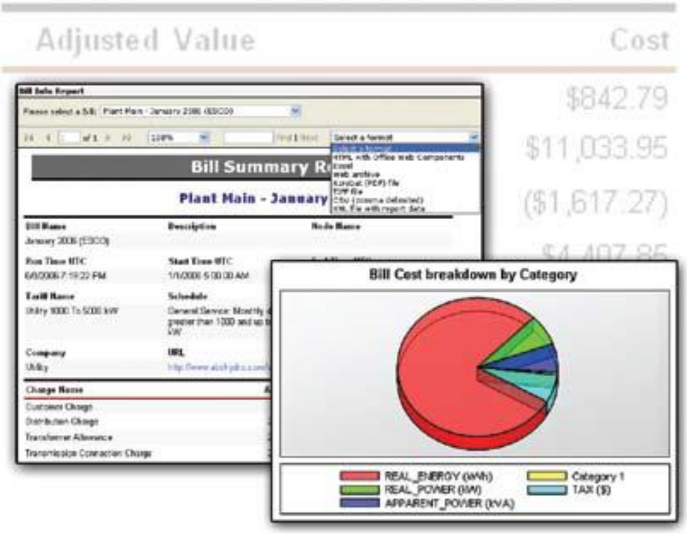


Figure 3.3.1-1 PowerLogic® ION EEM

ENMAT Energy Monitoring Software

ENMAT provides many feature as energy usage report, target setting, carbon reporting, power and demand, cost analysis, tenant billing and alert triggers. Among the reports, the software provides electricity consumption charts to enable users to actively monitor and reduce electricity usage across a single or multiple sites [EMT4]. The main charts that can generate include:

- Consumption kWh Bar Graphs split by day and night, clustered or stacked
- Detailed Consumption kWh Line Graphs

Figure 3.3.1-2 ENMAT Energy Monitoring Software

eSightEnergy

The eSight Energy provides a comprehensive and intuitive energy management suite where an extensive range of techniques for managing all aspects of energy data can be found. It allows to bring together a full set of features as advanced energy analysis tools, utility contracts analysis, reporting tools, importing and exporting data, setting up alarms, tenant billing and billing verification and benchmarking [EMT5].

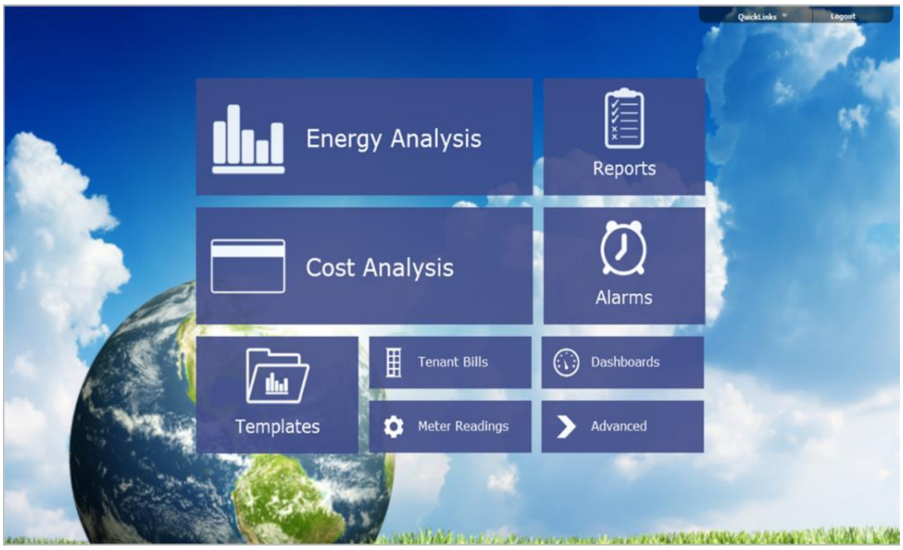
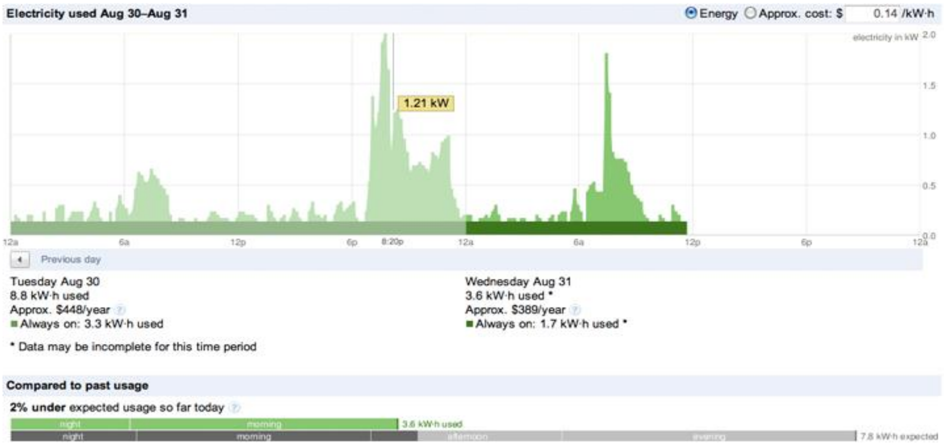


Figure 3.3.1-3 eSightEnergy software analysis dashboard view

Google Power Meter

Google launched a free energy monitoring tool which was active from 2009 to 2011 aiming to raise the awareness about the importance of giving people access their energy information. As a result, a pilot initiative from IBM revealed that, people using who monitored its consumptions this way achieved energy savings of up to 11% [EMT6].


Electricity used Aug 30–Aug 31

● Energy ○ Approx. cost: $ 0.14 /kW·h

Tuesday Aug 30
8.8 kW·h used
Approx. $448/year
Always on: 3.3 kW·h used

Wednesday Aug 31
3.6 kW·h used *
Approx. $389/year
Always on: 1.7 kW·h used *

* Data may be incomplete for this time period

Compared to past usage

2% under expected usage so far today

Figure 3.3.1-4 Google PowerMeter

3.3.1.3 Commercial Solutions

Critical Power Management Systems (CPMS)

There are many products that are used to manage the emergency/backup power system. At one end of the spectrum are simple systems with limited capabilities. However, when power management is critical to business operations, the best practice is to use a dedicated critical power management system (CPMS) to monitor, control and analyze their emergency power. Sophisticated CPMS are used in medical centers, high-end data centers and co-location facilities, and telecommunications sites, among other types of facilities.

Power controls often need to cover emergency generation sets, circuit breakers, transfer switches, bus bar, paralleling control switchgear and other emergency power system equipment. The focus is to ensure power reliability should something happen to the main utility feeds.

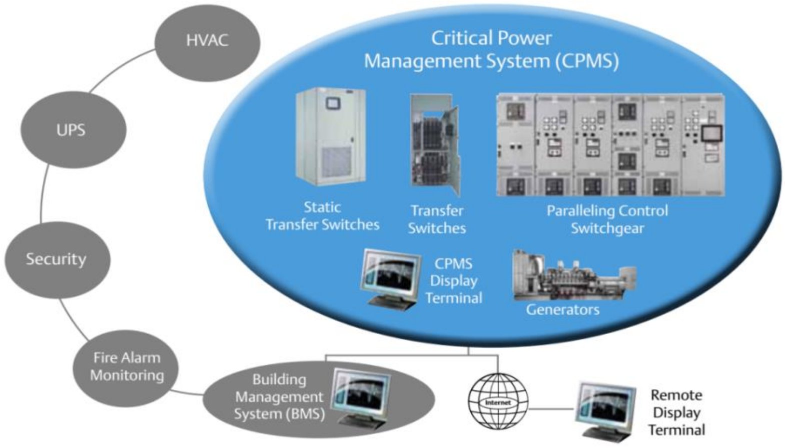


Figure 3.3.1-5 Critical Power Management Systems Overview Diagram

ViGIE Energy Audit Solution

ViGIE Energy Audit is a continuous monitoring solution for buildings, which allows the monitoring of indoor air quality conditions (IAQ), energy consumption and other parameters, integrating all data in the same software application. This continuous monitoring allows to establish a baseline scenario which defines a function of temporal projection, therefore is possible to improve through the implementation of timely corrective measures. The follow up and measurement of obtained results from the implemented measures are also made by the same process [EMT7].

This system is composed by wireless sensors with communication capabilities over high distances, which monitor the required parameters and send the data to the central processing unit, where the database and the ViGIE Energy Audit software is installed.

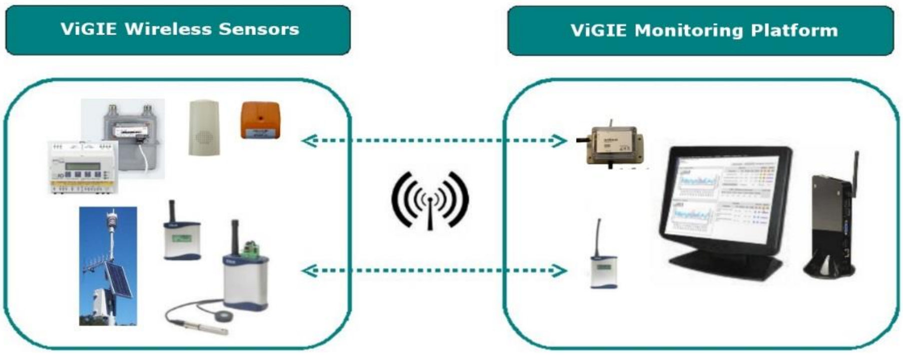


Figure 3.3.1-6 ViGIE Energy Audit main components

3.3.2 Multi-agent Systems for Building Management Systems

With rising energy costs, the need to design and integrate scalable energy consumption reduction strategies in buildings calls for novel approaches. In particular, a building management system could benefit from prediction and planning functions in order to adapt and schedule facility usages. Furthermore, in the context of collective energy schemes or when applying cost accounting, sharing mechanisms could provide incentives for energy saving and adaptation. To tackle these issues, multi-agent technologies are particularly attractive. Multi-agent theories [BMS3, BMS14] propose frameworks to capture the interactions among multiple actors in competitive and collaborative environments. In more detail, multi-agent systems address this need by proposing new control paradigms in which a set of control entities embedded in dynamic environments, are able to coordinate in a cooperative manner and to autonomously (re-) configure or to adapt their behaviour to external practitioners (e.g. energy supplier pricing scheme).

At a building level, the multi-agent technology has been mainly applied to the following three aspects of the energy management:

Building management: To model, predict and optimize buildings' energy consumption, building agents, facility managers and human occupants are demanding robust, intelligent and adaptable planning techniques to maximise the satisfaction of all actors involved.

Human-agent interaction: To develop new human-agent technologies by which the agents' decisions can be effectively communicated to, and controlled by, their human owners, while allowing a varying range of autonomous behaviours.

Collective incentivization: To address two paramount questions that arise in collective energy schemes, namely how to partition actors into the most efficient groups and how to distribute the benefits of such group interaction among its members such that all the members are satisfied with the share of profits generated.

Since the three above-mentioned categories constitute the most important and most discussed multi-agent applications in the context of building energy management, we have subdivided the rest of this section accordingly. Moreover, a section drawing potential multi-agent applications to different aspects of FUSE-IT project concludes this section.

3.3.2.1 Building Management

Building energy management needs algorithms that can continuously adapt the operation of a building in response to information such as weather, energy prices, energy carbon content and the lifestyle and preferences of its occupants. Motivated by this, several works on multi-agent systems focus on the design agent-based models of different actors and processes in a building in order to generate optimal strategies to effectively trade-o_ their individual (possibly conflicting) preferences. This entails quantifying various aspects of the system in order to be able to compare options in an optimization of multiple competing objectives.

In a home setting, [BMS11] proposes a home heating management agent that learns the characteristics of a building and its owner and the predicted local weather conditions to minimize energy costs and carbon emissions whilst satisfying the end-user comfort. Similarly, [BMS9] presents AgentSwitch, a prototype agent-based platform that make predictions of hourly energy usage and detect (and suggest to the user) deferrable loads that could be shifted to non-peak times thus maximizing home savings.

In a building setting, [BMS7, BMS4] proposes a novel algorithm (based on Markov Decision Processes) that explicitly considers multiple-objective optimization (energy and personal comfort) to generate an optimal plan not only for building usage but also for occupants. Another example is TESLA [BMS6], an agent optimizing energy usage in commercial buildings by exploiting the flexibility of different occupants to hold event/meeting schedules. In a validated simulation using a testbed building, TESLA is projected to save about 94000 kWh of energy (roughly 18K) annually.

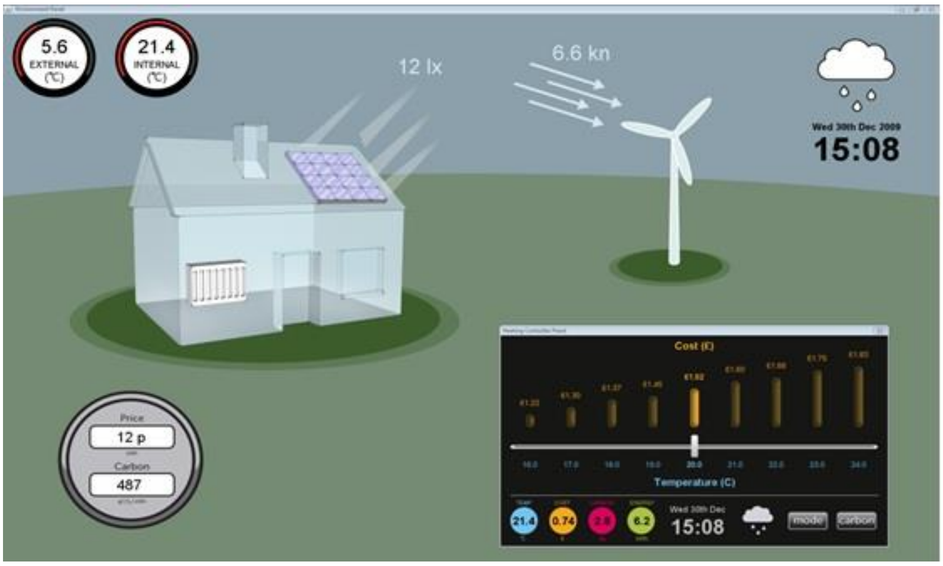


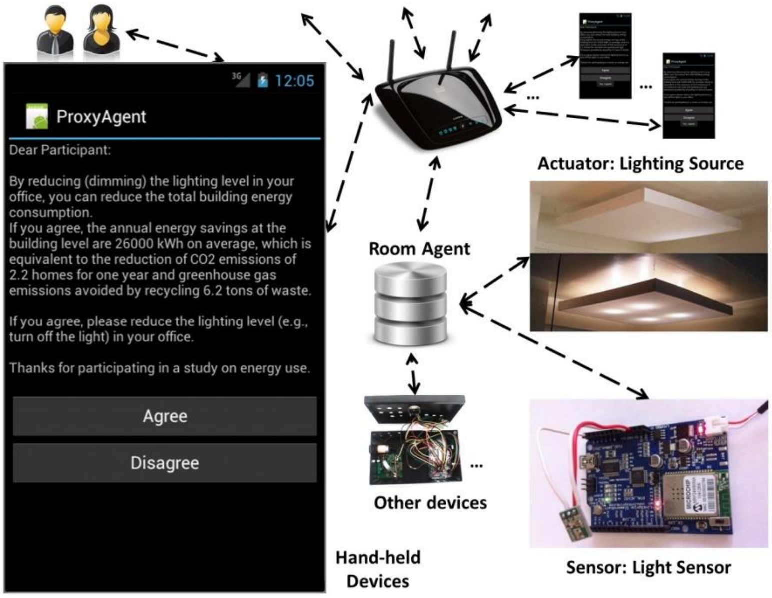
Figure 3.3.2-1 Visual interface representing the home heating energy deployed in [BMS11]

It is noticeable that conflicts can arise not only among occupants' preferences but also among subsystems of the building such as security (e.g., firewalls, antivirus, encryption) or quality of service. In [BMS8] authors addressed the problem of optimizing among various aspects of Quality of Service and Information Assurance in a way that maximizes the satisfaction of all stakeholders. Specifically, they model the problem of taking coordinated decisions as to what local actions to take to optimize QoS/IA levels as a Distributed Constraint Optimization Problem (DCOP).

3.3.2.2 Human-agent Interaction

As surveyed in the previous section, many algorithms have been developed for autonomous agents to manage building energy use on behalf of their human owners or occupants. This requires agents to interact with the humans they are representing in order to learn their preferences and improve their reactivity to the provided information (i.e. to understand what types of feedback are most effective to affect occupant's energy-related decisions). These human-agent interfaces will need also to learn which is the level of autonomy (a.k.a. adjustable autonomy) that the user prefers for such agent: if he prefers fully autonomous agents as opposed to control their preferences manually or any semi-autonomous level in the middle.

In [BMS1] authors study the notions of flexible autonomy in the context of tariff switching. They investigate a scenario where human participants may have to make, or delegate to their agent (in different ways), tariff switching decisions given uncertainties about their own consumption and tariff prices. They carried out a field trial and, from both quantitative and qualitative results, formulate novel design guidelines for systems that implement flexible autonomy.



ProxyAgent

Dear Participant:

By reducing (dimming) the lighting level in your office, you can reduce the total building energy consumption.
If you agree, the annual energy savings at the building level are 26000 kWh on average, which is equivalent to the reduction of CO2 emissions of 2.2 homes for one year and greenhouse gas emissions avoided by recycling 6.2 tons of waste.

If you agree, please reduce the lighting level (e.g., turn off the light) in your office.

Thanks for participating in a study on energy use.

Agree

Disagree

Figure 3.3.2-2 A proxy agent and its interaction with other occupants' and rooms' agents [BMS2]

The authors of [BMS2] designed and conducted a validation experiment on a group of human occupants in commercial buildings via a set of agents. A proxy agent was deployed for each individual occupant's hand-held device with the corresponding occupant's models. Proxy agents communicate on behalf of an occupant to the room agent based on their adjustable autonomy - when to interrupt a user and when to act autonomously. They conducted an investigation: i) to verify if our system can lead to changes in occupants' behaviours and to reduce energy consumption in commercial buildings, ii) to validate the parameter values and the feedback used during the negotiation process such as the acceptance/compliance rate for the suggestion.

3.3.2.3 Collective Incentivization

Significant energy actions rarely can be achieved by the action of a single individual but instead it requires the coordinated joint action of different actors. For example, in an office building, companies listed on different spaces (or even single workers) may have different preferences regarding their working hours keeping the buildings lighting, heating and cooling ongoing for most of the day. In such settings, we cannot assume that individuals will collaborate (i.e. will change their working times) if they are not properly engaged via negotiation mechanisms that allows them to agree in which groups to form at different points in time and how to share the profits. The strategic and computational aspects of such negotiation processes are typically studied within multi-agent systems using tools such as cooperative game theory [BMS13].

This is the focus of work of [BMS5] that finds ways to positively promote energy saving behaviour among buildings occupants by means of a meeting reservation system that allows the user to offer a certain level of flexibility when scheduling a meeting (i.e. by expressing a possible time window around the preferred slot). This allows energy savings (i.e. reducing re-cooling costs of vacant rooms) that are divided among the group participants using fair game-theoretic solution concepts. Game-theoretic solution concepts are different allocation criteria to divide the benefits among the participants. In particular, authors propose several redistribution mechanisms that build on the concept of Shapley value [BMS15] (developed by the Nobel winning economist Lloyd Shapley). In particular, the Shapley value is taken for each participant and is an average over all possible scenarios or combinations of the groups' flexibility related to the scheduling effect of a single participant. As a result, participants whose flexibility allows higher energy savings to the system are the ones less taxed. In this way participants are incentivized through monetary compensation that may yield towards future offerings of flexibility.

Another initiative, to go beyond the building level, is the creation of collective energy purchasing initiatives in which different individuals come together to get a better deal with the retailers. Such group buying has been shown to be both popular and effective in e-commerce (e.g. due to the success of e-sites such as Groupon or LivingSocial). In the context of energy, real-world initiatives such as the BigSwitch (https://www.whichbigswitch.co.uk/) or thePeoplesPower (http://www.thepeoplespower.co.uk/) achieved significant discounts by bringing a large number of consumers together and negotiating a better deal on their behalf with suppliers. This problem of how to take advantage of group discounts from the retailers is studied in the core of the AgentSwitch platform [BMS9] that ensures individual members of a collective fairly share discounts based on the Shapley value. Robu & Vinyals [BMS10, BMS12] take this line further by studying the group-buying incentives for a tariff scheme that encourages users to provide reliable consumption predictions. Since consumers with a stable consumption involve lower costs than consumers with an unpredictable future demand, the so-called prediction-of-use (POU) tariffs ask customers to predict their baseline consumption and charges them based on both their actual consumption and a deviation from their prediction. The above-mentioned propose cost allocation schemes that can fairly allocate the expected bill among customers taking part in an electricity group buying initiative whilst ensuring that, in expectation, any individual consumer or subset of consumers will pay less by being part of the group initiative.

3.3.2.4 Conclusions

In this section we analysed some of the main contributions of multi-agent systems to building energy management. Moreover, we foresee that such multi-agent technology can contribute to achieve the following FUSE-IT objectives and challenges.

First, FUSE-IT envisages different managers at a building level (security, energy, facilities, network) acting as a coordinated. As we have seen in this section, multi-agent technology can address this challenge by providing optimization algorithms that combine different building management objectives and solve the conflicts among

Second, research on human-agent interaction can help FUSE-IT to deliver a single-user interface for building management. In more detail, it can define what decisions are automated and what information needs to be exchanged with the building manager in order to provide him with a synthetic and readable vision of the building situation and the means to achieve the related functional requirements.

Finally, notice that even when in FUSE-IT different managers are collaborative (i.e. they are interested on collaborating to get the most efficient building operation), their vision of what is necessary to achieve such success may be extremely biased by their background and the particular focus of their activity. This can lead to each manager to be inflexible when submitting its constrains or to inflate the importance of their objectives. In this context, more than a tax, cooperative game theory concepts as the Shapley value can be seen as a social indicator, a value that characterizes the impact that the operation of this subsystem has on the level of accomplishment achieved by other subsystems in the final team configuration (i.e. if it is very low it will mean that the restrictions submitted by the manager of this subsystem are strongly undermining the performance of other subsystems). Such values can encourage individual managers to be more reasonable and neutral when expressing their constraints and restrictions or even be used to penalize their priority or their budget on future decisions.

3.3.3 Network Operation Centers (NOC)

A Network Operation Centre (NOC) is the central location where IT components, including servers and networking equipment, are monitored and controlled. It's the first place where network operator monitors, manages and troubleshoots incidents on company's network. Basically, the scope of network operation centre includes the followings aspects of: Fault Management, Configuration Management, Performance Management, Security Management and Accounting Management.

3.3.3.1 Missions

Service desk: The service desk provides the first level of service for network operations. The mission of a help desk is to troubleshoot network problems or provide guidance about software or applications. It could be part of a NOC or not, depending on the organization size and maturity.

Network monitoring: This is an activity of network management; it is used primarily to monitor performance, as it is also used to monitor availability.

Incident management: According to ITIL, an incident can be defined by an unplanned interruption to an IT service or reduction in the availability. ITIL separates incident management into: detection and recording, classification and initial support, investigation and diagnosis and resolution and response.

Forensics analysis (handling and analysis): Forensic analysis is the use of controlled and documented analytical and investigative techniques to identify, collect, examine and preserve digital information.

Communications and reporting: For controlling the efficiency of a network operations centre, it's important to evaluate key performance indicators (KPI), such as the following ones:

- How much time is spent on incident management?
- Are Service Level Agreements respected?
- How much resources and budget are being consumed?

Large institutions and massive network architecture are the ones that usually have a network operation centre. All organizations implementing complex networking environments require a high level of monitoring. Sometimes it could possible for organizations to have several operations centre either to manage different networks or to provide redundancy. A NOC embeds all workstations architecture and detailed status of the network, the operation team manages the virtualization, software, applications.

3.3.3.2 Technologies & Protocols

SNMP (Simple Network Management Protocol) is a standard widely used with TCP/IP. It allows managing devices like routers, switches, servers, workstations. In SNMPv3, USR (User-based Security Model) authentication is implemented along with encryption, allowing configuring a secure SNMP environment.

TELNET is a terminal emulation program for TCP/IP network. This protocol client-server enables to control the server and communicate with other servers on the network. For security reasons Telnet protocol has dropped rapidly in favour of SSH.

SSH (Secure Shell) is a secure network protocol for data communication, remote logins and remote command execution. Using a SSH client, a user can connect to a server to transfer information in a more secure manner than telnet for example.

SYSLOG is a standard for network devices that generates messages to a logging server. The protocol is supported by a wide range of devices and can be used to log several types of events. Unlike SNMP, Syslog can't be used to "poll" devices to gather information. Polling could be indirectly executed through a SSH channel, though.

Network management platforms are deployed in the enterprise to manage an infrastructure that consists of multivendor network elements. The platform receives and processes events from network elements in the network. Usually, in standard management platform, the following functions are available:

- Network discovery
- Topology mapping of network elements
- Event handler
- Performance data collector and grapher
- Management data browser

Troubleshooting infrastructure: Trivial File Transfer Protocol (TFTP) and system log (syslog) servers are crucial components of troubleshooting infrastructure in network operations.

Fault detection and notification is accomplished when the devices send SNMP trap messages, SNMP polling, remote monitoring thresholds and syslog messages.

3.3.3.3 Solutions & Products

In NOC solutions, a system monitoring solution is a hardware or software based system used to monitor resources and performance such as CPU.

Nagios [NOC01] is one of these solutions. It is an open source monitoring systems that keeps an eye on the network, hosts and even services using plug-ins and SNMP. It's a web-based user interface allow you to quickly discover problems and track their cause. In another kind of systems, it possible to find Ganglia [NOC02], a scalable distributed system designed to monitor clusters and grids while minimizing the impact on their performance. HP Operation Manager [NOC03] (formerly HP OpenView) is a product by Hewlett-Packard. Instead of just passively accepting SNMP traps from devices, HP Operation Manager has an agent that is installed on the various hosts monitored. These agents can be used to provide support for monitoring and automation type activities.

3.3.4 Site security supervision systems

Various technologies of the security domain and smart data analysis exist in site security supervision systems.

3.3.4.1 Infrastructure security technologies

Security of tertiary sites, public sites and industrial sites relies on a team of agents with dual role as ensuring the safety and the security of the site against accidental or volunteer damages. Optionally, night shifts are also provided.

The main technical equipments in these sites are:

- Mechanical protection of spaces, such as walls and barriers
- Access control of people and vehicles, usually thanks to a badge
- Perimeter protection for intrusion detection of people either outside the side without going through access control or inside the site to detect unauthorized entries in forbidden areas
- Video surveillance systems with the aim to visualize and record video streams coming from cameras set in the site

3.4 Security Management

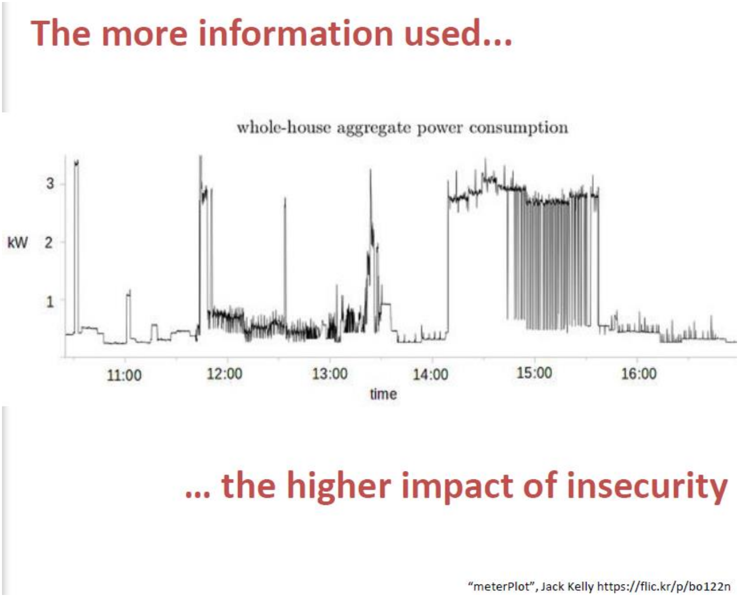
3.4.1 Smart meters and cyber security

Smart meters are a welcome change, but upgrading to a two-way communication system opens up privacy and security concerns. Despites being “Smart Meters” it appears that some of these devices are smarter than others in their ability to dissuade hackers and block unauthorized modifications.

Some interesting facts from [SM1] are presented below:

- “Smart” meters features:
    - Electronic device that records [real time] consumption of [whatever] energy
    - Send electronic meter readings to your energy supplier
    - Enable two-way communication
    - Supply outage notification
    - Supply quality monitoring
    - Change supply conditions
    - Start / stop supply provision
- What could go wrong:
    - Disclosure of confidential information
    - Compliance
    - Unauthorized manipulation
    - Interoperability
    - Business continuity
- Protection is required
    - Normally, considered ‘critical infrastructure’
        - Specific regulation
        - Government tutelage
    - Integral approach (information security + physical security/safety)
    - Both, the information and the information processing facilities

From a technical perspective this can be our future. Privacy-preserving metering aggregation is regarded as an important research topic in securing a smart grid [SM2]. In that research study it is formalized and identified a new attack, in which the attacker could exploit the information about the presence or absence of a specific person to infer his meter readings.


The more information used...

... the higher impact of insecurity

“meterPlot”, Jack Kelly https://flic.kr/p/bo122n

3.4.1-1 Impact of information usage on security [SM1]

Two novel protocols are proposed to ensure that smart meters periodically upload encrypted measurements to a (electricity) supplier/aggregator such that the aggregator is able to derive the aggregated statistics of all meter measurements but is unable to learn any information about the human activities.

The electric power grid is facing a major paradigm shift, away from static structures to a more intelligent and flexible energy utility. In order to increase the efficiency of the power net and implement new services, such as dynamic pricing, a rigorous monitoring of the grid status is required, resulting huge amount of metering data to deal and sharing with various parties [SM3]. In this regard, in [SM3] it is presented the most important results of an in-depth analysis of threats and attack vectors that could impede the wide adoption of automatic metering in smart grids.

Either in the electric power grid, or in buildings, the collection of information concerning the electrical installation status deserves special attention, mainly taking into account the use of smart meters. The most obvious risk is the meter tampering. Indeed, if a smart meter can be hacked, inaccurate information can be sent back to the utility, allowing an attacker to adjust the reading and resulting in an inflated bill.

The connectivity of the smart meters can be a security risk. Some meters can use the cellular network to provide the connection to the main servers of their utility. A truly determined hacker could abuse this “free” phone to make calls, send text messages, and even connect to the Internet. Alternately, the smart meter may use the same Internet connection as the home/businesses. This represents a potential risk because if someone was able to hack the smart meter from the outside, then that attacker would have access to the building’s internal network.

All these attacks are possible to perform, and it is extremely important to figure out how to defend against them, especially once smart meters become more prevalent.

3.4.2 Security Operation Centers (SOC)

Cybersecurity management is performed by a Security Operations Centre (SOC). This is a centralised entity devoted entirely to IT cybersecurity, which is operational 24 hours a day, seven days a week. Within companies, this unit is part of the IT department. Its specialised teams perform a series of operations on behalf of the various internal departments. When companies or organisations outsource their IT cybersecurity management to a trusted service provider, the services are said to be operated by a Managed Security Services Provider – or MSSP. A MSSP provides its services to several different customers.

As said above, a SOC is the central location where the information system cybersecurity is monitored, controlled and defended from. The scope of a SOC is to monitor, detect and process with cybersecurity incidents, to answer to strong requirements, which are not different from other information services: service continuity, information confidentiality, hardening of the network to limit as possible intrusions, experienced and accredited employees, and optionally physical security of host site.

3.4.2.1 Missions

The main activities performed by a SOC may be categorised as follows:

- Cybersecurity monitoring: Event monitoring, alarm detection and management, incident classification and management.
- Cybersecurity management: Maintenance of the information system under secure and operational conditions, provision of Key Performance Indicators, communication and reports, security component administration and change management, threat, vulnerability and non-conformity monitoring.
- Cybersecurity control: A priori and a posteriori analyses (forensics analysis which includes evidence handling and analysis), audits and penetration tests (technical infrastructure)

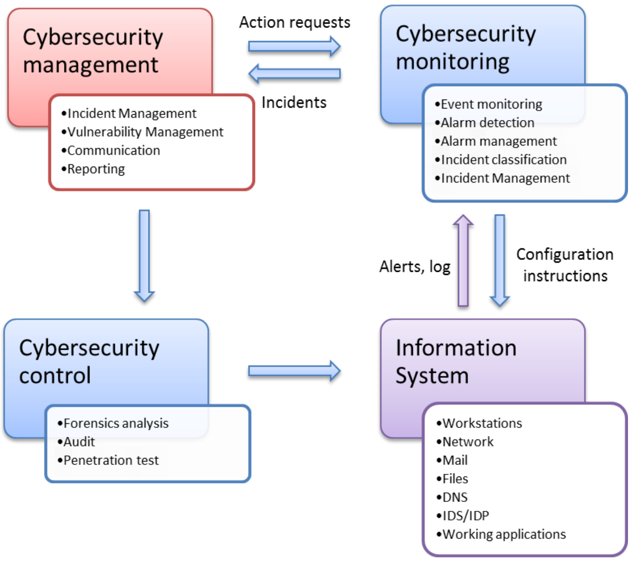


Figure 3.4.2-1 SOC activities

Cybersecurity monitoring mainly consists in performing a passive surveillance (the SOC collects security logs and incidents) or active surveillance (the SOC performs scans over the system to protect so as to detect any deviation from a known cybersecurity status). The monitoring activity consists in collecting security events (such as firewalls, anti-virus or VPN alerts and logs), asset logs (such as operating system logs), configuration changes, application logs, network flows (this packet capture is required to perform deep pack inspection), user activities.

Cybersecurity management is related governance, risk and compliance (GRC) activities, including risk analysis and security consulting for instance.

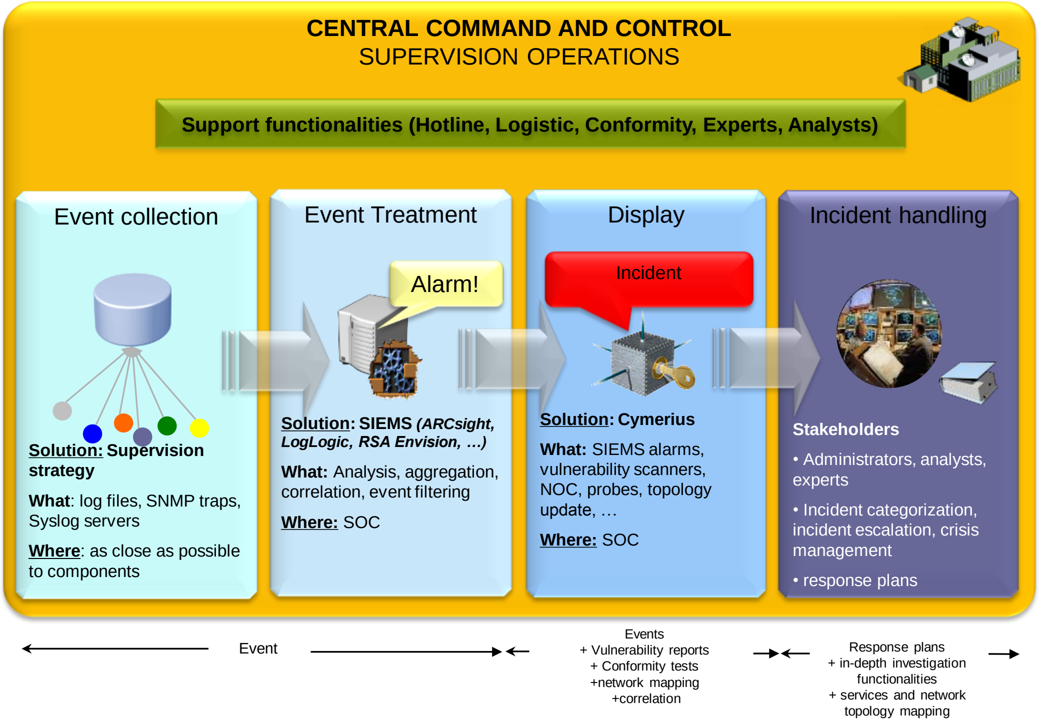
Cybersecurity control can be understood as a cybersecurity compliance policy where evidences of alterations or attacks may be collected, while at the same time a remediation plan can be enforced in order to gain knowledge over the cyberattacks and to deter similar cybersecurity risks.

It has to be emphasized that some services delivered by a SOC could overlap with the ones provided by a Computer Security Incident Response Team (CSIRT) (also known as a CERT – Computer Emergency Response Team – in the US; CERT is a registered trademark owned by Carnegie Mellon University). However a CSIRT (or CERT) should be more focused on addressing reactive services than supervision services.

Carnegie Mellon University classifies CSIRT services in three categories [SOC01]:

- Reactive services, such as alerts and warnings, incident handling, vulnerability handling
- Proactive services, such as technology watch, security audits, configuration and maintenance of security tools, intrusion detection/prevention services
- Security quality management services, such as risk analysis, security consulting or education and training

Core functionalities as described above require support functionalities, such as hotline, logistic, which are not described in this document. Best practices for service management, including support functionalities, are identified in Information Technology Infrastructure Library (ITIL) [SOC12].



CENTRAL COMMAND AND CONTROL
SUPERVISION OPERATIONS

Support functionalities (Hotline, Logistic, Conformity, Experts, Analysts)

Event collection

Solution: **Supervision strategy**

What: log files, SNMP traps, Syslog servers

Where: as close as possible to components

Event Treatment

Solution: **SIEMS *(ARCsight, LogLogic, RSA Envision, …)***

What: Analysis, aggregation, correlation, event filtering

Where: SOC

Display

Solution: **Cymerius**

What: SIEMS alarms, vulnerability scanners, NOC, probes, topology update, …

Where: SOC

Incident handling

Stakeholders

- Administrators, analysts, experts
- Incident categorization, incident escalation, crisis management
- response plans

Event

Events
+ Vulnerability reports
+ Conformity tests
+network mapping
+correlation

Response plans
+ in-depth investigation functionalities
+ services and network topology mapping

Figure 3.4.2-2 Example of an event workflow in a SOC

3.4.2.2 Technologies & Protocols

The SOC may include the following functions or tools in its scope:

- Anti-virus and anti-malware, and Advanced Persistent Threat (APT) monitoring
- Host based intrusion detection system (H-IDS)
- Network intrusion detection system (N-IDS)
- Network intrusion prevention system (N-IPS)
- Wireless intrusion prevention system (W-IPS)
- Log collectors, log aggregation, log management systems
- Unified Threat Management (UTM), firewalls, VPN, SSL, proxy, gateway; management
- Network discovery, inventory and vulnerability assessment
- Penetration testing tools
- Web site assessment and monitoring systems
- Application, middleware and database scanners
- Denial of service monitoring systems
- Security Information and Event Management (SIEM)

As part of the information sharing between SOC providers, or between security components, the next two formats may be employed:

- RFC 4765 [SOC03], Intrusion Detection Message Exchange Format (IDMEF), is an experimental protocol that defines data formats and exchange procedures for sharing information related to intrusion detection and response systems.
- RFC 5070 [SOC02], Incident Object Description Exchange Format (IODEF), defines a data representation that provides a framework for sharing cybersecurity incident amongst Computer Security Incident Response Teams (CSIRTs)

As the SOC may centralize sensitive information from many sensors, networks or security components, the aggregated information may be considered as being more sensitive than the original one.

However, data protection security target levels, or even privacy concerns, may prevent exchanging sensitive information between SOC providers, or aggregating raw logs from different customers. To that extent, privacy and anonymization techniques may be used to prevent unauthorized disclosure and to guarantee privacy requirements. In addition, restrictions may apply, according to the EU member state regulation, to sanitize auditing logs or to retain data. In that case, monitoring across secure boundaries may be an architecture challenge as gateways and/or data diode must be enforced in the system.

As of today, there is neither mature technology nor commercial off-the-shelf (COTS) that cleans off log file and audit trail data, historical records or anonymizes evidences.

3.4.2.3 Solutions & Products

IDMEF is implemented by the following products:

- SIEM Prelude [SOC04]
- NIDS Snort [SOC05]
- NIDS Suricata [SOC06]
- HIDS OSSEC [SOC07]
- HIDS Samhain [SOC08]

SIEM: Gartner [SOC13] has identified the leading Security Information and Event Management (SIEM) solution provider in its famous “magic quadrant” as shown in the Figure 3.4.2-3.

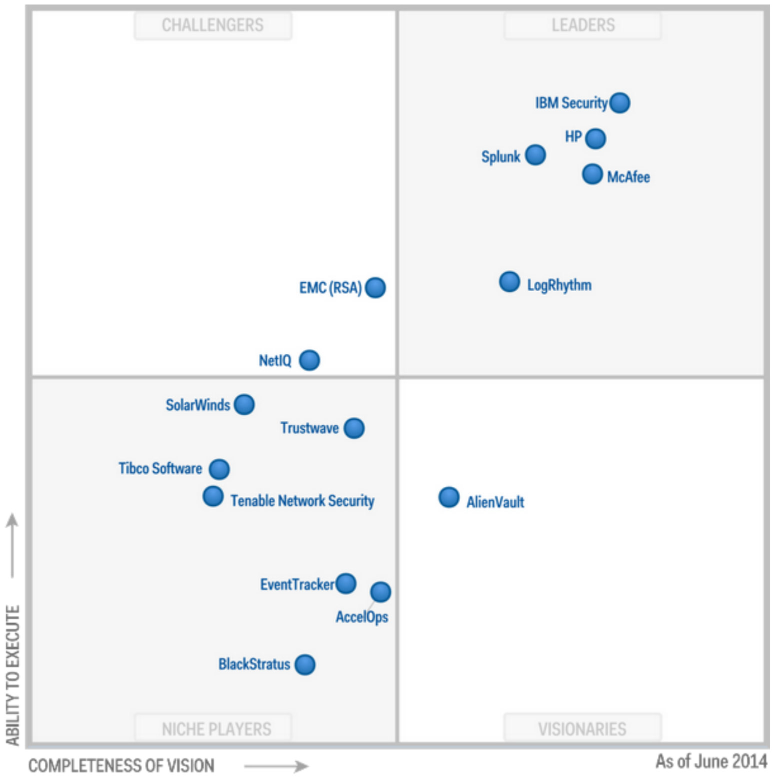


Figure 3.4.2-3 Magic Quadrant, by Gartner, for Security Information and Event Management

Leading SIEM solutions, based on Gartner’s report, are:

- HP Arcsight [SOC09]: it provides real-time monitoring, threat intelligence, behaviour profiling, and application monitoring.
- SPLUNK [SOC15]: it includes visualizations to identify anomalous behaviour, a threat intelligence framework to organize and de-duplicate threat feed data and data models and a pivot interface to enable the fast creation of analytics.
- IBM Security QRadar SIEM [SOC16]: it provides security intelligence by collecting, normalizing and correlating available network data using years' worth of contextual insights.
- McAfee [SOC18]: it brings event, threat, and risk data together to provide strong security intelligence, rapid incident response, seamless log management, and extensible compliance reporting.
- Logrythm [SOC19]: it provides rapid detection, response to and neutralization of damaging cyber threats

Some other security providers, like CISCO, also offer SIEM solutions but they are tailored for their product range. CISCO Security Manager [SOC14]: it provides consistent policy enforcement and rapid troubleshooting of security events for a wide range of Cisco security devices

3.4.2.4 Incident Response Orchestrators

In SIEM solutions, incident response capabilities are usually limited to basic reactions, such as launching a command line or sending an email after an alarm is raised. Furthermore the business and operational contexts, i.e. impacted assets, time in the day, day in the week, etc. are rarely taken into account either to raise an alarm or to launch a reaction process. It means reaction rules are statically defined, which prevents applying the right decision for a specific situation, with a combination of interdependent actions.

As a consequence this is far from satisfying when it deals with orchestrating a smart response against a complex incident. That is why, in the recent years, security incident response orchestrators appeared providing complementary solutions to fill the gap.

The purpose of a security incident response orchestrator is:

- To gather security problem notifications from various high-level systems, e.g., security information and event management systems (SIEM), vulnerability assessment systems (VAS), network management systems (NMS)
- To assess in real-time their impact on business and operational services,
- To display security status on a user interface once consolidated,
- To suggest response procedures describing needed actions to manage security issues in the objective of cancelling or reducing their effects.

Actions range from evidence collection, escalation to CSIRT teams, security policy reconfiguration and data analysis (e.g. forensics). These actions may be automatically enforced or just proposed. Getting the context in mind enables response orchestrators to trustfully trigger automated actions. Handling incident resolution means also implementing a workflow from incident notification to the incident closure. Learning capability and knowledge management are also features embedded in such tools.

The figure below shows the principles of security information process with a response orchestrator in a SOC.

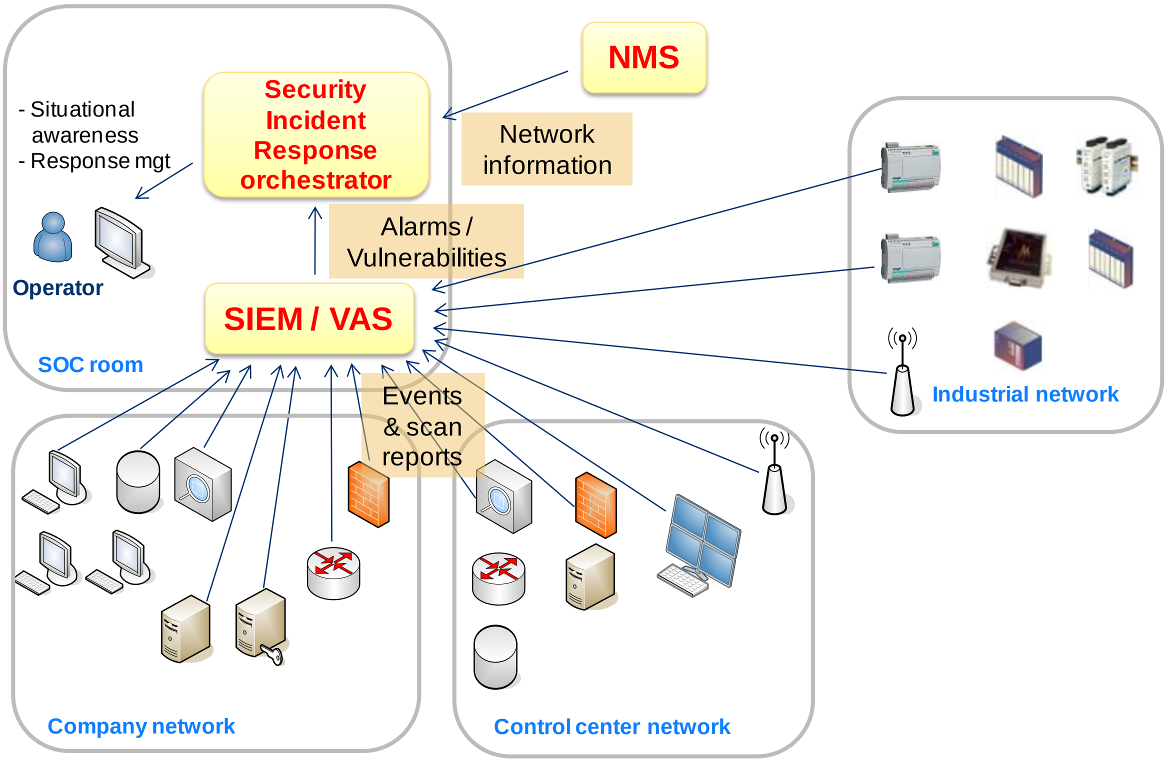


Figure 3.4.2-4 Security incident response orchestrator principles

A security incident response orchestrator is designed to interact with several types of users:

- Operators whose primary activity is network supervision,
- Decision-makers more focused on business and operational activities,
- Experts who are in between (help operators solving problems, explain decision-makers the ongoing situation).

Currently the competition is not restricted to US actors, contrary to what happens in the SIEM market. Hereunder three decision-support related solutions are described: two are American, one is European.

RSA Security Management

RSA [SOC20] is an American company specialised in security solutions owned by EMC. RSA proposes several product suites to address the whole scope of security: incident management, compliance and risk management.

To enable the capability to react to security incidents, it is mandatory to deploy different RSA products/modules. The core components are RSA Security Analytics (formerly envision), RSA Data Discovery coupled with RSA DLP (Data Protection Loss) and RSA ECAT. RSA eGRC (not shown on the picture) is the module dedicated to investigation and resolution.

RSA Security Analytics is the RSA's SIEM. It collects, aggregates, correlates event logs from different sources, and raises alarms on suspicious activities. Security Analytics is designed to handle large volumes of data in real-time. It can also provide reports.

RSA DLP suite aims at protecting personal and sensitive data. RSA offers a range of features on this product: DLP Datacenter is focused on protecting the entire storage infrastructure whereas the DLP Network monitors all network communication for sensitive data. DLP Endpoint enforces the security policy at physical and virtual machines level.

RSA ECAT is a tool dedicated to threat discovery and assessment through audits performed on machines: processes activity checking, comparison of application integrity with a reference base, kernel structure validation, and disks analysis. It follows a signature-less approach in order to be able to detect unknown threats. It is used as part of the RSA's SOC service offering and strongly integrates RSA Security Analytics. The integration model is the following: Security Analytics detects compromise signals and ECAT analyses data and confirms the compromise. If needed it conducts audits on other potentially compromised machines.

RSA eGRC is the module devoted to the compliance and risk management. It provides GRC dashboards. The role of this module is also to handle security incidents from alarms triggered by Security Analytics, and information on targeted data criticality given by ECAT. Investigation and resolution are then done through the eGRC console.

Airbus Defence& Space Cymerius

Cymerius® [SOC20] is the Airbus Defence and Space CyberSecurity's security incident response orchestrator. This solution integrates legacy security devices (IDS, SIEM, etc.) and is designed to get alarms from SIEMs or any other security alarm providers and evaluate consequences they may have on the assets to protect. The second main feature is to provide an advanced decision-support engine for response orchestration.

Situation awareness

Cymerius® is able to model elements such as networks, business and operational services and physical sites to supervise. In the context of Building Management System, it is worth noting its ability to model relationships like dependencies between those types of elements (HVAC, Energy, etc.). This is used afterwards to propagate in real-time effects of security incidents on sites, networks and operational services according to dependencies.

Cymerius® can adapt to different kinds of deployments and uses. In terms of interoperability, it can federate inputs coming from heterogeneous SIEMs, locate problem occurrences and assess their impact at any level (e.g., local area, national production).

Cymerius® can interact with incident ticket management tools (such as Remedy, EasyVista, Cerberus) in order to follow the resolution of security incidents and keep its situation views up-to-date.

Reaction plans

A response proposal against a security incident is triggered when all the conditions of a reaction context are fulfilled. These conditions deal with the alarm itself and the business and operational situation.

When an incident notification is received by Cymerius®, a reasoning engine examines the incident information, determines the operational situation, where the problem happens, which elements are impacted, etc., and searches if those conditions match one reaction context. If so, the corresponding reaction recommendations are displayed to the operator in charge of the incident. In every reaction plan, the operator gets a written step by step procedure for handling the incident.

Cymerius® is proposed by Airbus DS as a product or as part of a managed SOC service, completed with security information management, malware detection and analysis, forensics and vulnerability assessment.

NetCitadel Threat Response

NetCitadel [SOC21] Threat Response provides automated security incident response and containment capabilities. As depicted in the figure below, the NetCitadel tool relies on IDSs, SIEMs and antimalware systems to get aware of ongoing security problems. As RSA and Airbus solutions, it also gets external context information to determine the best decision regarding the incident remediation. The particularity of this tool is on the actuator support for the enforcement part of the response. It is able to update the security policy on security devices such as Cisco, Juniper, CheckPoint firewalls and web proxies.

NetCitadel stays at a technical level within the incident analysis process. In other terms, the response decision is not influenced by the consequence for the company business, which is a serious drawback for such a kind of solution. However the posture adopted by NetCitadel is to provide automated reliable changes on known situations. For instance, block network traffic towards Command & Control or drop zones as soon as malware compromise is detected and analysed by an external system such as FireEye. The idea is to minimize the SOC operator workload by eliminating repetitive actions, with no added-value, and granting the remediation gets faster. Getting trusted information on malware is done through the IOC collector and analyzer modules.

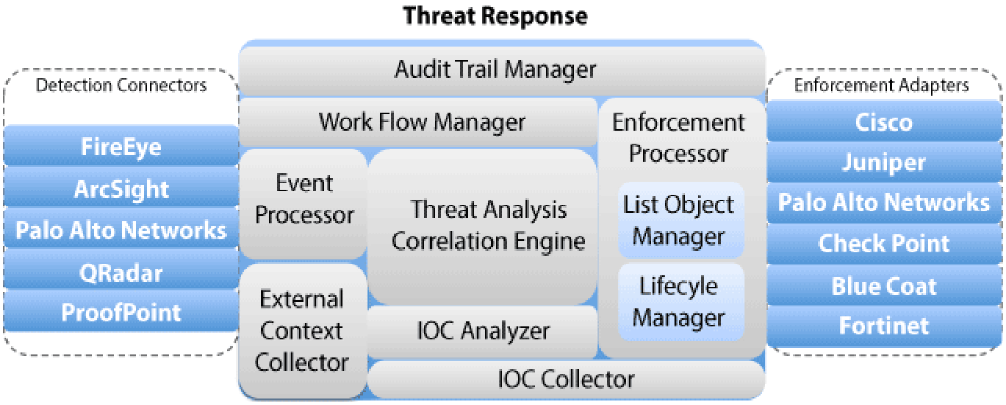


Figure 3.4.2-5 NetCitadel functional architecture

3.4.3 Attacks and threats in IoT

Internet of Thing based applications generate, process and communicate a large amount of data, raising many security and privacy concerns. Security and privacy issues in IoT system are actually an important topic and subject of many studies and surveys. We base our state of the art on very recent surveys in the domain [AII1, 2, 3, 4, 5]. An Internet of Things based system can be subject of many kinds of threats and attacks [AII1]. We can summarize them as follows.

1. **Eavesdropping**: consists in an unauthorized real-time interception of private communications. This attack aims to violate confidentiality and steal data.
2. **DoS**: it stands for a Denial of Service, and we can distinguish two kinds of DoS:
    a. **DoS1**: the threat comes from within the sensor network. It consists in disturbing the communication protocol by a continuous stream of messages causing collisions, which lead the sensors to consume their resources (power resource).
    b. **DoS2**: the threat comes from the outside of the sensor network. It consists of a storm of broadcast messages, which aims at saturating the server port.
3. **NodeCompromise**: it consists in reprogramming a legitimate node to steal secrets from the encrypted data, to launch attacks, to report misleading information to the network, etc.
4. **Sinkholeand Wormhole attacks**:
    a. **Sinkhole attack** aims to spread false routing information to make selective forwarding of packets. The malicious node can then suppress or modify packets as it wishes.

b. **Wormhole attack** consists in a replay of the same packet into the network to create confusion in routing. A malicious node forwards packets between two legitimate nodes to give them the impression that they are close to each other, leading to dissipate their valuable energy.

BMS security requirements are similar to those pointed out in the SMARTE approach [AII3]. SMARTIE approach is introduced to build a data-centric information-sharing platform in which information will be accessed through an information service layer, operating above heterogeneous network devices and data sources and provide services to diverse applications in a transparent manner. To strengthen security, privacy and trust at different IoT layers, SMARTIE approach considers the following IoT layers and their corresponding security requirements.

IoT layers	Security requirements
Applications (Intelligent Transportation, Smart Energy, Public Safety, Utilities, Service Providers, etc.)	• Authentication, Authorisation, Assurance; • Privacy Protection and Policy Management; • Secure Computation; • Application-specific Data Minimisation; • Discovery of Information Sources
Information Services (In-network Data Processing, Data aggregation, Cloud Computing, etc.)	• Cryptographic Data Storage; • Protected Data Management and Handling (Search, Aggregation, Correlation, Computation);
Network (Networking infrastructure and Network-level protocols.)	• Communication & Connectivity Security; • Secure Sensor/Cloud Interaction; • Cross-domain Data Security Handling
Smart Objects (Sensors for data collection, Actuators)	• Data Format and Structures; • Trust Anchors and Attestation; • Access Control to Nodes • Lightweight Encryption

To deal with security threats, we can consider the autonomic 4-part control loop architecture introduced in [AII6, 1]. The latter is divided into four separate parts on the basis of their functionalities:

Monitor: this module collects data from the environment (sensors, actuators, external data sources) and ensures data functionalities like aggregation, filtration, management, and reporting of all details.

Analyse: this module models complex situations based on received details. It can also be used to predict future states based on the current and the historical status of the execution process in the system.

Plan: this module provides mechanisms that guide actions with the help of higher-level policies, rules, and regulations. It plans further actions on the basis of the constraints that have been imposed in the system.

Execute: this module controls the implementation of the ”devised” plan with support of some kind of feedback.

3.5 Conclusion

In FUSE-IT project, some devices such as secured share sensors and effectors are interconnected through trusted federated energy and information networks to report data and events to the core building data processing and analysis module. In this section the related technologies are reviewed. Technologies related to smart energy sensors applied to give a feedback on consumed energy, HVAC sensors and effectors used to thermal and indoor air quality control, and physical detection and anti-intrusion sensors which secure extended areas. Also, these sensors interconnection is achieved through smart networks such as smart grids and micro-grids which are also explained in this section. Through mentioned technologies, FUSE-IT provides a site energy and automation system connected to the enterprise network and the internet which exposes the system to different kind of threats. Therefore, it still needs security management module to make the result of project marketable. This module deals with security of smart grids, SCADA, BAS ,BMS as well as security operation centers which are also discussed in this section. The last part of this section explains the solutions to monitor and control resource and electricity transmission system, building’s mechanical and electrical equipment as well as IT components applied by Fuse-IT.

4 Standards

4.1 Internet of Things

4.1.1 oneM2M

To prepare, approve, and maintain globally applicable, access-independent technical specifications and reports related to machine-to-machine communications (M2M) and Internet of Things (IoT) solutions, with initial focus on the Service Layer, oneM2M arises as a global initiative for M2M&IoT standardization with agreement of leading regional SDOs (Standards Developing Organizations) to create a global harmonization partnership.

4.1.1.1 Organization

This global partnership, oneM2M, avoids any duplication of work between SDOs involved in the same domain of M2M&IoT Service Layer with the opportunity for broad and equitable participation by all stakeholders in the M2M&IoT marketplace, including manufacturers, service providers, and end users from all industries.

Table 4-1 Seven institutional regional SDOs, so-called ‘Partners Type 1’

	Logo	Full Name	Country
ATIS	atis	Alliance for Telecommunications Industry Solutions	USA
ARIB	ARIB Association of Radio Industries and Businesses	Association of Radio Industries and Businesses	Japan
CCSA	CCSA	China Communication Standards Association	China
ETSI	ETSI World Class Standards	European Telecommunications Standards Institute	EU
TIA	TIA ADVANCING GLOBAL COMMUNICATIONS	Telecommunications Industry Association	USA
TTA	TTA	Telecommunications Technology Association	Korea
TTC	TTC Telecommunication Technology Committee	Telecommunication Technology Committee	Japan

Table 4-1 Seven institutional regional SDOs, so-called ‘Partners Type 1’shows all the SDOs in oneM2M partnerships, the most influential ones in terms of Information and Communication Technology (ICT), and the other additional partners. Totally, there are 227 members joined in the partners: ‘Partners Type 1’ and ‘Partners Types 2’.

4.1.1.2 Background and Goal

The purpose and goal of oneM2M is to develop technical specifications which address the need for a common M2M&IoT Service Layer that can be readily embedded within various hardware and software, and relied upon to connect the myriad of devices in the field with M2M&IoT application servers worldwide. For this, each WG provides its own scope and objects as follows:

WG1-Requirements: WG1 collects the requirements for specification and development of oneM2M. It is in charge of identifying and documenting use cases relevant for oneM2M. Use cases describe the interaction between actors and the system/subsystems using a sequence of steps to achieve a goal, and shall be described in an architecture neutral manner. This WG1 document contains an informative functional role model and normative technical requirements for oneM2M.

WG2-Architecture: The WG2 document describes the end-to-end oneM2M functional architecture, including the description of the functional entities and associated reference points. The oneM2M functional architecture focuses on the Service Layer aspects and takes Underlying Network-independent view of the end-to-end services. The Underlying Network is used for the transport of data and potentially for other services.

WG3-Protocols: The WG2 document specifies the communication protocol(s) for oneM2M compliant Systems, M2M Applications, and/or other M2MSystems. It also specifies the common data formats, interfaces and message sequences to support reference points(s) defined by oneM2M. Currently, they have developed the first release of oneM2M’s core protocol and binding mechanisms between itself and legacy transport protocols in application layers such as HTTP (Hypertext Transfer Protocol), CoAP (Constrained Application Protocol), and MQTT (Message Queue Telemetry Transport).

WG4-Security: The document of WG4 defines security solutions applicable within the M2M system. The Security WG performs the security analysis of the oneM2M system architecture and applies best practices to derive technical solutions, including but not limited to authentication, encryption, and integrity verification.

WG5-Management, Abstraction, and Semantics: The present document of WG5 specifies the protocol translation and mappings between the oneM2M Service layer and the management technologies.

In addition, each WG is going for approval of final oneM2M release 1 as following states:

WG1-Requirements: The initial requirement sets have been finished; new input is being received for additional M2M use cases that were not covered.

WG2-Architecture: The architecture technical specification is being prepared for final approval.

WG3-Protocols: oneM2M specific bindings between the core protocol of oneM2M and HTTP, CoAP, and MQTT protocol implementations are being developed. The first release of the protocol technical specification is being prepared for final approval.

WG4-Security: enabling flexible trust architecture well aligned to the current public and regulatory interest in user privacy and system security and resilience.

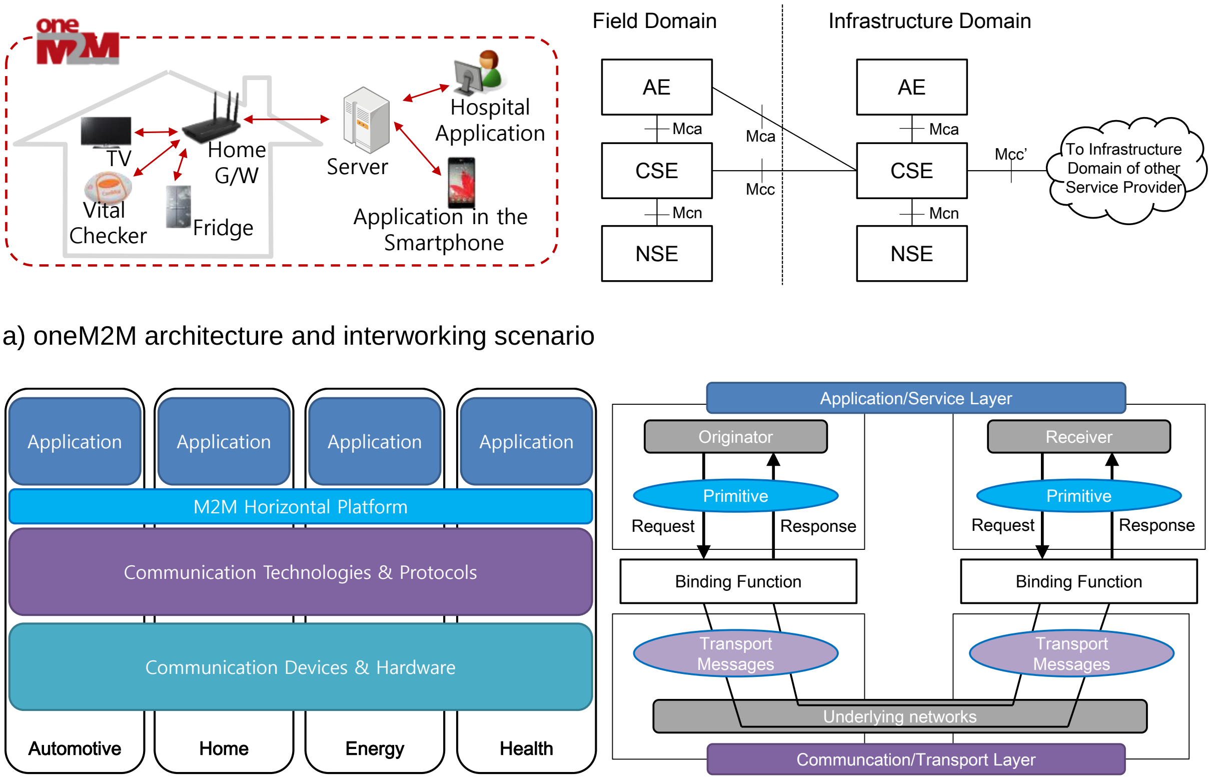
WG5-Management, Abstraction, and Semantics: working on management protocols as well as providing abstraction and semantic-based mechanisms to give support to a broad variety of IoT and M2M implementations.

4.1.1.3 Technical Characteristics

As mentioned above, the main objectives of the oneM2M partnership can be summarized as follows: 1) to develop globally agreed-upon M2M end-to-end specifications, 2) to define/focus on the service layer and to provide a detailed service architecture including protocols, APIs, standard objects, 3) common use cases, terminal/module aspects, and 4) security and privacy aspects.

It means that oneM2M develops end-to-end communication between M2M&IoT devices in wide area networks (WANs) as legacy networking in the Internet and its operation shall be carried out with transparency against legacy transport protocols in application layers such as HTTP, CoAP, and MQTT. Moreover, this operation follows the efficient method as Web communication, called RESTful.

Figure 4.1.1-1 illustrates system architecture and the position of oneM2M protocols in M2M&IoT service platform with its detailed operation idea in the oneM2M layer.



a) oneM2M architecture and interworking scenario

b) oneM2M layer

Figure 4.1.1-1 oneM2M architecture and landscape of M2M&IoT service platform

4.1.2 IETF Working Groups on IoT

Standardization activities on IoT related protocols and practices are bundled in working groups at the Internet Engineering Task Force (IETF). Prior to starting a working group a clear mandate is agreed upon by those aiming to participate to the group. This mandate is written down in the charter of the working group. Each working group operates in one of the following eight areas:

- Applications area
- General area
- Internet area
- Operations and Management area
- Real-time Applications and Infrastructure area
- Routing area
- Security area
- Transport area

So far, IoT standardization at the IETF has focused on the Internet, routing, apps and security areas. Each of these efforts is concentrated in one or more working group belonging to one of these areas. Which working groups and standardization work at the IETF are relevant for the IoT be discussed in the following subsections. The list starts with the three relevant working groups active from the Internet area.

4.1.2.1 The IPv6 over Low power WPAN working group (6LoWPAN)

The IPv6 protocol has a high overhead and restrictions that make it unsuitable for Low Power Networks (LLNs) such as IEEE 802.15.4 networks. For instance, considering the limited space available for the MAC payload in an 802.15.4 MPDU, the use of a 40-byte IPv6 header would be too excessive. Therefore, the IETF 6LoWPAN Working Group was formed to work on the IPv6 protocol extensions required for such networks where hosts are interconnected by IEEE 802.15.4 radios. Meanwhile the working group has completed its work and produced several proposed standards and informational documents regarding these required extensions.

Starting from a well-defined set of assumptions and a problem statement, as defined in the informational RFC 4919, a solution for transmitting IPv6 packets over IEEE 802.15.4 networks was defined, resulting in RFC 4944: Transmission of IPv6 Packets over IEEE 802.15.4 Networks. As a result, IEEE 802.15.4 network are able to deploy IPv6 thus allowing potentially billions of nodes to be addressed and to be interconnected to the Internet.

Two subsequent RFCs of the 6LoWPAN working group, Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks (RFC 6282) and Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs) (RFC 6775) respectively cover more advanced header compression and Neighbor Discovery optimization in 6LoWPANs and have updated RFC 4944. In addition, the working group has produced 2 other informational RFCs that address use case descriptions (RFC 6568) and routing requirements (RFC 6606) for 6LoWPANs. The group had also adopted an Internet draft on the transmission of IPv6 packets over Bluetooth (draft-ietf-6lowpan-btle). However, as the working group has come to an end this work has been moved to the 6lo working group.

Finally, the working group was also expected to collaborate with other organizations (such as IEEE and ISA SP100) and other IETF working groups (such as ROLL) on common interest issues and was mandated with providing implementation and interoperability guidelines to developers. Again, these tasks are now the responsibility of the 6lo WG while the lwig WG aims to provide additional guidelines.

4.1.2.2 IPv6 over Networks of Resource-constrained Nodes working group (6lo)

Where the 6LoWPAN WG brought IPv6 to one specific type of LLNs (IEEE 802.15.4 networks), the 6lo WG aims to connect devices running a number of different link layer technologies to the Internet. The results of these efforts will be a number of IPv6-over-foo adaptation layer specifications similar to RFC 4944. So far the working group has adopted four Internet drafts that define the necessary adaptations for IPv6 over Bluetooth Low Energy (draft-ietf-6lo-btle), DECT Ultra Low Energy (draft-ietf-6lo-dectule), MS/TP networks (draft-ietf-6lo-6lobac) and G.9969 networks (draft-ietf-6lo-lowpanz). The latter has already been finalized and has been submitted to the IESG for publication.

Furthermore, the 6lo working group has already published two proposed standards. RFC 7388 defines a portion of the Management Information Base (MIB) for use in LLNs with network management protocols. More specifically, the proposed standard defines a number of objects (called the LOWPAN-MIB) for managing IPv6 over 6LoWPANS that provide monitoring and troubleshooting support for the 6LoWPAN layer. RFC 7400 provides a generic method for header compression that can be applied to any header-like payload, without a need to define a new header compression scheme for every new header or header-like payload.

4.1.2.3 IPv6 over the TSCH mode of IEEE 802.15.4e working group (6tisch)

6tisch is another Internet area working aiming to bring IPv6 to a specific link layer technology, IEEE 802.15.4e in this case. The IEEE802.15.4e Timeslotted Channel Hopping (TSCH) is a recent amendment to the Medium Access Control (MAC) portion of the IEEE802.15.4 standard. As a result the 802.15.4e timeslotted channel hopping MAC differs fundamentally from the CSMA MAC found in standard 802.15.4. In short, TCSH allows for more controlled and deterministic network access as opposed to CSMA, while also offering increased resiliency to interference via channel hopping. As a result, TSCH MAC protocols are commonly used in industrial applications (e.g. Wireless HART and ISA100.11a are two popular technologies).

As 802.15.4e only defines the link-layer mechanisms, 6tisch aims to produce an IPv6 architecture on top of 802.15.4e. The resulting architecture should allow to decimate a distributed routing scheme to a 6tisch network. This scheme assigns the timeslots and frequencies to be used during channel hopping to nodes in the 6tisch network. To this end the WG will also define the necessary interfaces to configures 6tisch nodes to process this scheme. Finally the working group will provide a minimal 6tisch configuration, that defines how to build (i.e. provision) a 6TiSCH network employing the Routing Protocol for LLNs (RPL) and a static TSCH schedule.

4.1.2.4 Routing Over Low power and Lossy networks working group (roll)

Due to the distinctive characteristics of LLNs (e.g. low energy availability, throughput, reliability, availability, processing capabilities, …), LLNs have specific routing requirements that differ from those found in traditional IP networks. The ROLL working group focuses on building routing solutions for LLNs because evaluation of existing routing protocols like OSPF, IS-IS, AODV, and OLSR indicate that they do not satisfy all of the specific routing requirements. More specifically, the working group focuses on industrial (RFC 5673), connected home (RFC 5826), building (RFC 5867) and urban sensor networks (RFC 5548). For each of these domains different routing requirements were specified in the respective RFCs.

The working group focuses on an IPv6 routing architectural framework while also taking into account high reliability in presence of time varying loss characteristics and connectivity with low-power operated devices with limited memory and CPU in large scale networks. The main realization of this working group is the design of the IPv6 route-over Routing Protocol for LLNs, also called RPL, which covers the routing requirements of all these application domains.

With the specification of RFC 6550 “RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks”, the IETF has specified a proactive “route-over” architecture where routing and forwarding is implemented at the network layer, according to the IP architecture. The protocol provides a mechanism whereby multipoint-to-point, point-to-multipoint and point-to-point traffic are supported. Although RPL was specified according to the routing requirements for LLNs, its use is not limited to these applications. RPL routes are optimized for traffic to or from a root that acts as a sink/root for the topology. The roll WG has defined a number of different routing metrics for path calculation in LLNs in

RFC 6551. The variety of these metrics gives RPL the necessary versatility so that it can be deployed in the application domains mentioned above.

4.1.2.5 Constrained RESTful Environments working group (CoRE)

The CoRE working group was founded to work on the standardization of a framework for resource-oriented applications, allowing realization of RESTful embedded web services in a similar way as traditional web services, but suitable for the most constrained nodes and networks. The biggest achievement of the WG thus far is the Constrained Application Protocol (CoAP), a specialized RESTful web transfer protocol for use with constrained networks and nodes.

The CoAP protocol specification was published in June 2014 as RFC 7252. CoAP uses the same RESTful principles as HTTP, but it is much lighter so that it can be run on constrained devices. To achieve this, CoAP has a much lower header overhead and parsing complexity than HTTP. It uses a 4-bytes base binary header that may be followed by compact binary options and payload.

The CoAP interaction model is similar to the client/server model of HTTP. A client can send a CoAP request, requesting an action specified by a method code (GET, PUT, POST or DELETE) on a resource (identified by a URI) on a server. The CoAP server processes the request and sends back a response containing a response code and payload. Unlike HTTP, CoAP deals with these interchanges asynchronously over a datagram-oriented transport such as UDP and thus it also supports multicast CoAP requests. This allows CoAP to be used for point-to-multipoint interactions which are commonly required in automation. Optional reliability is supported within CoAP itself by using a simple stop-and-wait reliability mechanism upon request. Secure communication is also supported through the optional use of Datagram Transport Layer Security (DTLS).

Apart from CoAP, the working group has also published two other RFCs. RFC 6690 standardizes a web link format suitable for constrained devices, known as the CoRE link format. RFC 7390 is an experimental RFC (i.e. it is unclear whether the proposal will work as intended) that defines how CoAP should be used in a group communication context. More specifically RFC 7390 details an approach for employing CoAP on top of IP multicast.

The working group has adopted a number of various other drafts as working group documents. Topics include a notification extension (known as CoAP observe), transfer of large resources over multiple request/response messages (known as block transfer), guidelines for implementing mappings between HTTP and CoAP, a directory service that indexes CoAP servers and their resources (a so-called resource directory), guidelines on designing the interfaces offered by RESTful CoAP applications and finally a mapping from the CoRE link format to JSON.

4.1.2.6 DTLS In Constrained Environments working group (DICE)

The DICE WG focuses on supporting the use of DTLS transport-layer security in constrained environments. DTLS is the UDP adaptation of TLS (hence the name Datagram TLS) that provides end-to-end security between two applications. CoAP has defined a new URI scheme to be used inconjuction with DTLS (coaps), which is analogous to the use of TLS to secure http (https). The scope of working group includes both constrained devices and constrained networks.

The first task of DICE is to define a profile for DTLS that is suitable for Internet of Things applications and that is reasonable to implement on large variety of constrained devices. To this end, the WG has adopted a draft (draft-ietf-dice-profile) that discusses the use of pre-shared keys (PSKs), raw public keys and certificates as well other practical issues that might arise when using DTLS.

A second key issue that DICE will aim to solve is that of multicast security. The group will look at how the DTLS record can be used to transmit message securely. Key management and multi-cast session setup (where the group has to agree upon a shared session key) are explicitly stated to be out of scope.

Finally, the working group will investigate practical issues resolving around the DTLS handshake (which is used to setup a secure session) in constrained environments. Proposed work includes compressing the DTLS handshake and using alternative TLS transport for completing the handshake (such as CoAP, which might be able to provide the necessary reliability).

4.1.2.7 Light-Weight Implementation Guidance working group (lwig)

The final working group discussed here is one that does not produce proposed standards. Instead lwig is chartered to produce informational standards with the goal to aid developers that are active in the constrained space. This is necessary because developers that are familiar with Internet technology, are not necessarily familiar with the world of embedded systems.

One result is that lwig has agreed upon a common terminology to be used across all of the IoT working groups (as mentioned above) while discussing the constrained space (RFC 7228). One adopted Internet draft provides implementation guidance for implementing the CoAP protocol on constrained devices. Here a number of protocol implementation choices are discussed, together with a number of implementation optimizations. Two other adopted drafts look at how protocols within the IETF scope can be made to behave energy friendly (draft-ietf-lwig-energy-efficient) and how CoAP can be employed on cellular devices (draft-ietf-lwig-cellular).

4.1.2.8 Overview of the IETF IoT stack

Figure 4.1.2-1 gives a layered overview of the IoT protocol stack as envisioned by the IETF today. Applications and devices are interconnected via the IPv6 Internet with its inconceivably large address space. IPv6 Internet is foreseen to be available on a wide variety of different link layer technologies, each of which are tailored to meet the specifics demands of their domain: wired vs wireless, short vs long range, line of sight vs non LoS, high vs low data throughput, narrowband vs wide band, etc.

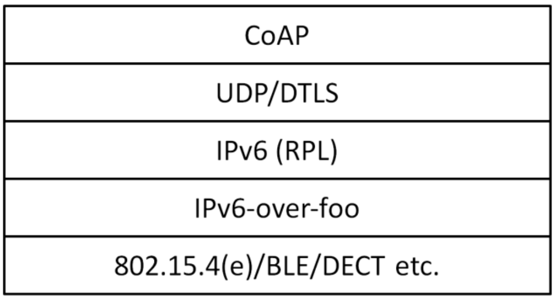


Figure 4.1.2-1 IoT protocol stacks

Within the constrained parts of the network, the RPL routing protocol is used as a uniform and efficient method for realizing multihop networks. On top of the IPv6 Internet, constrained IoT devices are able to reap the benefits of a lightweight RESTful application protocol with a robust and proven protocol for end-to-end security where necessary. The large IPv6 address space also means that IoT devices and their services can be integrated into applications directly.

Figure 4.1.2-2, referenced from [IETF], gives an overview of a typical deployment of the stack in a multihop low power and lossy network. Using IPv6 and CoAP Internet hosts can communicate directly to the constrained devices and their RESTful resources. At the same time the gateway offers a number of services to translate between protocols that are popular on the traditional Internet (e.g. HTTP/TLS) and those that are commonly found in the constrained network (e.g. DTLS/CoAP). This gateway can also function as a proxy where it might offer additional application services such as caching of responses, enforcing access control and mitigating other inoperabilites between an IoT device/application and an Internet device/application.

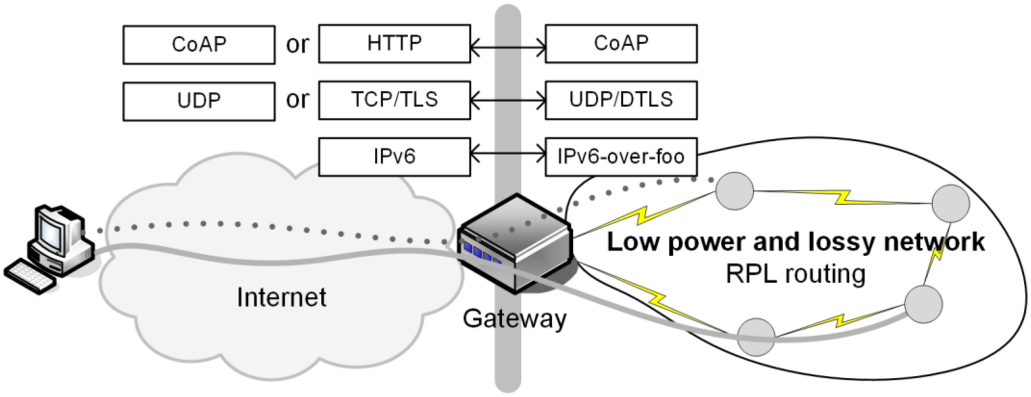


Figure 4.1.2-2 Deployment of networking stacks in a multihop low power and lossy network

4.1.3 Internet of Things Alliances

This chapter presents commercial partnerships operated by firms, dealing with Internet of Things.

4.1.3.1 IPSO Alliance (founded 2008)

Goals: The IPSO Alliance is an organization promoting the Internet Protocol (IP) for "smart object" communications i.e. IoT & M2M

Initiatives: To serve as a thought leader across the board for communities seeking to establish the Internet Protocol (IP) as the network for the connection of Smart Objects. Moving forward from explaining “Why use IP”, to “How to use IP”. Educate and inform on the numerous fundamental benefits of IP. Embark on defining the set of appropriate protocols, architecture and data definitions for Smart Objects so that engineers and product builders will have access to the necessary tools for “how to build the IoT RIGHT”

“Starter Pack 1.0 Abstract » is downloadable. It provides a basis for interoperability across devices connected to the IoT through an open common object model

Board members: Geoff Mulligan: Presented himself as an innovator, inventor notably of 6LoWPAN & IpV6. Not associated to a firm: Oracle, Micrium, Grid Connect, Ericsson, Bosch, Eaton.

4.1.3.2 AllSeen Alliance (founded 2013)

Goals: The AllSeen Alliance is aimed at collaborating and contributing to the AllJoyn open source project.

Initiatives: Act as a portal for downloading and inform about AllJoyn framework. Launch a comprehensive certification and compliance program with third-party test labs to ensure smart products in the ecosystem are truly interoperable

Board members: Affinegy, Silicon Image, Lg, Qualcomm, Haier, Icontrol, Electrolux, Weaved, Panasonic, Sony, Sharp, Microsoft

4.1.3.3 Open Interconnect Consortium (founded 2014)

Goals: Define a comprehensive communications framework to enable emerging applications in all key vertical markets. Security and open source considerations

Initiatives: OIC promotes interoperability between Internet of Things (IoT) devices. Relay some articles about IoT. Define specification, certification & branding to deliver interoperability.

Board members: Samsung, Intel, Mediatek, Cisco.

(complete list: http://www.openinterconnect.org/about/members/).

Proposed Framework: The IoTivity is an open source project is sponsored by the OIC and was created to bring together the open source community to accelerate the development of the framework and services required to connect these billions of devices.

4.1.3.4 Thread Group (founded 2014)

Goals: Find/Define a network protocol for IoT using IPv6/6LoWPAN and broadcast on some existent media: 802.15.4. Try to set up a Certification Program.

Initiatives: Home-focused i.e.: End-user oriented. Thread is designed for various household products that facilitate: Access control, Climate control, Energy management, Lighting, Safety, Security, Thread Group intends to provide rigorous testing, certification, and enforcement.

Board members: Nest labs, Silicon Labs, Frescale, ARM, Yale Security.

4.1.3.5 IEEE WG P2413 - Standard for an Architectural Framework for the IoT

Goals: Foster technological innovation and excellence for the benefit of humanity. IEEE covers a wide kind of subjects. A sub-domain URL is dedicated to IoT : iot.ieee.org.

Initiatives: IEEE proposes standards and publications. “Internet of things journal” gathers publications which are accessible through a search engine. Most consultations of these articles are charged. IEEE prepares a standard for IoT architecture. A working group is currently on creation : IEEE P2413.

Board members: 33 directors with no mention of firm affiliations.

Scope: This Working Group defines a standard focusing on 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.

The Project is sponsored by the IEEE-SA Board of Governors/Corporate Advisory Group (BOG/CAG).

4.1.3.6 Intel IoT Solution Alliance

Goals: Promote IoT hardware equipped with Intel components.

Initiatives: Members of the alliance provide the hardware, software, firmware, tools, and systems integration that developers need.

Board members: Integrated part of Intel

4.1.3.7 Industrial Internet Consortium (founded 2014)

Goals: Utilize existing and create new industry use cases and test beds for real-world applications;

Deliver best practices, reference architectures, case studies, and standards requirements to ease deployment of connected technologies;

Initiatives: Help member companies to involve into testsbeds. A testbed is a controlled experimentation platform, conforming to an IIC reference architecture, where solutions can be deployed and tested in an environment that resembles real -world conditions. Testbeds explore untested technologies or existing technologies working together in an untested manner. Testbeds generate requirements and priorities for standards organizations, and culminate in new (potentially disruptive) products and services.

Board members: The IIC is a non-profit consortium managed by the Object Management Group, another non-profit group dedicated to computer industry standards

4.1.3.8 Homeplug Alliance (founded 2014)

HomePlug Alliance develops technology specifications and certification programs for powerline networking at home.

4.1.3.9 OneM2M (founded 2012)

oneM2M aims to develop technical specifications which address the need for a common M2M (IoT) Service Layer that can be readily embedded within various hardware and software. Founded by leading ICT standards : ETSI, ARIB, TTC, ATIS, TIA, CCSA and TTA. 200+ adherents.

4.1.3.10 4.5.3. AllJoyn (2011)

AllJoyn is an Open Source software framework allowing communication for IoT. Software Development Kit are now available on iOS (Apple), Android (Google), Windows seven and Linux. This product has passed the experimental step and is now stable.

4.1.3.11 UK/s Hypercat (2014)

There are 40+ Adherents (most UK’s) including BT, ARM, BAE and Rolls Royce. UK’s Hypercat is an Open Source catalogue exposing information (interface) about IoT assets over the Web. It allows a server to provide a set of resources to a client, each with a set of semantic annotations. JSON textual descriptions are used. The project is still experimental

4.1.3.12 Google Physical Web (2014)

Google Physical Web consists in an Open Source application onboard on smartphones, allowing single interaction between Smart Devices and people via their mobiles devices. Such kind of Smart Devices should broadcast URLs on area where display devices (i.e. smartphones) can catch them. First targets aims are Android (Google) and iOS (Apple).

Technically, the current design uses Bluetooth Low Energy (aka Bluetooth Smart) devices for broadcasting the URL via the advertising packet. Once the client connected, the server send a JSON data structure listing all meta-information available. The project is still experimental: No security consideration for the moment, since URLs are displayed as plain text. Another current issue is that URL should point to a HTTP page. Such kind of IoT service may not rely on a single HTTP page.

4.1.3.13 Alliance of Internet of Things for Innovation – A European initiative

The new Alliance Internet of Things for Innovation (AIOTI) was launched in April 2015. The European Commission is, currently, supporting the development (in Europe) of the most dynamic and agile IoT ecosystem and industry in the world, which could really transform people's lives, drive growth, create employment and address societal challenges. According to estimates, nearly five billion things will be connected by 2015, reaching 25 billion by 2020, helping users save energy, reduce traffic jams, increase comfort, and get better healthcare and increased independence. IoT will not only allow companies to change their traditional business models through new services, but will also help combine the benefits of selling products with value-added digital service.

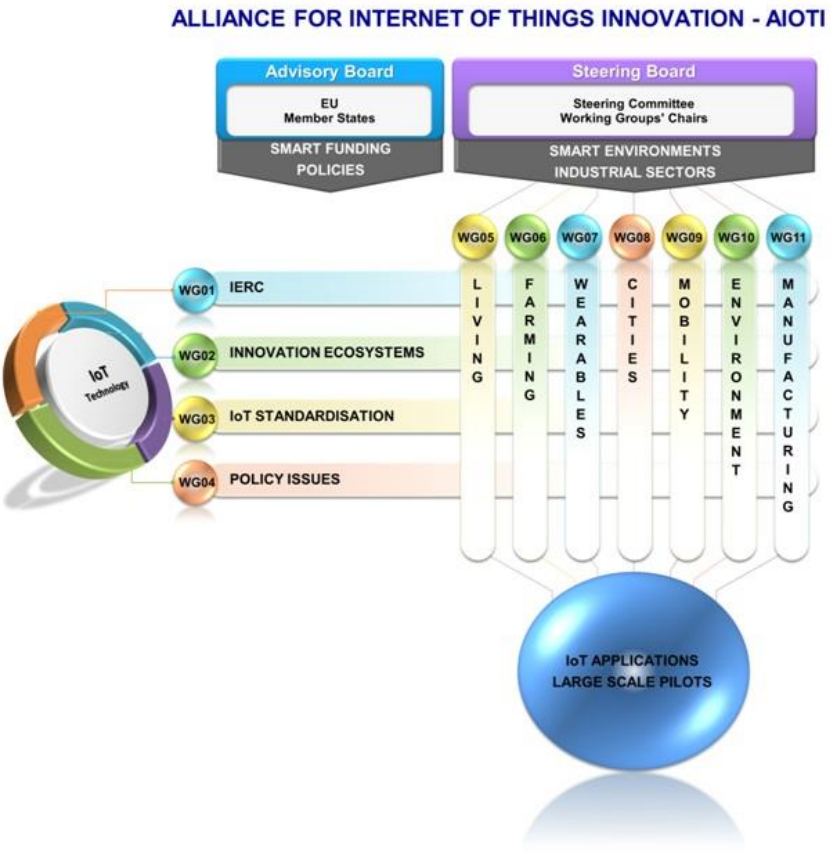


Figure 4.1.3-1 AIOTI Scope

IoT will be a major focus for European Commission during 2016-2017 with revenue is estimated to represent €400 million in 2015 and is expected to increase to more than one trillion euro in 2020.

The newly created Alliance for Internet of Things Innovation brings together:

- Different industries: nanoelectronics/semiconductor companies, Telecom companies, Network operators, Platform Providers (IoT/Cloud), Security, Service providers
- Different sectors: energy, utilities, automotive, mobility, lighting, buildings, manufacturing, healthcare, supply chains, cities, etc.

AIOTI has already involved some of Europe's largest tech and digital companies in this initiative: Alcatel, Bosch, Cisco, Hildebrand, IBM, Intel, Landis+Gyr, Nokia, ON Semiconductor, Orange, OSRAM, Philips, Samsung, Schneider Electric, Siemens, NXP Semiconductors, STMicroelectronics, Telecom Italia, Telefonica, Telit, Thales, Vodafone, Volvo, and start-ups such as SIGFOX

AIOTI is organized as a lean structure with two layers: the Board (Steering Committee) and the Working Groups (WGs). The chairs of the WGs will be the members of the Board, thus any AIOTI member that would like to be part of the Board must also chair a WG. AIOTI members may propose different representatives for the role within the Board and the respective working group.

The eleven WGs are structured as below, corresponding to current prominent areas of the IoT:

- WG 1: IoT European Research Cluster
- WG 2: Innovation Ecosystems
- WG 3: IoT Standardisation
- WG 4: Policy issues (trust, security, liability, privacy)
- WG 5: Smart living environments for ageing well (e.g. smart house)
- WG 6: Smart farming and food security
- WG 7: Wearables
- WG 8: Smart cities
- WG 9: Smart mobility (smart transport/smart vehicles/connected cars)
- WG 10: Smart environment (smart water management)
- WG 11: Smart manufacturing

The current priority for the EC is to extend AIOTI memberships, not only to involve major IoT players, but also innovative SMEs, startups, or any entity that has a legitimate interest in joining this Alliance. The European Commission launched a call for expression of interest to join the Alliance for Internet of Things Innovation.

Europe’s goal is to be able to compete with USA or Japan, and make experimentation at a larger scale than today. The Commission published recently a €51 million call for IoT projects: The initiative cuts across several technological areas such as smart systems integration, cyber-physical systems, smart networks, and Big Data; and targets SME and IoT innovators to create an open IoT environment.

4.2 Building Automation and Energy

4.2.1 Building Automation Standards

BACS standards: Since Smart Building System is one of the domains which Fuse-IT deals with, this section gives a short introduction into two standards of building automation and control systems namely DIN EN ISO 16484 and VDI 3814.

ISO 16484: ISO 16484 [EMT8] consists of the following parts, under the general title Building automation and control systems (BACS):

- Part1: Overview and vocabulary
- Part2: Hardware
- Part3: Functions
- Part4: Applications

- Part5: Data communication protocol
- Part6: Data communication conformance
- Part7: Project implementation

This series of standards is intended for designing of new buildings and retrofit of existing buildings for an acceptable indoor environment, practical energy conservation and efficiency. The application of this series of standards for BACS is envisaged as follows.

The environmental design for all building types requires complex methods for automation and control. The functional integration of services other than HVAC e.g. lighting and electric power distribution control, security control, transportation, maintenance management or facilities management is a general task for all parties employed to develop an integrated multi-application system. This integration allows the user to take advantage of synergies between the different applications. This standard will give guidance to architects, consultants and contractors as well as to users on how to share such resources,

The innovation cycles between devices, systems and networks vary. To make it possible to add and to change existing devices, and extend the building automation and control network, several interfaces both proprietary and standardized are defined between the BACS network and the other systems. A manufacturer can design a product, both to meet his specific marketing objectives and to give the option to integrate that special device into a multi-application BACS. Interfaces are also defined in appropriate parts of this standard along with the necessary communications protocol and conformance test required to support the inter-working of devices,

A manufacturer, a systems house, or an electrical or mechanical contractor can assemble an implementation of a building automation and control system. The application of this standard is not to standardize the hardware and software design or the architecture of a System, but to define the process for the creation of project specifications, where functionality and the quality of the solution are clearly defined.

BACnet Standard for Building Automation Systems (BAS) ISO 16484 -5: BACnet is a communications protocol for building automation and control networks. It is an ASHRAE, ANSI, and ISO standard protocol. BACnet was designed to allow communication of building automation and control systems for applications such as heating, ventilating, and air -conditioning control, lighting control, access control, and fire detection systems and their associated equipment. The BACnet protocol provides mechanisms for computerized building automation devices to exchange information, regardless of the particular building service they perform. Proper communication between building automation devices is critical for maximizing building energy efficiency, indoor air quality, and other aspects of "green" buildings. BACnet became ASHRAE/ANSI Standard 135 in 1995, and ISO 16484-5 in 2003. The Method of Test for Conformance to BACnet was published in 2003 as BSR/ASHRAE Standard 135.1. BACnet is under continuous maintenance by the ASHRAE Standing Standard Project Committee. ISO 16484 defines a general conceptual framework of BAS. There is a need for standards enabling open systems in the sense of systems “which can be repaired, modified, and extended by everybody with the necessary basic qualification without having to rely on the original manufacturer”. Consequently, corresponding standards were developed, like KNX, and LONworks, and have already achieved considerable significance in the world-wide market. They, however, concentrate on field communication issues, while the integral automation and management functions still rely on proprietary solutions. Additionally, standards for specific functional domains are currently being developed, e.g. the IEC standard DALI (Digital Addressable Lighting Interface). In front of that background, newest trends in BAS raise an urgent need for enhanced inter -working between different functional domains. This would enable open, flexible and integral high-level automation functions and overcome the limitations of the current heavyweight gateway architectures. Moreover, new trends in data communication for distributed building automation arise from the adoption of new IP-based device communication technology (IPv6, 6LoWPAN), of wireless communication (Wifi, IEEE 802.15.4, ZigBee, 6LowPAN), of new emerging communication systems (e.g. digitalStrom), and from the development of BAS-oriented application layer communication protocols (e.g. Web Services, BACnet/WS, oBIX, CoAP, Sensor Observation Service).

VDI 3814: The VDI 3814 [VDI3811] in the actual version was created after publication of the DIN EN ISO 16484. As the international standard does not contain regional requirements, e.g. for Central Europe, they are covered within this VDI standard. The VDI 3814 is subdivided into several parts:

- Part1: System basics
- Part2: Legislation, technical rules
- Part3: Advice for operators
- Part4: Points lists and functions - Examples
- Part5: Intersystem communication
- Part6: Representation of logic interlocks
- Part7: User interface design

The series of guidelines VDI 3814 applies to systems, software and services for automatic control, monitoring, optimization, and operation and to the management needed for an energy-efficient and safe operation of Total Building Solution (TBS). Building automation and controls (BAC) is a prerequisite for a comprehensive building management. Since the international standard ISO 16484 does not account for all regional requirements, the guideline VDI 3814 undertakes to lay down those typical middle-European requirements placed on BAC systems that go beyond those stated in the said standard. On the basis of an operator concept, this guideline can be used throughout the entire planning process. A user interface complying with this guideline's instructions is also the prerequisite for the proper operation of a building service plant.

IEC – International Electro-technical Commission (CENELEC): "The IEC TC57 develops and maintains International Standards for power systems control equipment and systems including EMS (Energy Management Systems), SCADA (Super visory Control And Data Acquisition), distribution automation, teleprotection, and associated information exchange for real-time and non-real-time information, used in the planning, operation and maintenance of power systems." CENELEC is the European counterpart of IEC. It proposes International Standards to IEC TC57, and develops and maintains European Standard in the electro-technical domain. The IEC61850: is a standard for the design of electrical substation automation. The abstract data models defined in IEC 61850 can be mapped to a number of protocols. Current mappings in the standard are to MMS (Manufacturing Message Specification), GOOSE, SMV (Sampled Measured Values), and soon to Web Services. These protocols can run over TCP/IP networks or substati on LANs using high speed switched Ethernet to obtain the necessary response times below four milliseconds for protective relaying. The objectives set for the standard were to: 1/ have a single protocol for complete substation considering modeling of different data required for substation, 2/ define basic services required to transfer data so that the entire mapping to communication protocol can be made future proof, 3/ promote high interoperability between systems from different vendors, 4/ set up a common method/format for storing complete data, 5/ define complete testing required for the equipment which conform to the standard.

DNP Users Group– Distributed Network Protocol Users group: The DNP3 Users Group is a forum for users and implementers of the DNP3 protocol, which is a set of communications protocols used between components in process automation systems. Its main use is in utilities such as electric and water companies. Usage in other industries is not common. It was developed for communications between various types of data acquisition and control equipment. It plays a crucial role in SCADA systems, where it is used by SCADA Master Stations (aka Control Centers), Remote Terminal Units

(RTUs), and Intelligent Electronic Devices (IEDs). It is primarily used for communications between a master station and RTUs or IEDs. ICCP, the Inter -Control Center Communications Protocol (a part of IEC 60870-6), is used for inter-master station communications. Although the protocol was designed to be very reliable, it was not designed to be secure from attacks by hackers and other malevolent forces that could potentially wish to disrupt control systems to disable critical infrastructure. Because smart grid applications generally assume access by third parties to the same physical networks and underlying IP infrastructure of the grid, much work has been done to add Secure Authentication features to the DNP3 protocol. The DNP3 protocol is now compliant with IEC 62351-5. Some vendors implement elliptic curve cryptography which the US NSA considers sufficient to protect information as "top secret" with only 384 bits, an order of magnitude less than those recommended for RSA.

The DNP3 protocol is also referenced in IEEE Std. IEEE 1379-2000, which recommends a set of best practices for implementing modern SCADA Master-RTU/IED communication links. These include not just encryption but other practices that enhance security against well -known intrusion methods

BIM Standards – Building Information Modeling (ISO/PAS 16739): Building information modeling (BIM) is a process involving the generation and management of digital representations of physical and functional characteristics of a facility. The resulting building information models become shared knowledge resources to support decision-making about a facility from earliest conceptual stages, through design and construction, through its operational life and eventual demolition. BIM is supported by organizations specialized in the field of construction. A construction project always involves many actors among which lot of redundant information are exchanged and multiple data transfers are done (designs that are reviewed and modified, details, quanti ties...). The digital data sharing provides an increase in efficiency and improves the quality of the exchanges during the construction process. This sharing is the heart of the process of BIM and it must ensure that the same data should not be entered repeatedly. This process is also called "model -based product design". Most software vendors have implemented proprietary methods to share data models with their third-party providers. The OpenBIM initiative, regrouping the major BIM software vendors (e.g. Autodesk, Bentley, Nemetscheck, …) lead to the new ISO standard ISO/PAS 16739. This approach although started several years ago is not adopted yet by the actors of the command-control systems. Also, current digital models don't include Access Control Lists (ACL). This limitation prevents them from being fully integrated in the business process, as security and validation is not yet taken into account for BIM interoperability. The existing ISO 29481-1:2010 standard (“Building information modeling -- Information delivery manual -- Part 1: Methodology and format”) will be extended to embrace the security needs addressed by Fuse-IT.

AGA 12 Task Group: The American Gas Association (AGA), founded in 1918, is an American trade organization representing natural gas supply companies and others with an interest in the manufacturing of gas appliances as well as the production of gas. About 92% of the 70 million natural gas customers in the US receive their gas from AGA members. Following the September 11, 2001 terrorist attack on U.S. soil the AGA Gas Control Committee (GCC) and Automation & Telecommunication (A&T) Committee agreed to support the development of an AGA report that would demonstrate how encryption may be applied to protect gas SCADA communication systems from cyber attacks. The AGA 12 Task Group was mandated to offer initially a short-term retrofit solution for existing systems and later a long-term solution applicable to new systems and internet-based SCADA communications. Shortly after AGA 12 Task Group began its work on developing a report to protect gas SCADA, the group expanded its scope to include water and electric SCADA systems. One of the things AGA 12 stresses is that the use of cryptographic protection is effective only if it is deployed as a component of a comprehensive set of cyber security policies combined with adequate attention to the physical security of the utility's infrastructure. Encryption of Internet communications is relatively uncomplicated in that one size fits all. SCADA communications, however, are another matter. The Internet uses communication protocols that are very well defined and are not timing based. Offthe-shelf encryption solutions have been available for some time for the Internet, but a security solution that actually suits utility SCADA systems is a much more difficult proposition. First, different utilities use different SCADA protocols. Second, many of the SCADA communication protocols are timing based, and the gas control systems for which they are designed are time-critical. As a result, the task group wanted to provide a cryptographic solution that minimizes the time delay caused by encryption and also works with the majority of the SCADA protocols in use. AGA 12 report is radically different from the prescriptive checklist approach to cyber security usually seen. Instead, the task group decided to give utili ties a business-oriented framework and show them how to do a risk assessment on the vulnerability of their SCADA systems to cyber attack. The intention is to help utility managers evaluate the risks and to offer an appropriate way to protect their SCADA communications. Part 1 discusses SCADA system vulnerabilities that could be exploited, offers steps to define cyber security goals, recommends activities to determine the best course of action and spells out SCADA system cryptographic system requirements should a utility decide SCADA encryption to be necessary. Part 2 defines how the encryption should take place and discusses the protocols and the encryption algorithms that should be used. Part 3, covers cryptographic protection of existing networked SCADA systems. The fourth part focuses on embedding encryption technology into SCADA components at the manufacturing stage. AGA is working with the U.S. Department of Energy (DOE) to seek collaborative activities between the AGA Report 12 Task Group and DOE's nati onal laboratories to achieve completion of the AGA 12 series.

4.2.2 Energy Related Standards

There are some standards commonly used in to communicate with energy monitoring devices and read their data. Some of those are:

IEC 62056-42: Also known as DLMS – Device Language Message Specification. This is an electricity metering data exchange for meter reading, tariff and load control [EMT7]. Correct exchange of meter data is of major importance to the liberalized energy market. Remote energy meter interrogation is essential for the fast and reliable determination of balance or unbalance between forecasts and actual energy usage. The data collection protocol DLMS/COSEM is an internationally recognized standard that is ideal for this very purpose.

ISO 50001:2011: This is based on the management system model of continual improvement also used for other well-known standards such as ISO 9001 or ISO 14001. This international standard outlines energy management practices that are considered to be the best, globally. Energy management experts developed the standard to promote energy saving, cut costs and meet environmental requirements [EMT8].

IEC 61000-4-30: Power Quality measurement is still a quite embryonic market although there are hundreds of manufacturers around the world. Whereas basic variables like RMS values of voltage and current are well defined, some power quality variables are not. This has led to a situation, that different instruments might show different results. The standard, issued by the International Electrotechnical Commission, IEC 61000-4-30 defines for each type of parameters the measurement methods to obtain reliable, repeatable and comparable results. [EMT9].

4.2.3 Standards Related to Sensors Network Technologies Applied to Physical Security

Worldwide standards make innovation easier thanks to their significant impact on markets. They allow being more competitive, they widen market segments thanks to their interoperability and ensure the system reliability.

4.2.3.1 Open Network Video Interface Forum (ONVIF)

The Open Network Video Interface Forum (ONVIF) is a non-profit organization, promoting and developing global standards for interfaces of IP-based physical security products. The work in ONVIF is driven and carried out by its member in various committees and working groups. The ONVIF specification defines a common protocol to share information between IP-based video sensors, especially automatic discovering of new equipments, continuous video stream and metadata.

Figure 4.2.3-1 ONVIF logo

4.2.3.2 Physical Security Interoperability Alliance (PSIA)

The Physical Security Interoperability Alliance (PSIA) is a global consortium of more than 65 physical security manufacturers and systems integrators focused on promoting interoperability of IP-enabled security devices and systems across the security ecosystem and beyond. Their focus is on how devices, services and systems can easily share among themselves the information and intelligence they generate.

Figure 4.2.3-2 PSIA logo

4.3 Smart Grid

To date, nearly 2,500 papers focused on smart grid have been published in over 40 IEEE journals. IEEE has nearly 100 standards and standards in development relevant to smart grid, including the over 20 IEEE standards named in the NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0. The NIST report describes a high-level reference model for the smart grid, identifies nearly 80 existing standards that can be used now to support its development, and identifies high priority gaps for which new or revised standards are needed [http://smartgrid.ieee.org/ieee-smart-grid].

Standards currently in development include [http://ieeexplore.ieee.org/xpl/opacstd.jsp]:

- IEEE P2030 Draft Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), and End-Use Applications and Loads
- IEEE SCC21 1547 Standards for Interconnecting Distributed Resources with Electric Power Systems
- IEEE SCC 31 Automatic Meter Reading and Related Services
- IEEE 802 LAN/MAN Standards Series

IEEE P2030 - Draft Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), and End-Use Applications and Loads provides guidelines for smart grid interoperability. This guide provides a knowledge base addressing terminology, characteristics, functional performance and evaluation criteria, and the application of engineering principles for smart grid interoperability of the electric power system with end-use applications and loads. The guide discusses alternate approaches to good practices for the smart grid. It also provides guidelines in understanding and defining smart grid interoperability of the electric power system with end-use applications and loads. Integration of energy technology and information and communications technology is necessary to achieve seamless operation for electric generation, delivery, and end-use benefits to permit two way power flows with communication and control. Interconnection and intra-facing frameworks and strategies with design definitions are addressed in this standard, providing guidance in expanding the current knowledge base. This expanded knowledge base is needed as a key element in grid architectural designs and operation to promote a more reliable and flexible electric power system.

IEEE SCC21 1547 – Standard for Interconnecting Distributed Resources with electric Power Systems establishes criteria and requirements for interconnection of DER with EPS and associated interfaces, providing a uniform standard for the interconnection and interoperability of DER with EPS. It provides requirements relevant to the interconnection and interoperability performance, operation and testing, and, to safety, maintenance and security considerations.

IEEE SCC 31 Automatic Meter Reading and Related Services promotes the research and development of standards, guidelines, and practices in the field of telemetry technology for meter reading, energy management and customer premises equipment. This field includes automatic meter reading and energy management through telemetry technologies (telephone, radio, power line carrier, cable, etc.) primarily for gas, electric and water utilities.

IEEE 802 LAN/MAN Standards Series provides an overview to the family of IEEE 802 standards. It describes the reference models for the IEEE 802 standards and explains the relationship of these standards to the higher layer protocols; it provides a standard for the structure of IEEE 802 MAC addresses; it provides a standard for identification of public, private, prototype, and standard protocols; it specifies an object identifier hierarchy used within IEEE 802 for uniform allocation of object identifiers used in IEEE 802 standards; and it specifies a method for higher layer protocol identification

Others recommended cited Standards of interest are SAE J1772 - Electrical Connector between PEV and EVSE – Electrical connector between Plug-in Electric Vehicles (PEVs) and Electric Vehicle Supply Equipment (EVSE); SAE J2847/1-3 - Communications for PEV Interactions; J2847/1 Communication between Plug-in Vehicles and the Utility Grid; J2847/2 Communication between Plug-in Vehicles and the Supply Equipment (EVSE); J2847/3 Communication between Plug-in Vehicles and the Utility Grid for Reverse Power Flow [GRID1].

Security and privacy issues are of major concern for smart grid users. A report from the European Union agency for Network and Information Security (www.enisa.europa.eu) describes the need for a harmonized European smart grid certification practices. It contains information about several certification approaches, describes the European situation, discusses the advantages and challenges and provides recommendations to involved stakeholders [GRID2].

Despites evolution of the power grid has been slow, it should follow the same development trends as many technologies. For George Flammer (Chief Scientist, Standford University), it is important to look back when it is intended to envisage the future of the smart Grid. Therefore, a decade ago the industry effectively had no standard products, making vendor-to-vendor or utility-to-utility compatibility rare and fragile. Ten years from now almost everything will be interoperable and standardized, creating a large and robust product ecosystem. Ten years ago utility applications ran isolated in their own operational silos, extending from the sensors in the field to the management software in the office. Ten years from now, the smart grid network will be the “big data” platform that utility – and other – applications will run on.

Ten years ago the speeds and capacity of most of the Field Area Networks (FANs) measured in kilobits and transactions per minute. Ten years from now, FANs will run at megabits and there will be more sensors and devices deployed than anyone today has predicted.

Ten years ago there were just a few suppliers dedicated to utilities' needs – the metering companies, the distribution companies, and some software concerns. Ten years from now, easier entry into the smart grid industry combined with greater demand for novel solutions will allow solution providers from other industries to compete with the agile survivors of current incumbents in a larger, more dynamic smart grid ecosystem.

The JRC's 2013-14 Smart Grid database (ses.jrc.ec.europa.eu) contains 459 smart grid R&D and Demo & Deployment projects from all 28 European Union countries, launched from 2002 up until today, which amount to €3.15 billion in investments. Conclusions state that key obstacles and challenges still appear to be at the social and regulatory levels (rather than technical constraints). The range of legal and regulatory arrangements in Europe might present significant barriers to the replicability of project results in different areas and to the scalability of projects to larger regions. Targeted analyses are necessary to understand the impact of the current wholesale and retail market schemes (and the related electricity prices and tariffs structures) on smart grid deployment opportunities. Uncertainty persists in several countries over: roles and responsibilities in new smart grid applications, sharing of costs and benefits and consequently new business models [GRID3].

4.4 Security Standards

ISO/IEC 27032:2012 - (Guidelines for cybersecurity) provides guidance for improving the state of Cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains, in particular:

- information security,
- network security,
- internet security, and
- critical information infrastructure protection (CIIP).

It covers the baseline security practices for stakeholders in the Cyberspace. This International Standard provides:

- an overview of Cybersecurity,
- an explanation of the relationship between Cybersecurity and other types of security,
- a definition of stakeholders and a description of their roles in Cybersecurity,
- guidance for addressing common Cybersecurity issues, and
- a framework to enable stakeholders to collaborate on resolving Cybersecurity issues.

ISO/IEC 27001:2005 - (Information security management) covers all types of organizations (e.g. commercial enterprises, government agencies, not-for profit organizations). ISO/IEC 27001:2005 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof. ISO/IEC 27001:2005 is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties.

ISO/IEC 27001:2005 is intended to be suitable for several different types of use, including the following:

- use within organizations to formulate security requirements and objectives;
- use within organizations as a way to ensure that security risks are cost effectively managed;
- use within organizations to ensure compliance with laws and regulations;
- use within an organization as a process framework for the implementation and management of controls to ensure that the specific security objectives of an organization are met;
- definition of new information security management processes;
- identification and clarification of existing information security management processes;
- use by the management of organizations to determine the status of information security management activities;
- use by the internal and external auditors of organizations to determine the degree of compliance with the policies, directives and standards adopted by an organization;
- use by organizations to provide relevant information about information security policies, directives, standards and procedures to trading partners and other organizations with whom they interact for operational or commercial reasons;
- implementation of business-enabling information security;
- use by organizations to provide relevant information about information security to customers.

ISO/IEC 27005:2011 - (Information security risk management) provides guidelines for information security risk management. It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach. Knowledge of the concepts, models, processes and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is important for a complete understanding of ISO/IEC 27005:2011.

ISO/IEC 27005:2011 is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) which intend to manage risks that could compromise the organization's information security.

4.5 Conclusion

In this section the standards related to FUSE-IT value-chain/building-blocks and some vendor-specific interfaces which are used in FUSE-IT, are discussed. In this regards, activity of oneM2M, IoT working groups of IETF and IEEE, IoT Alliances and their implementations are quoted. OneM2M aimed at producing globally applicable, access-independent technical specifications and technical reports to define and specify a common, efficient, easily and widely available M2M Service Layer. The other activity in this domain is IoT standardization at the IETF which has focused more on the Internet, routing, applications and security areas. In addition to mentioned organizations, IEEE working groups and IoT Alliances focuses on "smart object" communications (i.e. IoT & M2M) and making the internet of things smarter. These working groups have a number of standards, projects and events that are directly related to FUSE-IT projects.

Acronyms

CoAP	Constrained Application Protocol
CoRE	Constrained RESTful Environments
DTLS	Datagram Transport Layer Security
FUSE-IT	Facility Using smart Secured Energy & Information Technology
IETF	Internet Engineering Taskforce
ITEA	Information Technology for European Advancement
LLN	Low Power and Lossy network
LS	Laser Scanner
MW	Microwave Sensor
PIR	Passive Infrared Sensor
RPL	IPv6 Routing Protocol for Low-Power and Lossy Networks
WG	Working Group

References

[RAD] http://www.tecknisolar.com/2/109/militaire-et-securite-civile/protection-surveillance-radar-de-detection-maritime.html

[RAPID] http://www.ara.com/rapid/

[HGH] http://www.hgh.fr/Produits/Optronique-de-securite

[PIS] http://en.wikipedia.org/wiki/Passive_infrared_sensor

[PIR_BI] “Infrarouge passif, Hyperfréquence ou Bi-Technologie ?”, SYS.MI.LAN, 2007

[VID] http://www.mobilevideosurveillance.com/options.htm

[IVSS] “Intelligent Video Surveillance Systems”, edited by Jean-Yves Dufour, Networks and Telecommunications Series, 2013

[EXEN] http://www.exensor.com/product-category/?cat=ugs

[CRE] «Smart Grids CRE,» [Online]. Available: http://www.smartgrids-cre.fr/index.php?p=definition-smart-grids.

[ESU1] Stuart Borlase, “Smart Grids: Infrastructure, technology and solutions”, CRC Press, Taylor and Francis Group, 2012.

[ESU2] Stephen F. Bush, “Smart Grid: Communication-Enabled intelligence for the Electric Power Grid”, IEEE Press, John Wiley & Sons Ltd. Ed., 2014.

[ESU3] Chun-Hao Lo, Ansari, N., “The Progressive Smart Grid System from Both Power and Communications Aspects”, Communications Surveys & Tutorials, IEEE , vol.14, no.3, pp.799,821, Third Quarter 2012.

[MIC1] Nikos Hatziargyriou, et al., “Microgrids: Architectures and control”, Edited by Prof. Nikos Hatziargyriou, IEEE Press, John Wiley and sons, Ltd., 2014.

[MIC2] Robert Lasseter, “Microgrids [distributed power generation]”, Power Engineering Society Winter Meeting, 2001. IEEE. pp. 146–149 vol.1, 2001.

[MIC3] Robert Lasseter et.al., “White Paper on Integration of Distributed Energy Resources The CERTS Microgrid Concept”, 2002. Available at: http://certs.lbl.gov/.

[MIC4] Giri Venkataramanan and Mahesh Illindala, “Microgrids and sensitive loads”, 2002 IEEE Power Engineering Society Winter Meeting, Vols 1 and 2, Conference Proceedings 315–322, 2002.

[MIC5] Manuel Sánchez-Jiménez, “European Technology SmartGrids Platform – Vision and Strategy for Europe’s Electricity Networks of the Future”, European Commission for Research Sustainable Energy Systems, Brussels 2006.

[MIC6] Logenthiran, T. & Srinivasan, D., “Multi-agent system for the operation of an integrated microgrid”, Journal of Renewable and Sustainable Energy, 4, 2012.

[MIC7] Dimeas, A. L. & Hatziargyriou, N. D., “Operation of a multiagent system for microgrid control”, IEEE Transactions on Power Systems, 20, 1447-1455, 2005.

[MIC8] Nikos Hatziargyriou, Hiroshi Asano, Reza Iravani and Chris Marnay, “Microgrids: An Overview of Ongoing Research, Development, and Demonstration Projects”, IEEE Power & Energy magazine, July/August 2007.

[MIC9] Nikos Hatziargyriou, “Advanced Architectures and Control Concepts for More Microgrids – Specific Targeted Project”, Executive Summary Report, Final Results, 2009.

[MIC10] Lubna Mariam, Malabika Basu, Michel F. Conlon, “A Review of Existing Microgrid Architectures”, Hindawi Publishing Corporation, Journal of Engineering, Article ID937614, 2013.

[MIC11] N. W. A. Lidula and A. D. Rajapakse, “Microgrids research: a review of experimental microgrids and test systems, ”Renewable and Sustainable Energy Reviews,vol.15, no.1, pp.186–202, 2011.

[MIC12] C. Bossi, T. Degner, and S. Tselepis, “Distributed generation with high penetration of renewable energy sources,”Dispower, Final Public Report, Laboratory Tests Case Studies and Field Experience, Kessel, Germany, 2006.

[MIC13] Cesi Ricerca DER Test Facility (DER-TF), Italy, available online on http://www .microgrids.eu/.

[MIC14] J. Ostergaard and J. E. Neilsen, “The Bornholm Power System an Overview”, Kgs, Lyngby, Denmark, 2011.

[MIC15] The UK’s first Island Microgrid Goes Online, CAT, Wales, UK, 2009, available online on http://www.cat.org.uk/.

[MIC16] Manuela Sechilariu, Baochao Wang, Fabrice Locment, “Building-integrated microgrid: Advanced local energy management for forthcoming smart power grid communication”, Energy and Buildings, Volume 59, April 2013.

[MIC17] Xiaohong Guan; Zhanbo Xu; Qing-Shan Jia, "Energy-Efficient Buildings Facilitated by Microgrid," Smart Grid, IEEE Transactions on , vol.1, no.3, pp.243,252, Dec. 2010

[BAS1] I. Lück, Materna, “D02 - State of the Art” of Building as a Service (BaaS), ITEA 2 Project 12011, 2015.

[OPT1] I. Al-Anbagi, H. T. Mouftah, and M. Erol-Kantarci, “Design of a delaysensitive WSN for wind generation monitoring in the smart grid,” in Proc. IEEE CCECE, Niagara Falls, ON, Canada, May 8–11, 2011, pp. 001370–001373.

[OPT 2] I. Al-Anbagi, M. Erol-Kantarci, and H. T. Mouftah, “A low latency data transmission scheme for smart grid condition monitoring applications,” in Proc. IEEE Annu. EPEC, London, ON, Canada, Oct. 10–12, 2012, pp. 20–25

[OPT 3] J. Huang, H. Wang, Y. Qian, C. Wang, “Priority-based Scheduling and Utility Optimization for Cognitive Radio Communication Infrastructurebased Smart Grid,” IEEE Trans. Smart Grid, vol.4, no.1, pp.78-86, Mar. 2013.

[OPT 4] G. A. Shah, V. C. Gungor, and O. B. Akan, “A cross-layer QoS-aware communication framework in cognitive radio sensor networks for smart grid applications,” IEEE Trans. Ind. Informat., vol. 9, no. 3, pp. 1477–1485, Aug. 2013

[OPT 5] H. Wang, Y. Qian, H. Sharif, “Multimedia Communications over Cognitive Radio Networks for Smart Grid Applications,” IEEE Wireless Commun., vol. 20, no. 4, pp. 125-132, 2013

[OPT 6] Q. Li, Z. Feng, W. Li, A. Gulliver, P. Zhang “ Joint Spatial and Temporal Spectrum Sharing for Demand Response Management in cognitive Radio Enabled Smart Grid,” IEEE Trans. on Smart Grid, vol. 5, no. 4, pp. 1993-2001, July 2014.

[GRID] T. Q. Tuan, «Smart-Grid INtégration des Energies Renouvelables au réseau électrique,» 2014.

[EMT1] http://www.metrum.se

[EMT2] Jon Bickel et. al., “The Basics of Power Monitoring Systems”, Electrical Construction and Maintenance, Square D Co./Schneider Electric, 2007

[EMT3] http://www.powerlogic.com

[EMT4] http://www.en-mat.com

[EMT5] http://www.esightenergy.com/

[EMT6] http://en.wikipedia.org/wiki/Google_PowerMeter

[EMT7] “International Standard IEC 62056-42”, International Electrotechnical Commission, 1st Ed, ISBN 2-8318-6157-8, 02-2002.

[EMT8] http://www.iso.org/iso/catalog-ue_detail?csnumber=51297

[EMT9] “International Standard IEC 61000-4-30”, International Electrotechnical Commission, 2st Ed, ISBN 2-8318-1002-0, 10-2008

[BMS1] A. T. Alan, E. Costanza, J. E. Fischer, S. D. Ramchurn, T. Rodden, and N. R. Jennings. A field study of human-agent interaction for electricity tariff switching. In International conference on Autonomous Agents and Multi-Agent Systems, AAMAS '14, Paris, France, May 5-9, 2014, pages 965-972, 2014.

[BMS2] F. Jazizadeh, G. Kavulya, J. young Kwak, B. Becerik-Gerber, M. Tambe, and W.Wood. Human-building interaction for energy conservation in o_ce buildings. In Proceedings of the Construction Research Congress (CRC), 2012.

[BMS3] A. X. Jiang, M. Jain, and M. Tambe. Computational game theory for security and sustainability. JIP, 22(2):176-185, 2014.

[BMS4] L. Klein, J. young Kwak, G. Kavulya, F. Jazizadeh, B. Becerik-Gerber, P. Varakantham, and M. Tambe. Coordinating occupant behavior for building energy and comfort management using multi-agent systems. Automation in Construction, 22(0):525 - 536, 2012.

[BMS5] J. Kwak, D. Kar, W. B. Haskell, P. Varakantham, and M. Tambe. Building THINC: user incentivization and meeting rescheduling for energy savings. In International conference on Autonomous Agents and Multi-Agent Systems, AAMAS '14, Paris, France, May 5-9, 2014, pages 925-932, 2014.

[BMS6] J. Kwak, P. Varakantham, R. T. Maheswaran, Y. Chang, M. Tambe, B. Becerik-Gerber, and W.Wood. TESLA: an extended study of an energy-saving agent that leverages schedule flexibility. Autonomous Agents and Multi-Agent Systems, 28(4):605-636, 2014.

[BMS7] J. Kwak, P. Varakantham, R. T. Maheswaran, M. Tambe, F. Jazizadeh, G. Kavulya, L. Klein, B. Becerik-Gerber, T. Hayes, and W. Wood. SAVES: a sustainable multiagent application to conserve building energy considering occupants. In International Conference on Autonomous Agents and Multiagent Systems, AAMAS 2012, Valencia, Spain, June 4-8, 2012 (3 Volumes), pages 21-28, 2012.

[BMS8] H. Mostafa, P. Pal, and P. Hurley. Message passing for distributed qos-security tradeoffs. Comput. J., 57(6):840-855, 2014.

[BMS9] S. D. Ramchurn, M. A. Osborne, O. Parson, T. Rahwan, S. Maleki, S. Reece, T. D. Huynh, M. Alam, J. E. Fischer, T. Rodden, L. Moreau, and S. Roberts. Agentswitch: towards smart energy tariff selection. In International conference on Autonomous Agents and Multi-Agent Systems, AAMAS '13, Saint Paul, MN, USA, May 6-10, 2013, pages 981-988, 2013.

[BMS10] V. Robu, M. Vinyals, A. Rogers, and N. R. Jennings. Efficient buyer groups for prediction-of-use electricity tariffs. In Proceedings of the Twenty-Eighth AAAI Conference on Artificial Intelligence, July 27-31, 2014, Quebec City, Quebec, Canada., pages 451-457, 2014.

[BMS11] A. Rogers, S. Maleki, S. Ghosh, and N. R. Jennings. An intelligent agent for home heating management (demonstration). In International Conference on Autonomous Agents and Multiagent Systems, AAMAS 2012, Valencia, Spain, June 4-8, 2012 (3 Volumes), pages 1471-1472, 2012.

[BMS12] M. Vinyals, V. Robu, A. Rogers, and N. R. Jennings. Prediction-of-use games: a cooperative game theory approach to sustainable energy tariffs. In International conference on Autonomous Agents and Multi-Agent Systems, AAMAS '14, Paris, France, May 5-9, 2014, pages 829-836, 2014.

[BMS13] M. Wooldridge. Computational aspects of cooperative game theory. In Agent and Multi-Agent Systems: Technologies and Applications - 5th KES International Conference, KES-AMSTA 2011, Manchester, UK, June 29 - July 1, 2011. Proceedings, page 1, 2011.

[BMS14] M. Woolridge and M. J. Wooldridge. Introduction to Multiagent Systems. John Wiley & Sons, Inc., New York, NY, USA, 2001.

[BMS15] L. S. Shapley. A value for n-person games. In H. W. Kuhn and A. W. Tucker, editors, Contributions to the Theory of Games, volume II, pages 307–317. Princeton University Press,1953.

[NOC01] Nagios, http://www.nagios.org/

[NOC02] Ganglia, http://ganglia.sourceforge.net/

[NOC03] HP Operation Manager, http://www8.hp.com/us/en/software-solutions/operations-manager-infrastructure-monitoring/

[SM1] EuroCACS/ISRM 2014, “#143 Defining Information Security Governance for a Smart-meter Infrastructure”, Antonio Ramos, Managing Partner, Nplus1 Intelligence & Research

[SM2] Weiwei Jia; Haojin Zhu; Zhenfu Cao; Xiaolei Dong; Chengxin Xiao, “Human-Factor-Aware Privacy-Preserving Aggregation in Smart Grid”, Systems Journal, IEEE , vol.8, no.2, pp.598-607, June 2014.

[SM3] Skopik, F.; Zhendong Ma, "Attack Vectors to Metering Data in Smart Grids under Security Constraints" Computer Software and Applications Conference Workshops (COMPSACW), 2012 IEEE 36th Annual , pp.134-139, 16-20 July 2012.

[SOC01] CSIRT services by Canergie Mellon University, http://www.cert.org/incident-management/services.cfm

[SOC02] Incident Object Description Exchange Format (IODEF), RFC 5070, http://www.ietf.org/rfc/rfc5070.txt

[SOC03] Intrusion Detection Message Exchange Format (IDMEF), RFC 4765, www.ietf.org/rfc/rfc4765.txt

[SOC04] SIEM PRELUDE, http://www.prelude-ids.com/

[SOC05] NIDS Snort, http://www.snort.org/

[SOC06] NIDS Suricata, http://www.openinfosecfoundation.org/

[SOC07] HIDS OSSEC, http://www.ossec.net/

[SOC08] HIDS Samhain, http://la-samhna.de/samhain/

[SOC09] HP Arcsight (SIEM)

[SOC10] Loglogic

[SOC11] RSA envision

[SOC12] Information Technology Infrastructure Library (ITIL), https://www.axelos.com/itil

[SOC13] GARTNER, Magic Quadrant for Security Information and Event Management, http://www.gartner.com/technology/reprints.do?id=1-1W07M7N&ct=140626&st=sb

[SOC14] CISCO Security Manager, http://www.cisco.com/c/en/us/products/security/security-manager/index.html?referring_site=bodynav

[SOC15] SPLUN, http://www.splunk.com/

[SOC16] IBM Security Qradar SIEM, www.ibm.com/software/products/fr/fr/qradar-siem

[SOC18] McAfee SIEM, www.mcafee.com/cf/products/siem/index.aspx

[SOC19] LogRhythm, http://logrhythm.com

[SOC20] RSA Security Management, http://uk.emc.com/security/index.htm?nav=1

[SOC20] CYMERIUSTM, Airbus Defence & Space Cybersecurity, http://www.defenceandsecurity-airbusds.com/web/guest/cymerius2

[SOC21] NetCitadel Threat Response http://www.netcitadel.com/

[AII1] Qazi Mamoon Ashraf and Mohamed Hadi Habaebi. Autonomic schemes for threat mitigation in Internet of things. Journal of Network and Computer Applications, 49:112-127, 2015.

[AII2] Gianmarco Baldini, Trevor Peirce, Marcus Handte, Domenico Rotondi, Sergio Gusmeroli, Salvatore Piccione, Bertrand Copigneaux, Franck Le Gall, Foued Melakessou, Philippe Smadja, Alexandru Serbanati, and Julinda Stefa. Internet of Things Privacy, Security and Governance. Chapter 4 of book Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems. Ed. Ovidiu Vermesan and Peter Friess, pp. 207-224. 2013.

[AII3] Jens-Matthias Bohli, Peter Langendörfer and Antonio F. Gómez Skarmeta. Security and Privacy Challenge in Data Aggregation for the IoT in Smart Cities. Chapter 5 of book Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems. Ed. Ovidiu Vermesan and Peter Friess, pp. 225-244. 2013.

[AII4] Madhura P. M., Bilurkar Namrata, Jain Palash and Ranjith J. A survey on Internet of Things: security and privacy issues. IJITR, vol. 3, no 3, p. 2069-2074. 2015

[AII5] Sadeghi Ahmad-Reza, Wachsmann Christian and Waidner, Michael. Security and privacy challenges in industrial Internet of things. In Proceedings of the 52nd Annual Design Automation Conference (DAC '15). ACM, New York, NY, USA, Article 54, 6 pages. DOI=10.1145/2744769.2747942 http://doi.acm.org/10.1145/2744769.2747942. 2015.

[AII6] Jeffrey O Kephart and David M Chess. The vision of autonomic computing. Computer, 36(1): pp. 41–50, 2003.

[IETF] IETF standardization in the field of the internet of things (IoT): a survey. I Ishaq, D Carels, GK Teklemariam, J Hoebeke, Journal of Sensor and Actuator Networks, 2013

[VDI3811] http://www.beuth.de/

[GRID1] Douglas C. Hopkins, “Smart-Grid or the Microgrid?”, State University of New York at Buffalo, 2010.

[GRID2] European Union Agency for Network and Information Security (ENISA), “Smart grid security certification in Europe: Challenges and recommendations”, Dec 2014, available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/smart-grid-security-certification/smart-grid-security-certification-in-europe

[GRID3] Catalin Felix Covrig, et. al., “Smart Grid Projects Outlook 2014”, JCR Science and Policy Report, 2014.