ITEA 2

INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

FUSE-IT

EUREKA

FUSE-IT: Facility Using smart Secured Energy & Information Technology

Adrien BECUE

Cassidian CyberSecurity.SAS

PROJECT AMBITION

CCS (A. Bécue)

Project goal

Project goal:

Fuse-IT will address the need of sustainable, reliable, user-friendly, efficient and secure Building Management System (BMS) in the context of Smart Critical Sites.

Context:

–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.

Project Objectives

The result of Fuse-IT will be a Smart Secured Building System involving key innovative capabilities:

-M1-Secured shared sensors actuators & devices,

-M2-Trusted federated energy & information networks

-M3-Core building data processing & analysis

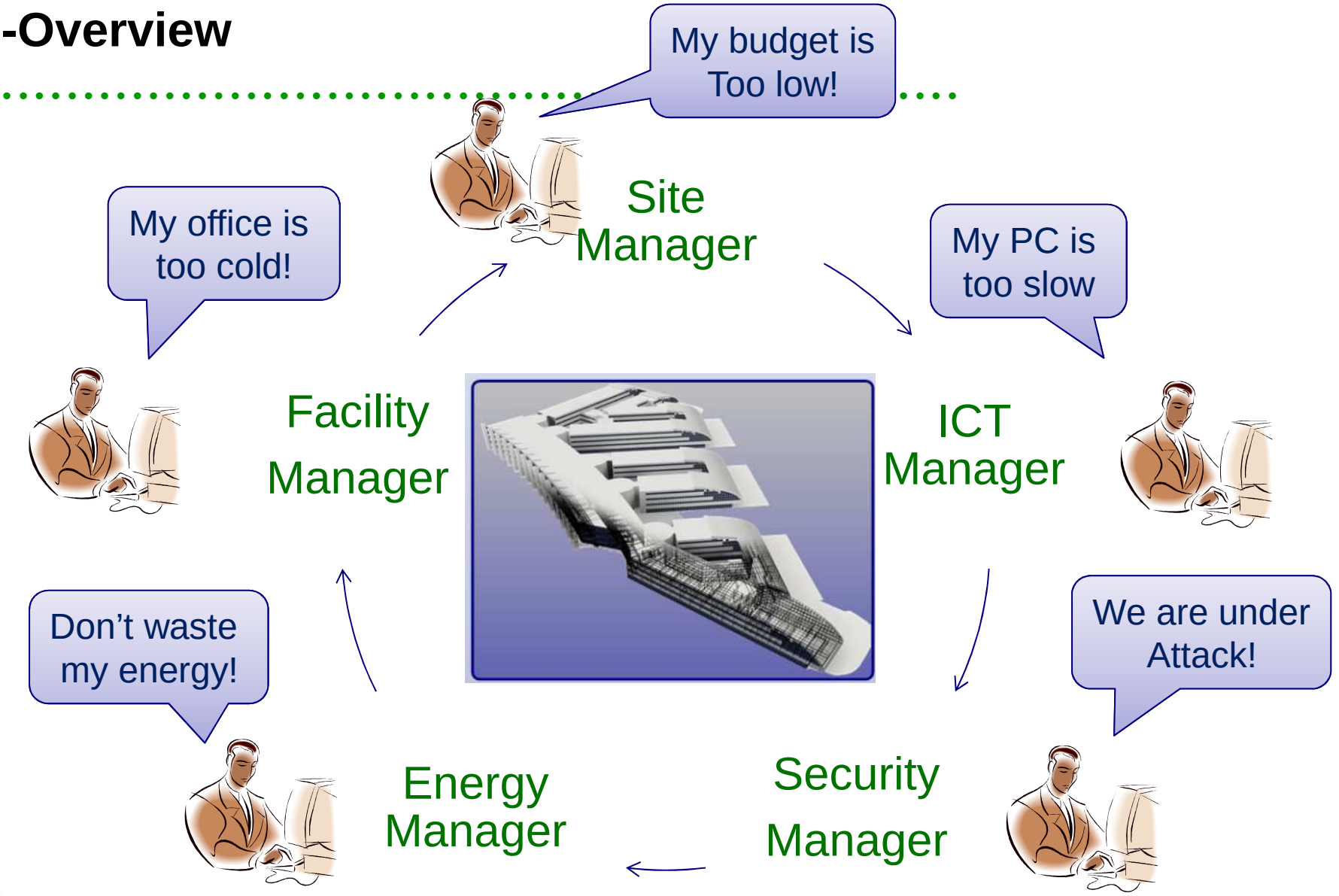
-M4-Smart unified building management interfaces

-M5-Full security Management Interfaces

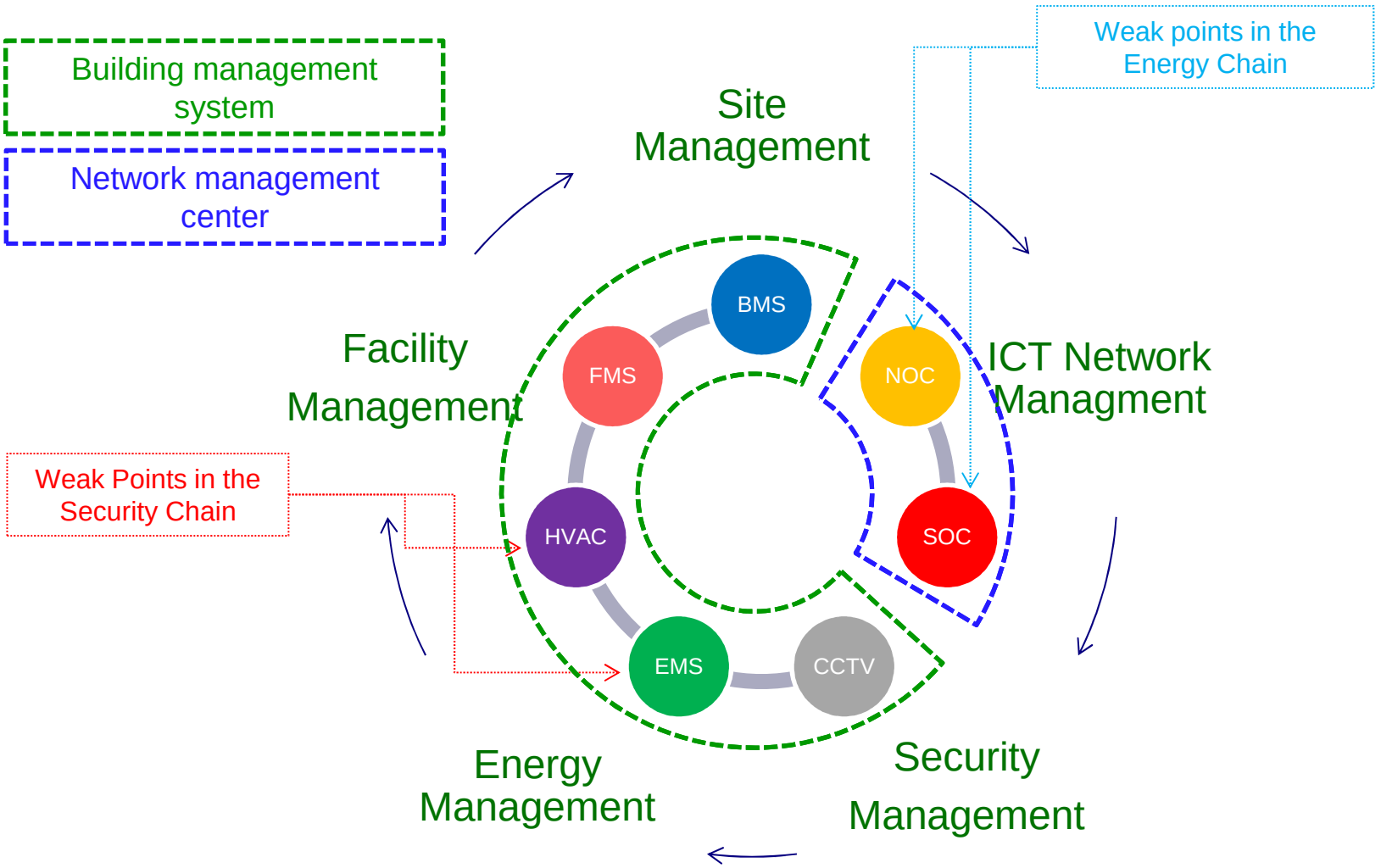
A service offering will also be set up to enable remote site monitoring under service contract, taking advantage from big data analytics capability.

A Smart Critical Building -Overview

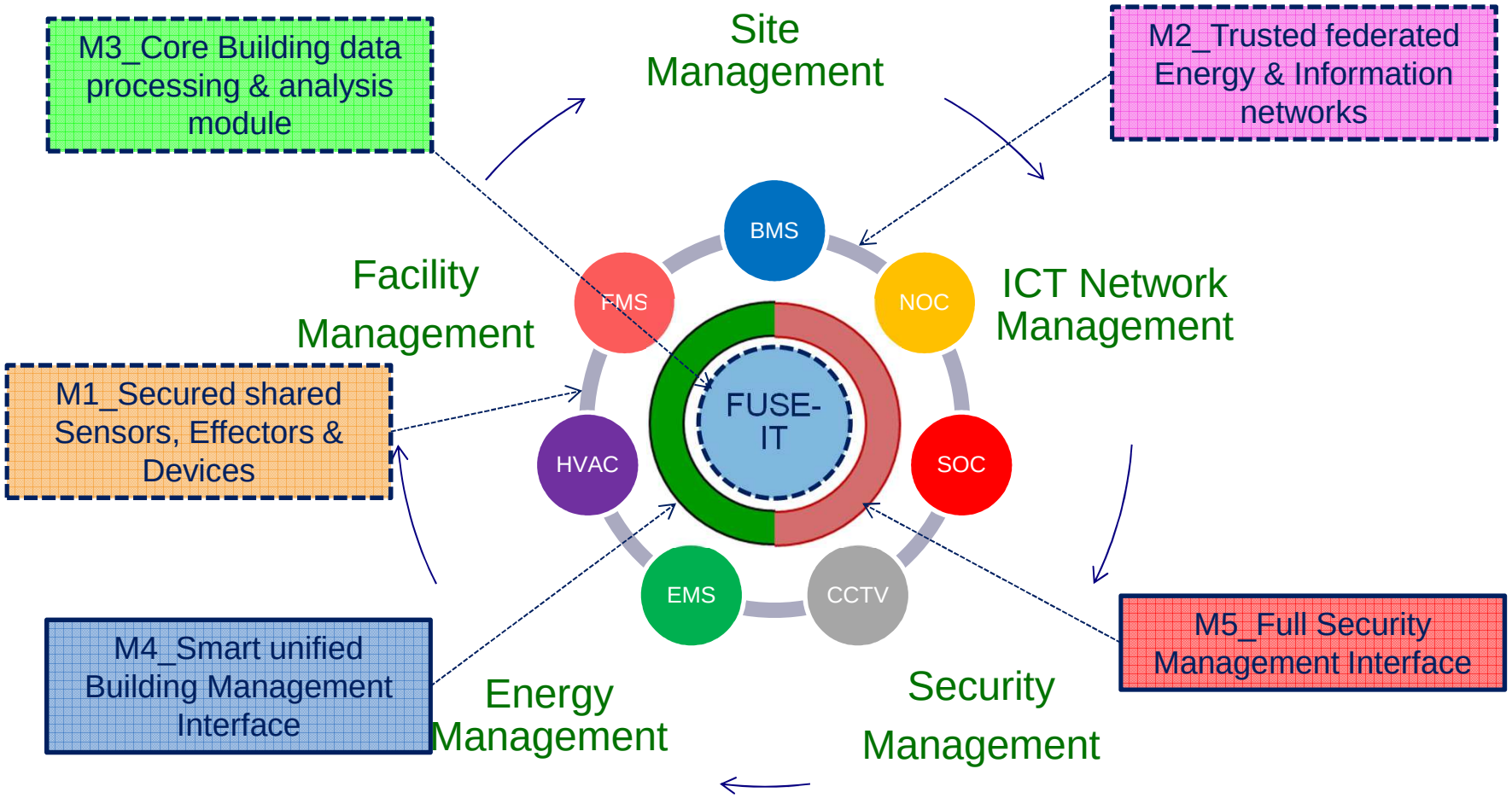
End-Users / Stakeholders -Overview



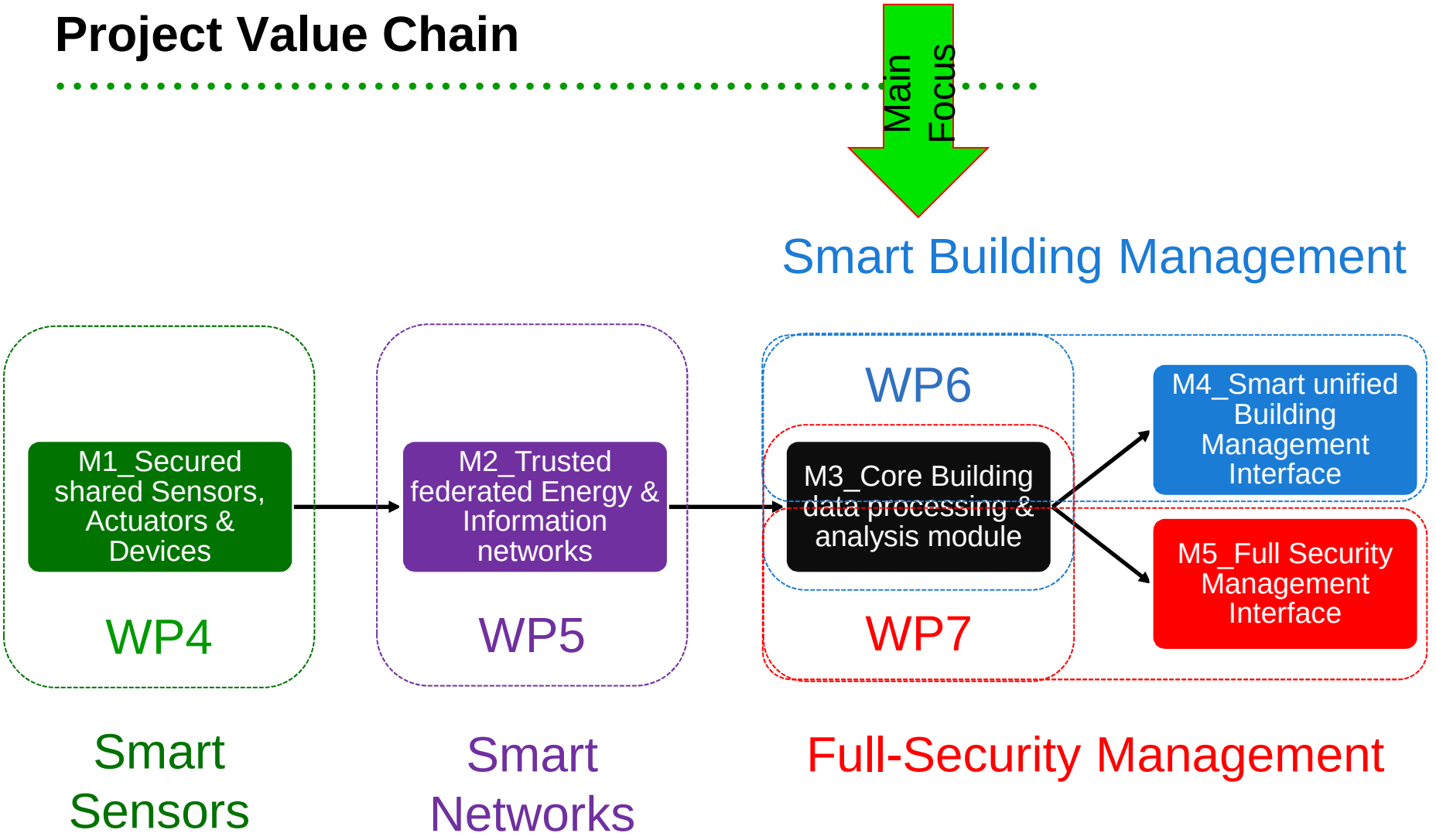
Technology bricks
-Legacy systems



Technology bricks
- Fuse-IT enhanced system



Project Value Chain



M1_Secured shared Sensors, Actuators & Devices

Innovations	Limitations addressed	Expected impact*
<u>M1_Secured shared Sensors, Actuators & Devices:</u> - Sensor placement optimization - Self* management of smart sensors - Trusted smart sensors implementing light crypto	<u>Flexibility limitations:</u> -Clash between security, energy efficiency and flexibility requirements -Clash between identity control and self-* device flexibility <u>Security limitations:</u> -Vulnerabilities “by design”	ST: support a major temporary event as Fuse-IT final demonstration (2000 exhibitors, 300 000 visitors) MT: marketing of an innovative sensor placement optimization tool helping reducing site equipment (5-10M$) LT: implementation of light crypto for embedded wireless sensor communication in building, aeronautics, automotive, train and ship industries (30-50M€)

M2_Trusted federated Energy & Information Networks

Innovations	Limitations addressed	Expected impact*
<u>M2_Trusted federated Energy & Information networks:</u> - Energy & information network federation - Trusted & efficient SCADA communication protocols -Secured wireless communication network capability - Physical / Logical network segregation capability	<u>Sustainability limitations:</u> -Wild-stacking of abounding information and control systems <u>Security limitations:</u> -Lack of SCADA-protocol aware network infrastructure -Vulnerabilities “by design” -Architecture weaknesses of cyber-physical networks	ST: secured indoor wi-fi accessible to employees of critical sites ST: SCADA certification and labelling services for manufacturers (10-15M€) MT: multi-B$ savings for energy suppliers on fraud and network recovery MT: Supply of security audit services in Smart Critical Buildings (200-500M€) LT: drastic cost savings in network infrastructure & cabling (average 100-200 K€ / building)

M3_Core Building Data Processing & Analysis module

Innovations	Limitations addressed	Expected impact*
M3_Core Building data processing & analysis module: -Common information base & KPIs -Cloud based holistic knowledge base and advanced monitoring layer -Correlation capability between logical & physical security events/incidents	Efficiency limitations: - Lack of appropriate building monitoring indicators -Effective management of physical/logical security events Flexibility limitations: -Micro-monitoring of energy at site level	ST: technological advantage in computational intelligence MT: marketing of a scalable universal data processing & analysis module for BMS application (1-5B€) LT: application to other activities demanding advanced data analysis capability (10-15 B€)

M4_Smart Unified Building Management Interface

Innovations	Limitations addressed	Expected impact*
M4_Smart unified Building Management Interface: -Advanced management and optimization capability -Smart management user-interface	Efficiency limitations: -Deadlock in the flow-down of energy production/consumption incentive Ergonomic limitations: -Profusion of vendor-specific user-interfaces:	ST: 30% energy savings on Smart Critical Sites MT: 50% savings on management software and maintenance cost related to building and energy monitoring MT: unified building management software sales (100-300M€) LT: remote site management service operation contracts (500-700M€)

M5_Full-Security Management Interface

Innovations	Limitations addressed	Expected impact*
M5_Full Security Management Interface: -Role-based assets & identity management capability -Event/process-based alerting capability -Integrated building security incident management interface	Security limitations: -Ignorance of cyber-physical network specificities Ergonomic limitations: -Non-existence of full-security supervision interfaces	MT: 30% savings on security and cybersecurity software, maintenance & upgrade cost MT: multi-B$ cost-avoidance related to cyber/physical attacks on critical sites MT: full-security management software sales (100-300M€) LT: remote full-security management service operation contracts (500-700M€)

FUSE-IT Technology Transfer Circle

FUSE-IT	Domains	A	B	C	D
WP	System layers/Activity domains	Energy & Smart Grids	Building Facilities	Information & communication systems	Security of Premises
4	Smart Sensors	Smart energy sensors	HVAC Sensors & effectors	Network sensors and ICT devices	Detection and anti-intrusion sensors
5	Smart Networks	Smart grids and micro-grids	Building Automation & SCADA	Information networks	Site security networks
6	[illegible]	[illegible] energy monitoring	Building Management Sytems (BMS)	Network Operation Centers (NOC)	Site security supervision systems
7	Security Management	Security of Smart Grids	Security of SCADA / BAS / BMS	Security Operation Centers (SOC)	Cyberprotection of Site security network

More efficiency in security

More security in efficiency

FUSE-IT Technology Transfer Circle

FUSE-IT exploitation strategy

Market drivers

Rules & Regulations
- European Policy
- National law

Demand Pull
- Corporate Policies
- End-users' needs

Supply Push
- Smart sensors netw.
- Big data analytics

Collective Awareness
- New vulnerabilities
- Attacks Resurgence

Market brakes

NICHE MARKET not targeted by existing Manufacturers
&
RELUNCTANCE from automation manufacturers to invest in related R&D

INVESTMENT COST related to Building Modernization
&
MIGRATION COST from Legacy Systems to FUSE-IT

PROPRIETARY Policy of Manufacturers
&
VERTICAL SILO standradization

Market enablers

HIGH PROFITABILITY Market (Critical Buildings)
&
Use of ITEA2 Label to get **R&T COFUNDING**

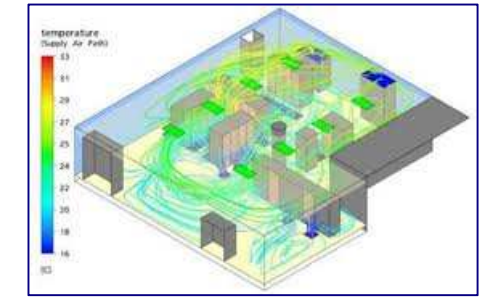
GLOBAL COST relevance
&
SERVICE Offering

CROSS-DOMAIN Approach
&
HORIZONTAL STRANDARDIZATION

Business Model

Fuse-IT Service Operation

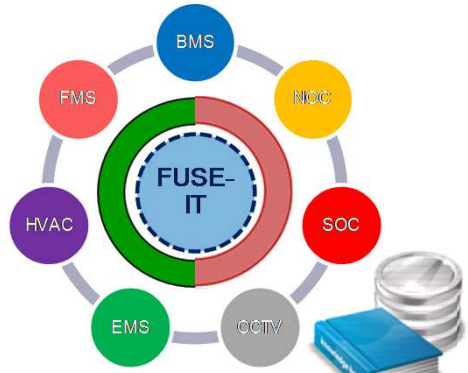
Remote monitoring



Data Center

Monitoring dashboard

Command & Control



KB

Expert ise

Command & Control

Full remote service operation

Strategic Office

Command & Control

Full remote service operation

Hospital

Full local operation

Power Plant

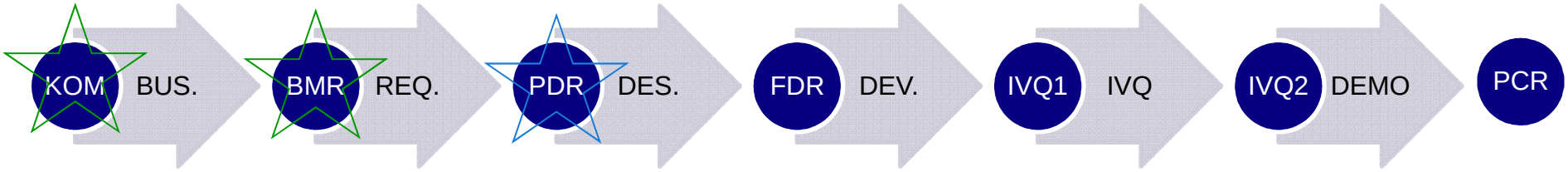
Full remote service operation

Technopark

MANAGEMENT OVERVIEW

CCS (A. Bécue)

Project Schedule



KOM	Kick-Off Meeting	M0	10/2014
BMR	Business Model review	M6	04/2015
PDR	Preliminary Design Review	M12	10/2015
FDR	Final Design Review	M18	04/2016
IVQ1	Validation of Network & Sensor layers	M24	10/2016
IVQ2	Integration, Validation & Qualification	M30	04/2017
PCR	Project Closing Review	M36	10/2017

Consortium Overview

France

Cassidian CyberSecurity
Institut Mines Télécom
ARC Informatique
ICAM Nantes
V-TREEM
CEA List
SOGETI High Tech
Université La Rochelle
Thales Research & Technology
Thales Systems
Université de Bourgogne

Canada

Cityzeen

Belgium

NIKO
i-Minds
LIN-K

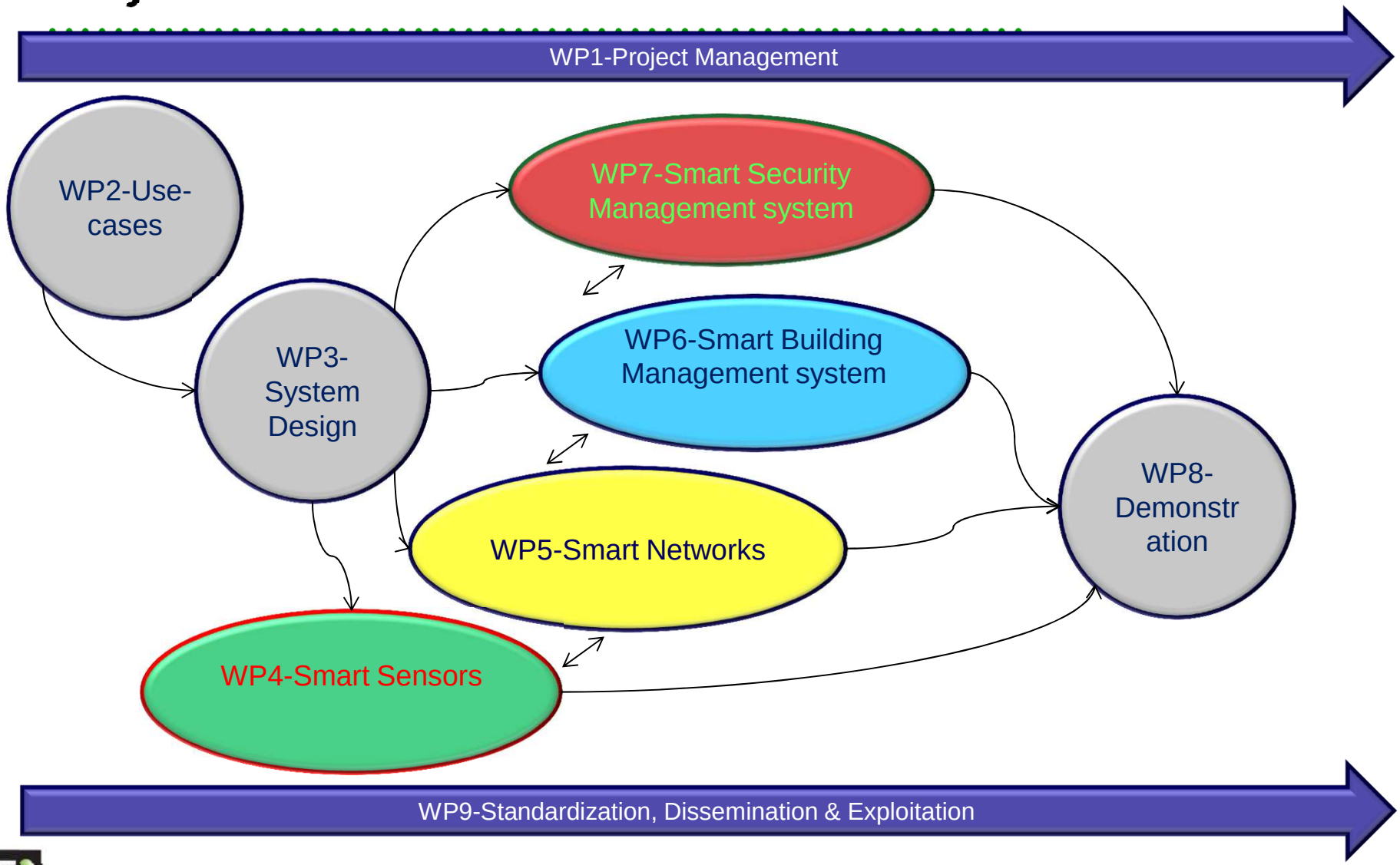
Portugal

ISEP-GECAD
SCHNEIDER PRT
SCHMITT Elevators
EVOLEO Technology
ISQ
IP-BRICK
Hospital San Jao

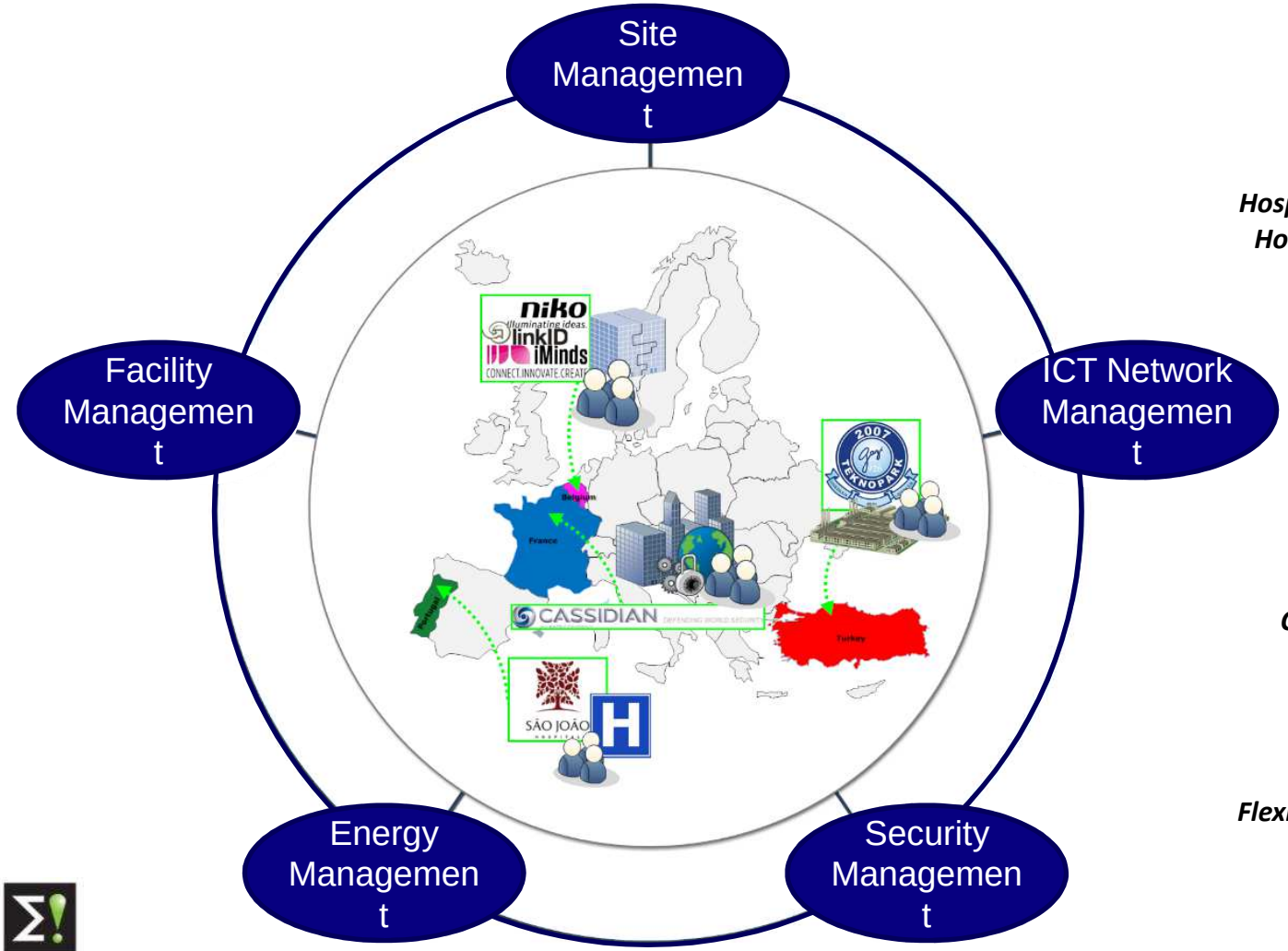
Turkey

MOSBIT
CTECH
GAZI Technopark
ENEL Energy plant

Project WBS


WP1-Project Management
WP2-Use-cases
WP3-System Design
WP4-Smart Sensors
WP5-Smart Networks
WP6-Smart Building Management system
WP7-Smart Security Management system
WP8-Demonstration
WP9-Standardization, Dissemination & Exploitation

DEMONSTRATION PLAN



Hospital S. João (HSJ), from Centro Hospitalar Saõ João, in Portugal

Gazi Teknopark, Turkey

Cassidian Elancourt, France

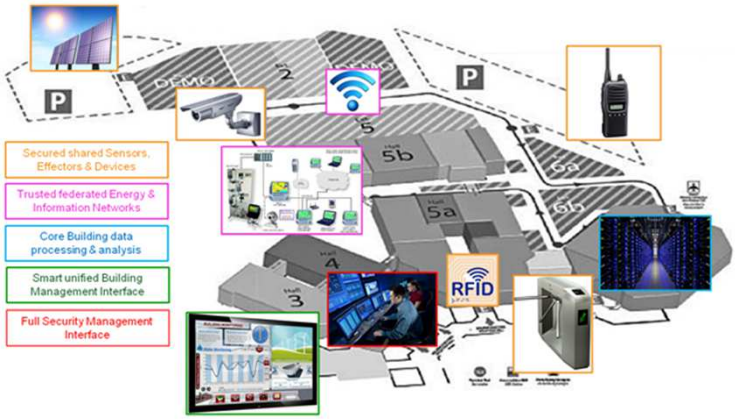
Flexible and reconfigurable offices, Belgium

PROJECT ACHIEVEMENTS

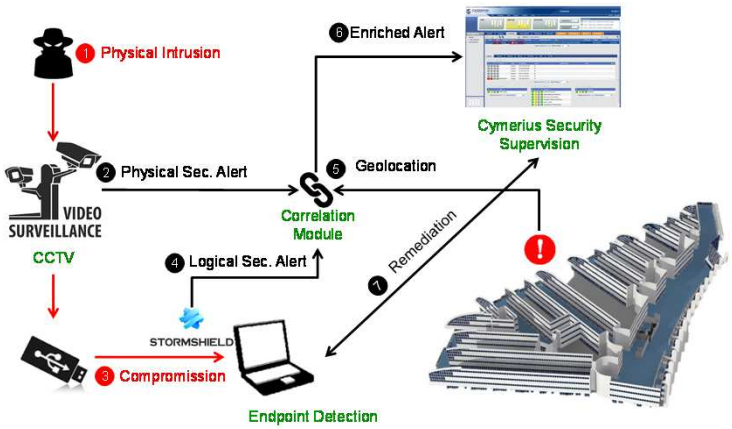
CCS (A. Bécue)

Key technical achievements

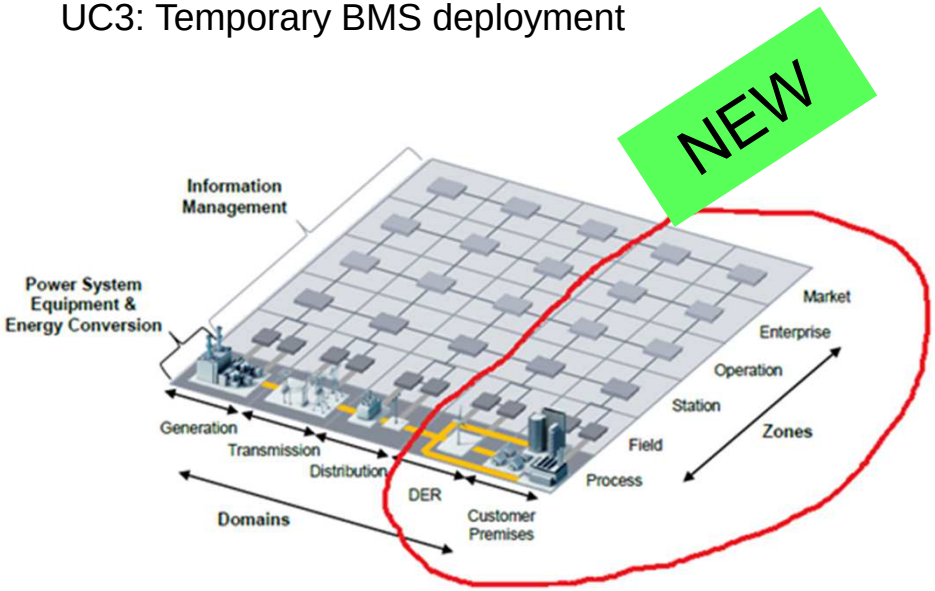
UC1: Adaptive Energy demand response



UC3: Temporary BMS deployment



UC2: Reaction to a cyber-physical attack



Common information base & KPIs (D3.3)

UC1-ADAPTATIVE DEMAND RESPONSE

GECAD (G. Marreiros)

Operational Challenge

- UC1 considers the Building Management System (BMS) of complex critical buildings considering the site activities – energy, facilities, ICT systems and site security
  - Intelligent energy resource management
  - Demand response will be considered internally, among installation owners in the building, and externally, in the smart grid context

- This UC will explore the possible aggregation of these installations to enable increased efficiency and lower costs

- Added topic: Building as a Microgrid

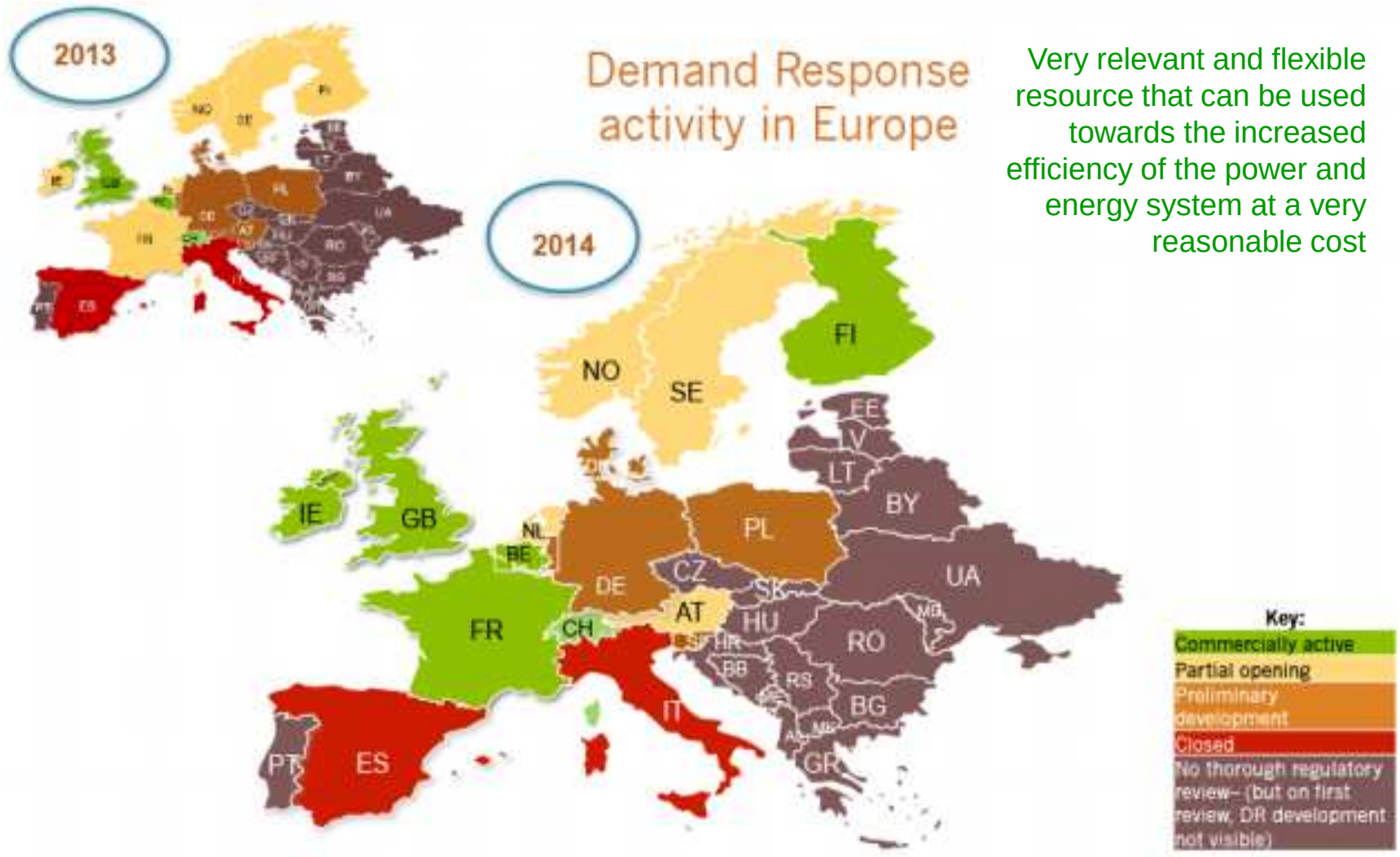
Technical Challenges

- Deal with intermittent resources (renewable)
- Apply devices for energy consumption/generation monitoring
- Information fusion
- Ensure data security and adequately dealing with privacy issues
- Implement forecasting methodologies to foresee energy generation, energy consumption and support resources scheduling
- Providing the required features so that the system is able to react at diverse time horizons (day-ahead, hour-ahead and real-time)
- Addressing large dimension resource management almost in real-time
- Cybersecurity needs to be appropriately applied to avoid jeopardize the safe and reliable power system operations
- Adaptive energy resources optimization while assuring critical services and locations
- Interoperability, replicability and scalability
- A new federative approach to assess impact of cyber-incidents and countermeasures on grid operation and processes

Use-case rationale

- Risks: energy blackouts:
  - 2003: Northeast USA/Canada 2003
  - 2003: Italy
  - 2006: Germany
  - 2015: Turkey
- Regulation: EU H2020 directives on Inefficient Use of Renewable Sources of Energy
- Opportunity: 2012 top countries with the highest penetration of wind:
  - Denmark (27.1%),
  - Portugal (16.8%)
  - Spain (16, 3%)
- Several wind curtailment situations: in Spain in the first four months of 2013, 850 GWh of wind were curtailed; between 28 to 31 of March, 637 GWh were curtailed!

Demand Response activity in Europe



Very relevant and flexible resource that can be used towards the increased efficiency of the power and energy system at a very reasonable cost

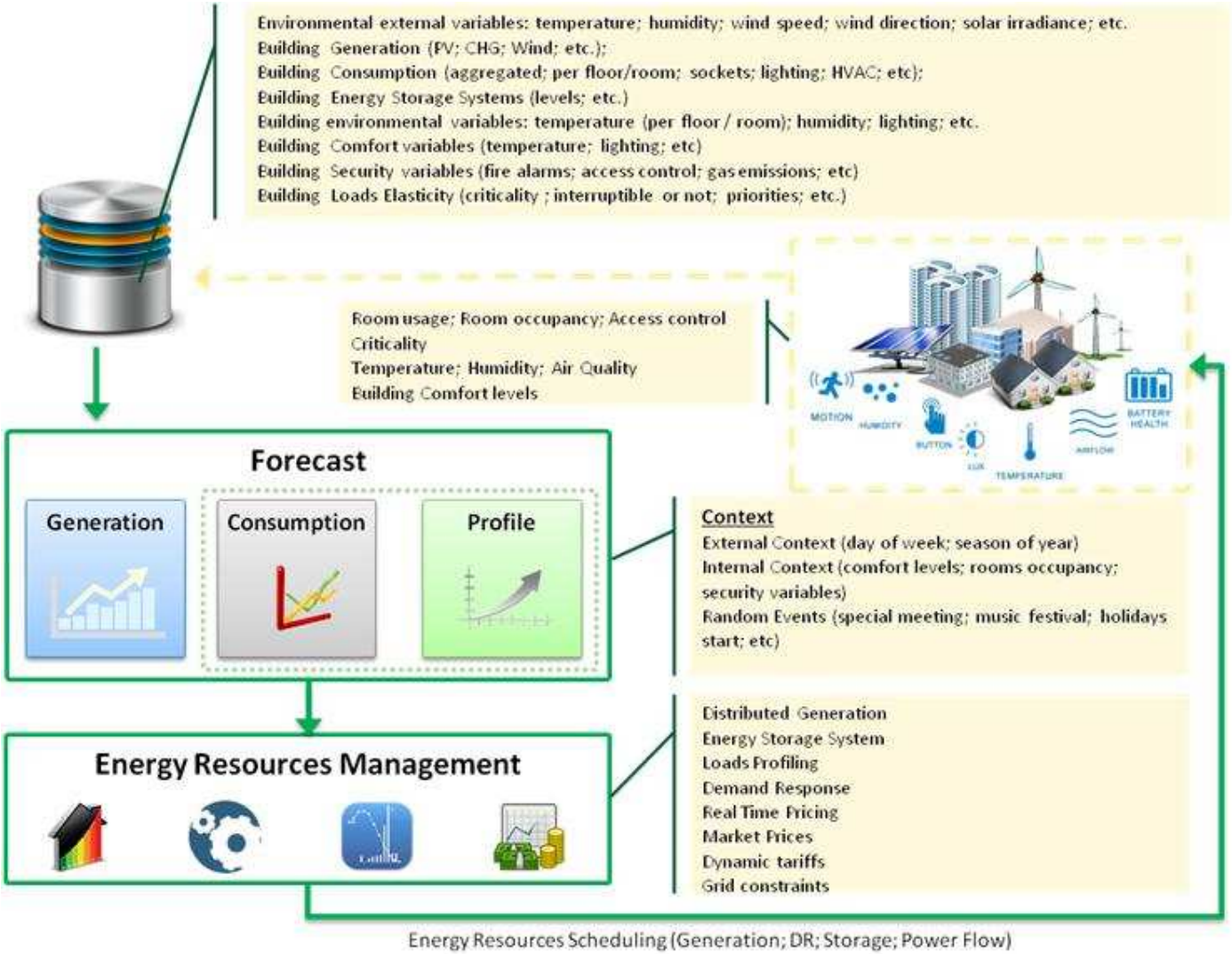
Sub-Cases

- **SC1: Resilient Dynamic Energy Resources Management and Secure Context Awareness**
  - Secure Generation Forecasting
  - Secure Load Profiling
  - Trusted and Smart Demand Response
  - Trusted and Smart Dynamic Tariffs
  - Trusted Billing
  - Optimization Methodologies
  - Secure Context Evaluation
  - Machine Learning of building users' preferences according to the context
  - Loads Elasticity and Dynamic Priorities

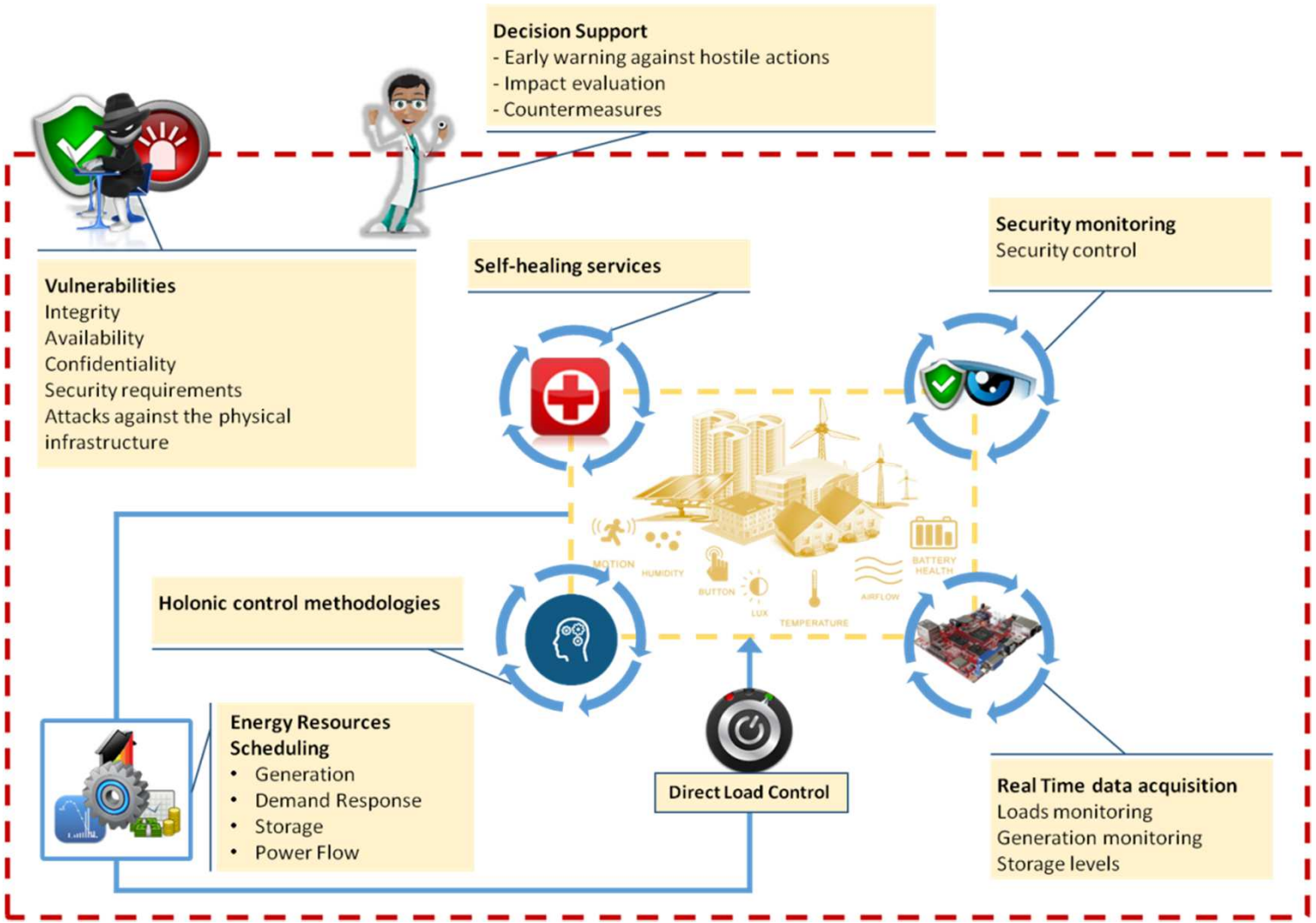
- **SC2: Distributed Control of Energy Resources**
  - Real loads monitoring and control
  - Security monitoring and control
  - Holonic control methodologies (based on real-time optimization)
  - Early warning considering cyber-attacks
  - Identification of impact on the Building
  - Self-healing services

- **SC3: Building as a Microgrid**
  - Obtain aggregated (Satellite) Buildings consumption / surplus
  - Forecast Market Prices
  - Apply DR to (Satellite) Buildings
  - Negotiations with neighbor Microgrids
  - Market participation
  - Switching between islanded vs grid-connected mode
  - DSO interaction
  - Manage several (Satellite) Buildings

SC1: Resilient Dynamic ERM and Secure Context Awareness



SC2: Distributed Control of Energy Resources



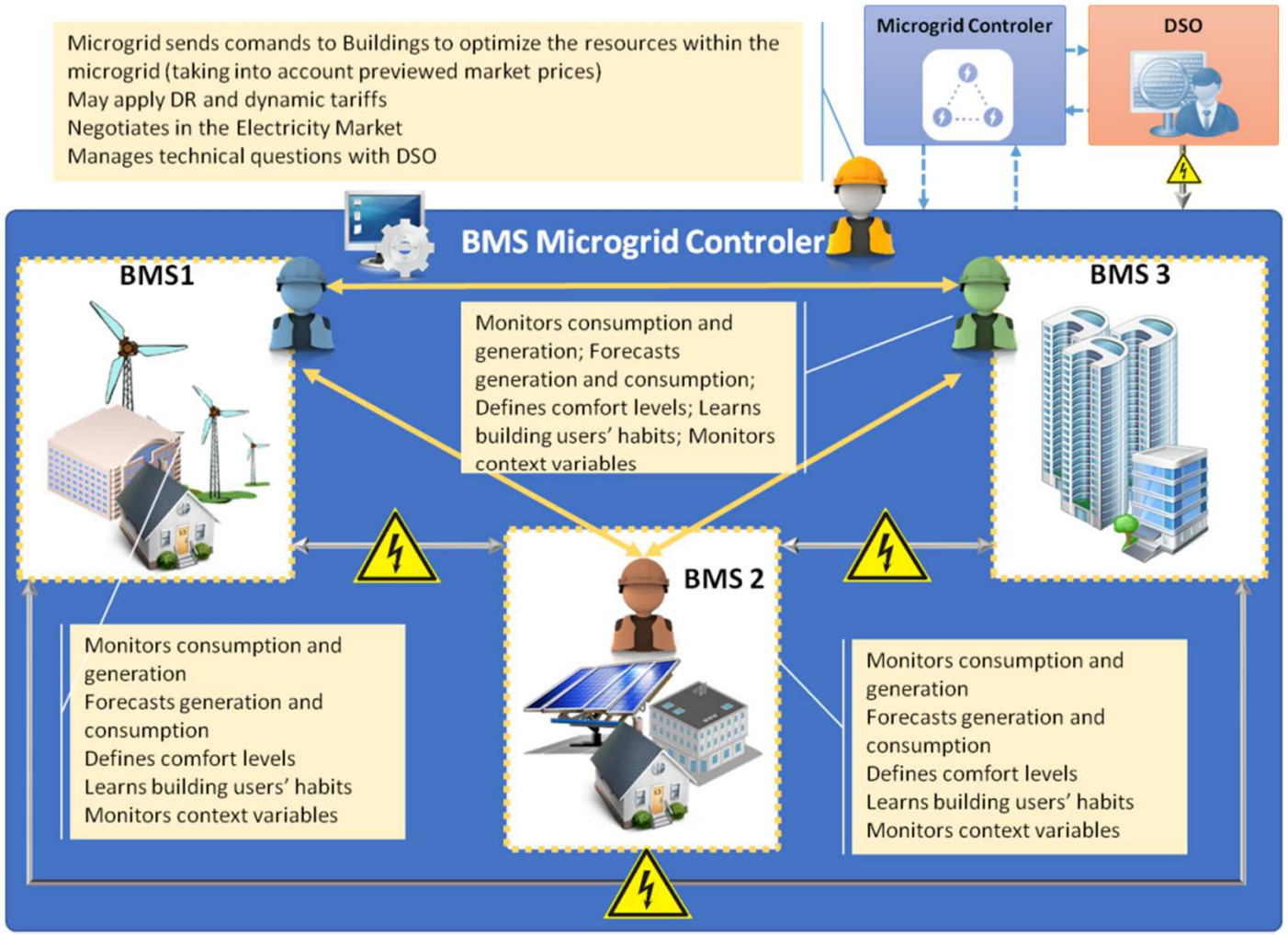
SC3: Building as a Microgrid

Microgrid 3

Microgrid 1

Microgrid 2

SC3: Building as a Microgrid

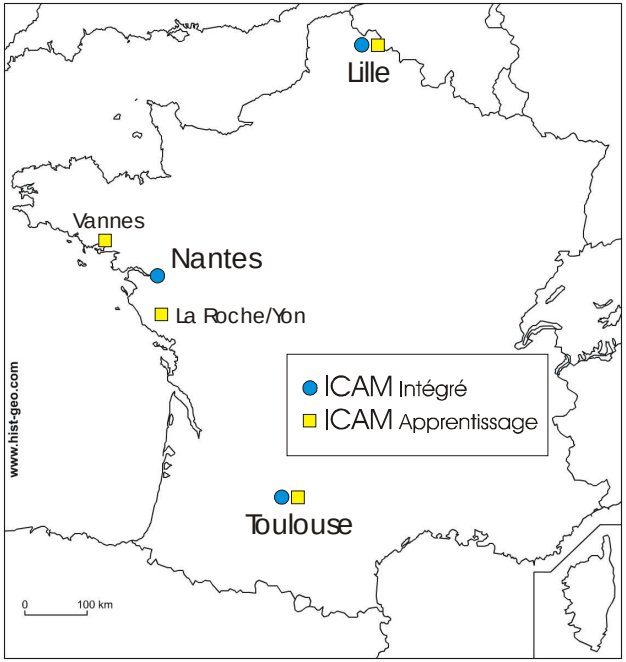


UC1-SC1-SMART LIGHTING EXPERIMENT

ICAM (L. Belhaj)

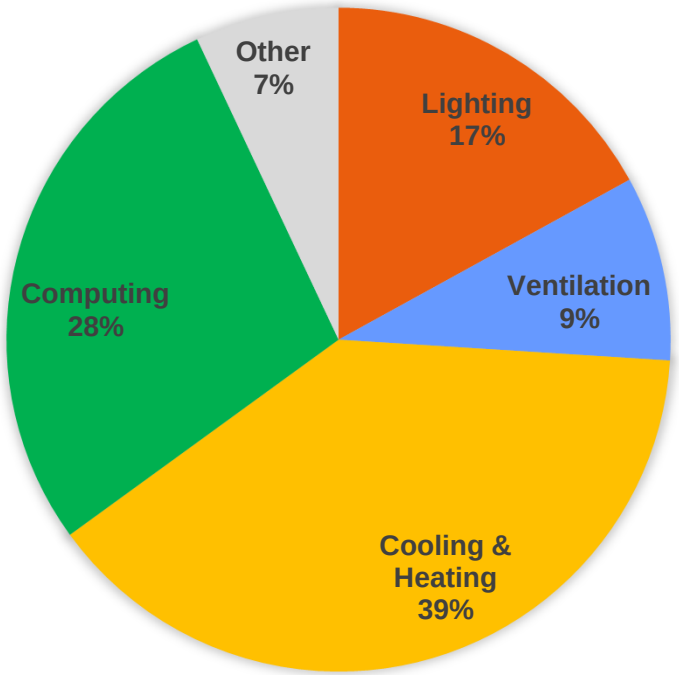
Experimentation site: Nantes Carquefou

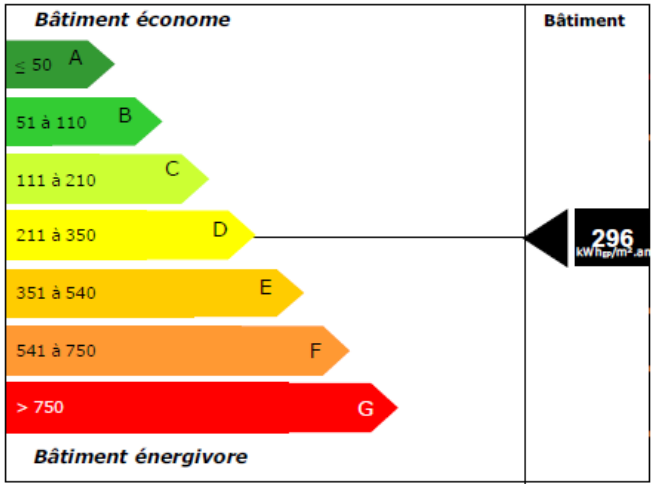
- 500 students
- 60 teachers and researchers
- Smart lighting demonstration



Smart Lighting Experiment

Power consumption measurements => Lighting consumption the actual building





- Proposition of scenarios and solutions for the whole building load management: batteries, PV and building loads: technologies and costs,
- **Available data for the actual offices building and the future one**

Smart sensors

- Targets :
  - Average illuminance= 500 lx (NBN EN 12464-1)
  - Comfort
  - Energy saving

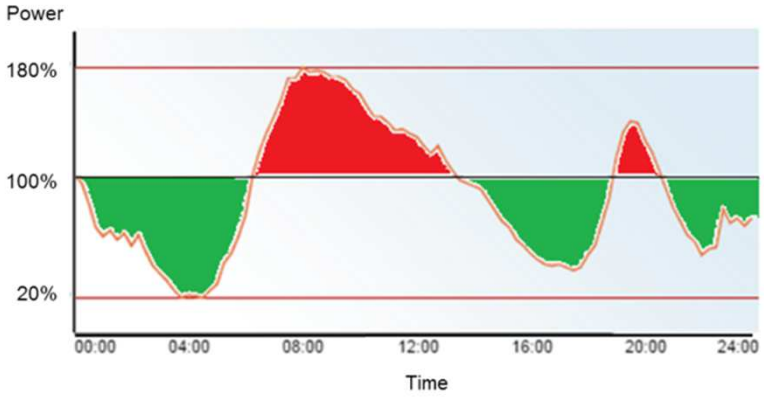
- Sensors :
  - Presence sensor

  - External/internal Brightness sensor

  - Power Meters

Office consumption regulation

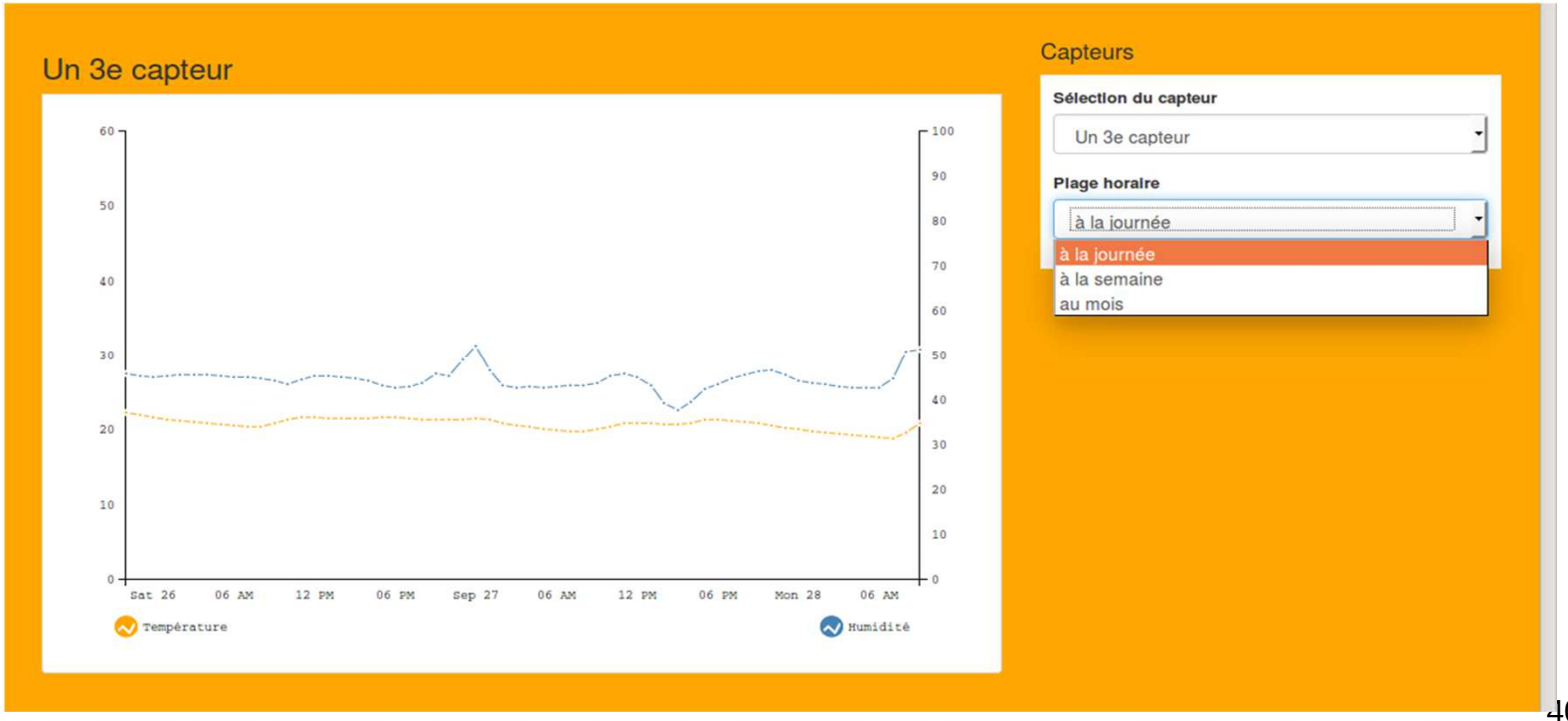
- Consumption regulation



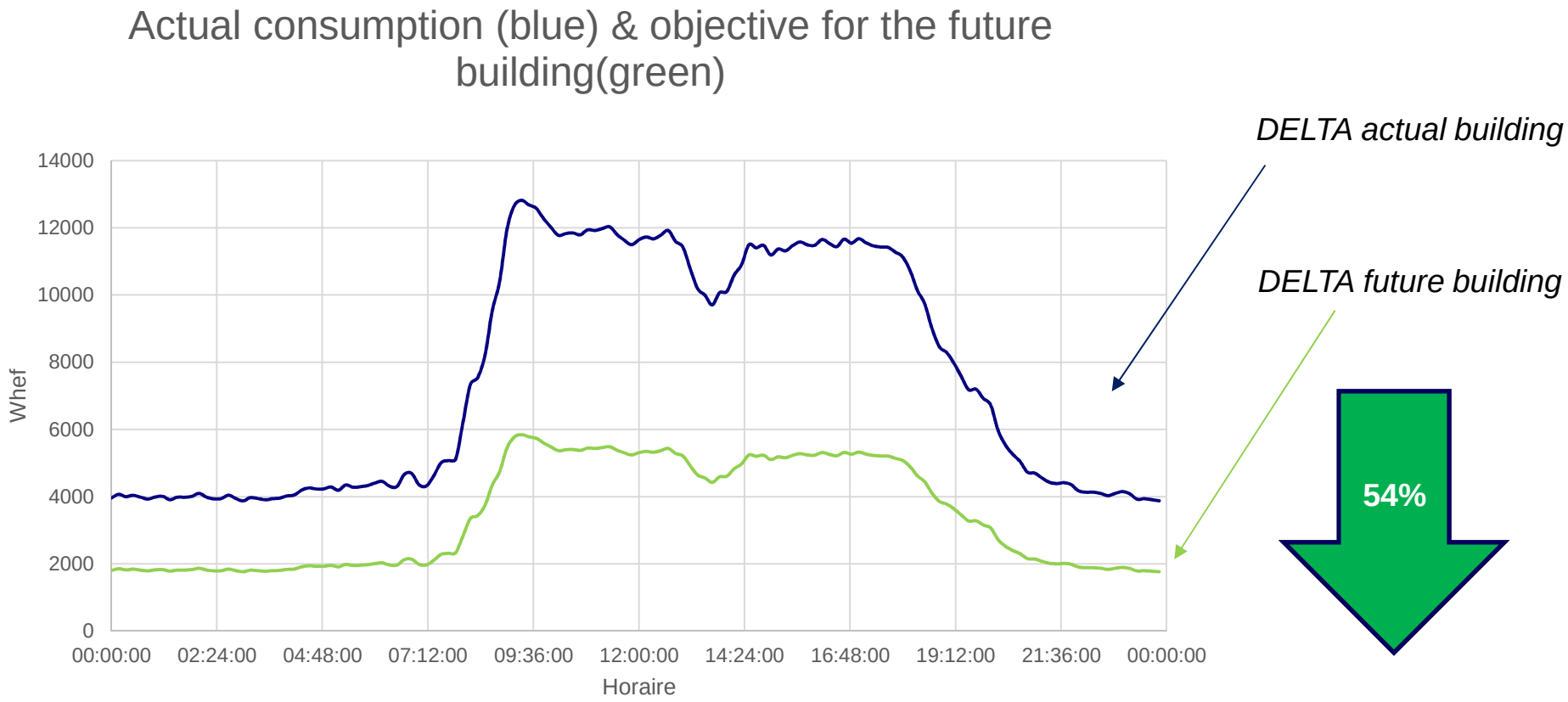
- Solar cell and dedicated battery

Data Management & Analysis

- Heterogeneous Data Management
- Fine-Grained Time Data Management & Analysis
  - Raw Data retrieved every minutes from sensors
  - End-User Data/preferences computed by slices of 1 hour, 1 day, 1 month



Smart Lighting Experiment



UC2-REACTION TO A CYBER-PHYSICAL ATTACK

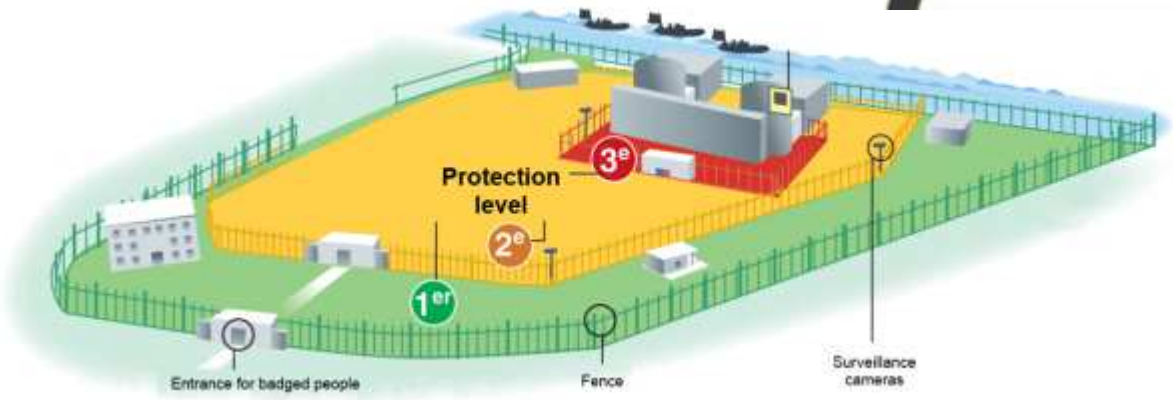
THALES (A. Galimberti)

Use Case 2 – Operational Challenges

- **Convergence of cyber security and physical security**
  - Securing cyber-physical systems such as:
    - Industrial Control Systems (ICS)
    - Building Management Systems (BMS)
    - Control Command (C2)
  - Securing critical infrastructures against blended attacks:
    - Physical intrusion to gain access to critical ICT assets as a mean to launch a cyber-attack
    - Cyberattacks on ICT-enhanced physical protection systems to enable a physical attack

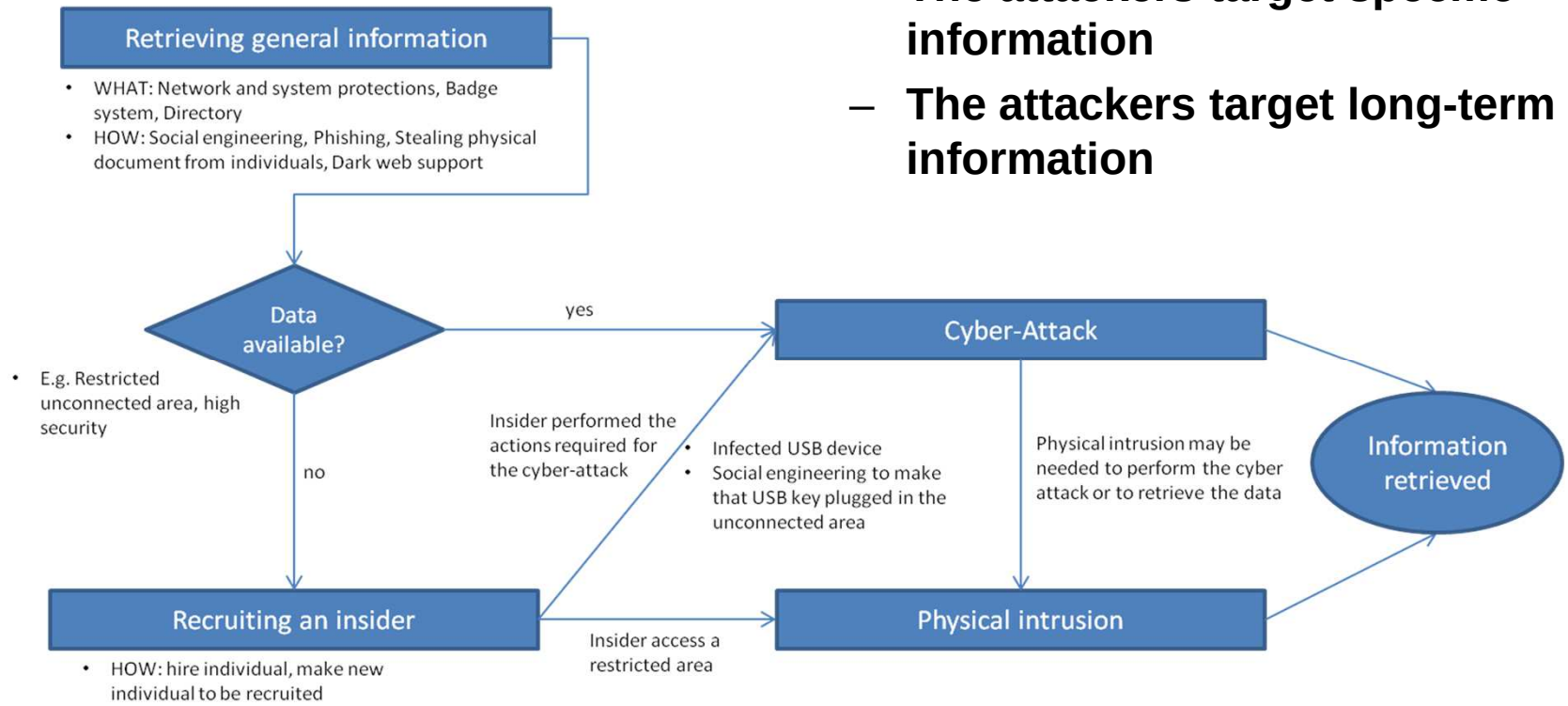
Use Case 2 – Actors and Assets

- **Typology of sites**
  - Strategic offices / Technoparks
  - Highly Critical Sites / Power Plants



UC2 – Sub Case 1: Industrial Espionage

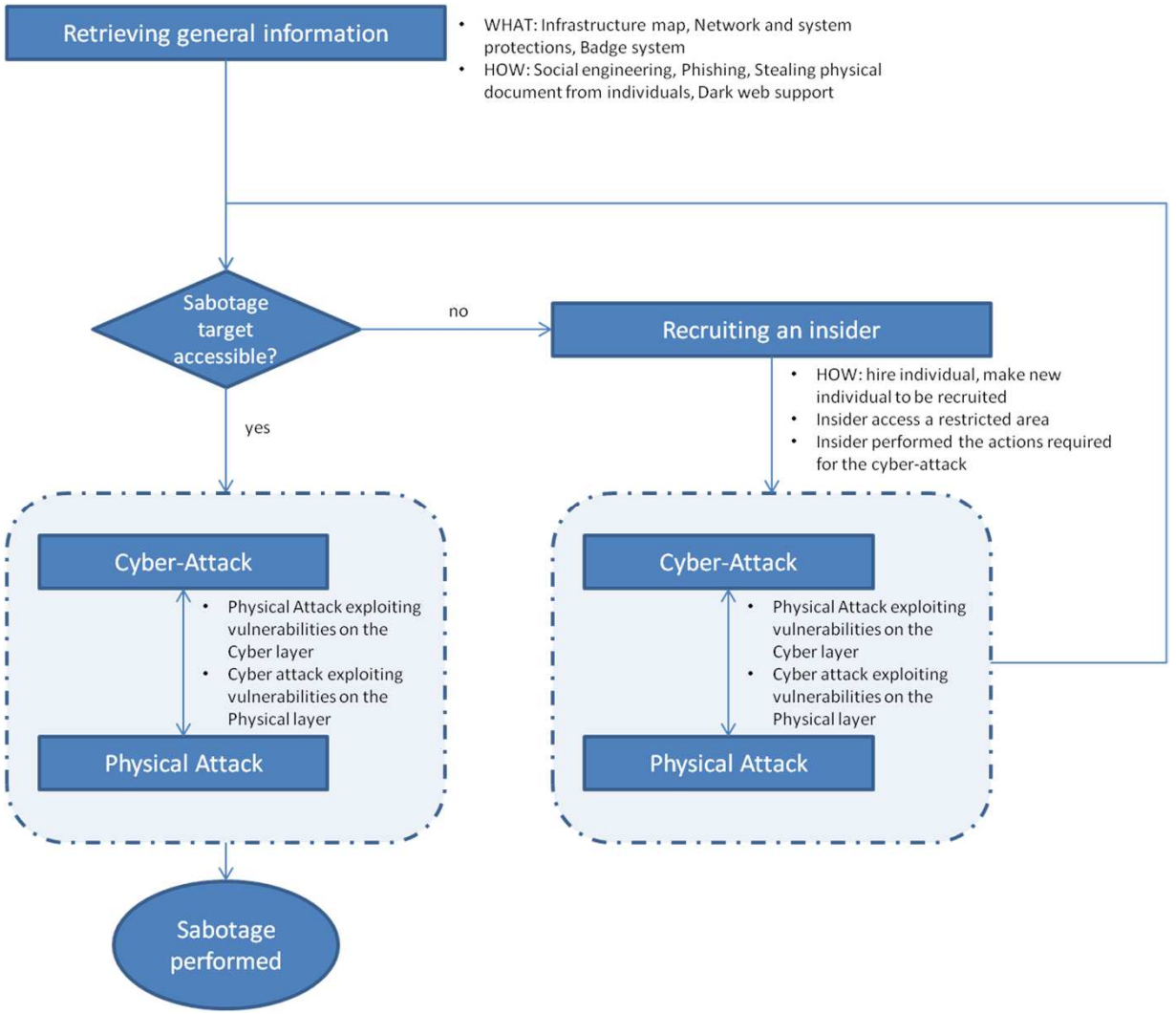
- **Workflow**



- **Instances**
  - **The attackers target specific information**
  - **The attackers target long-term information**

UC2 – Sub Case 2: Sabotage

- **Workflow**
- **Instances**
  - **Aramco scenario**
  - **Turkey oil pipeline scenario**
  - **German steel factory scenario**



Use Case 2 – Key features

Key Features	SC1 Inst. 1	SC1 Inst. 2	SC1 Inst. 3	SC2 Inst. 1	SC2 Inst. 2	SC2 Inst. 3
End-Point protection		X	X	X		X
Detection agent	X	X	X	X		X
End-to-end security		X	X	X		X
Role-based access management	X	X		X	X	X
Policies	X	X		X		X
Separation of power	X	X	X			
Separation of activities	X	X	X	X	X	X
Correlation physical security and logical security	X	X	X	X	X	X
Physical access control management	X	X		X	X	
Logical access control management	X	X	X		X	X
Adaptation of operational procedures			X	X	X	X
Detection and identification	X	X	X		X	

UC2: GEOLOCATION EXPERIMENT

CCS (C. Ponchel)

Alert in Elancourt!
Scenario 1: Network Intrusion

1 Network Intrusion

Keelback Net IDS

2 Network Sec. Alert

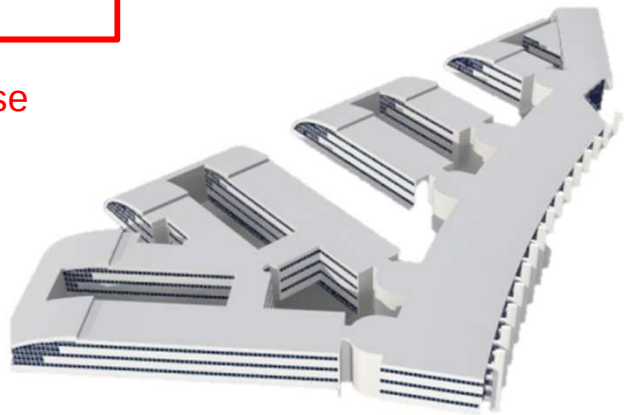
Cymerius Security Supervision

5 Investigation

3 Compromise

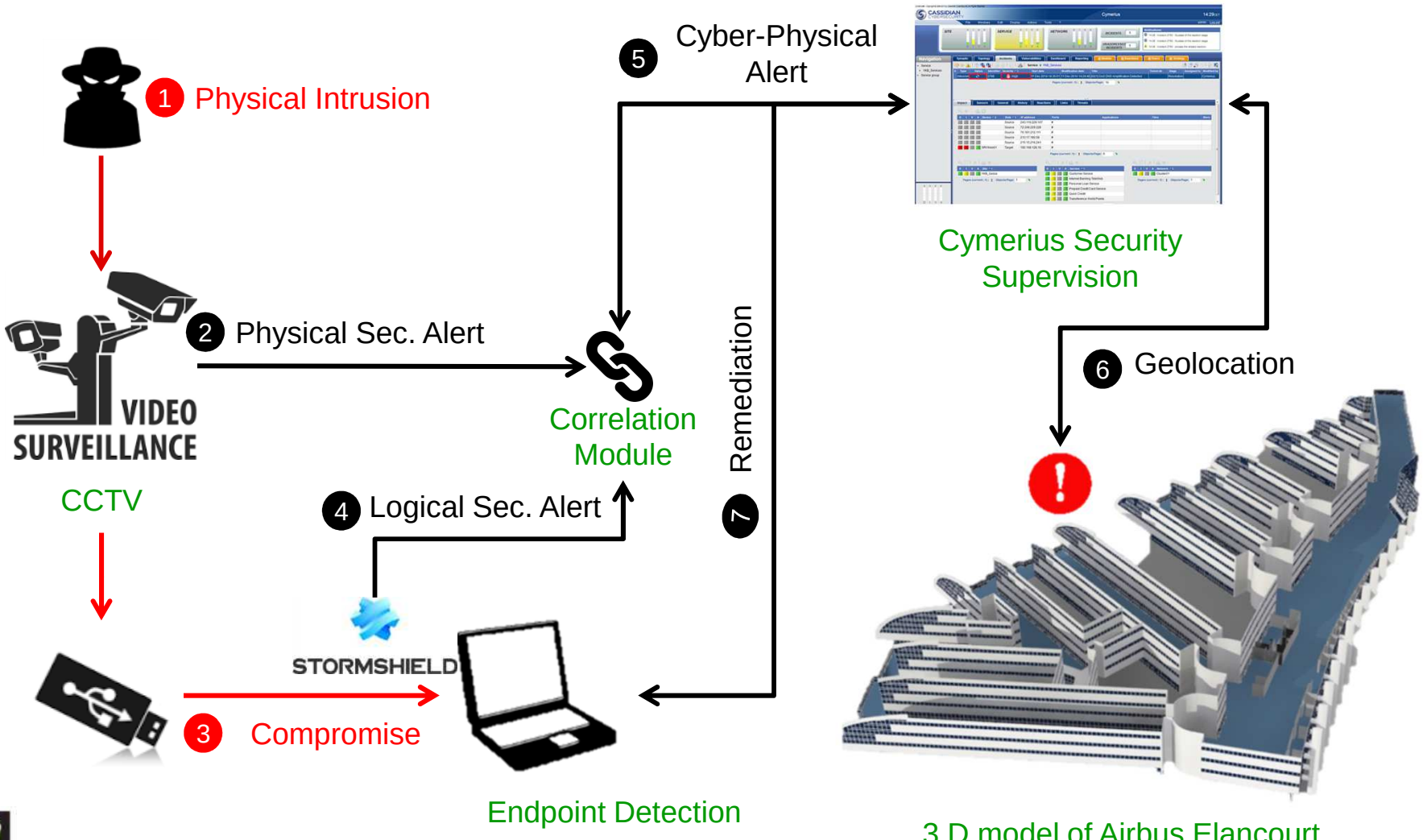
6 Remediation

4 Geolocation



3 D model of Airbus Elancourt

Alert in Elancourt!
Scenario 2: Cyber-Physical Attack

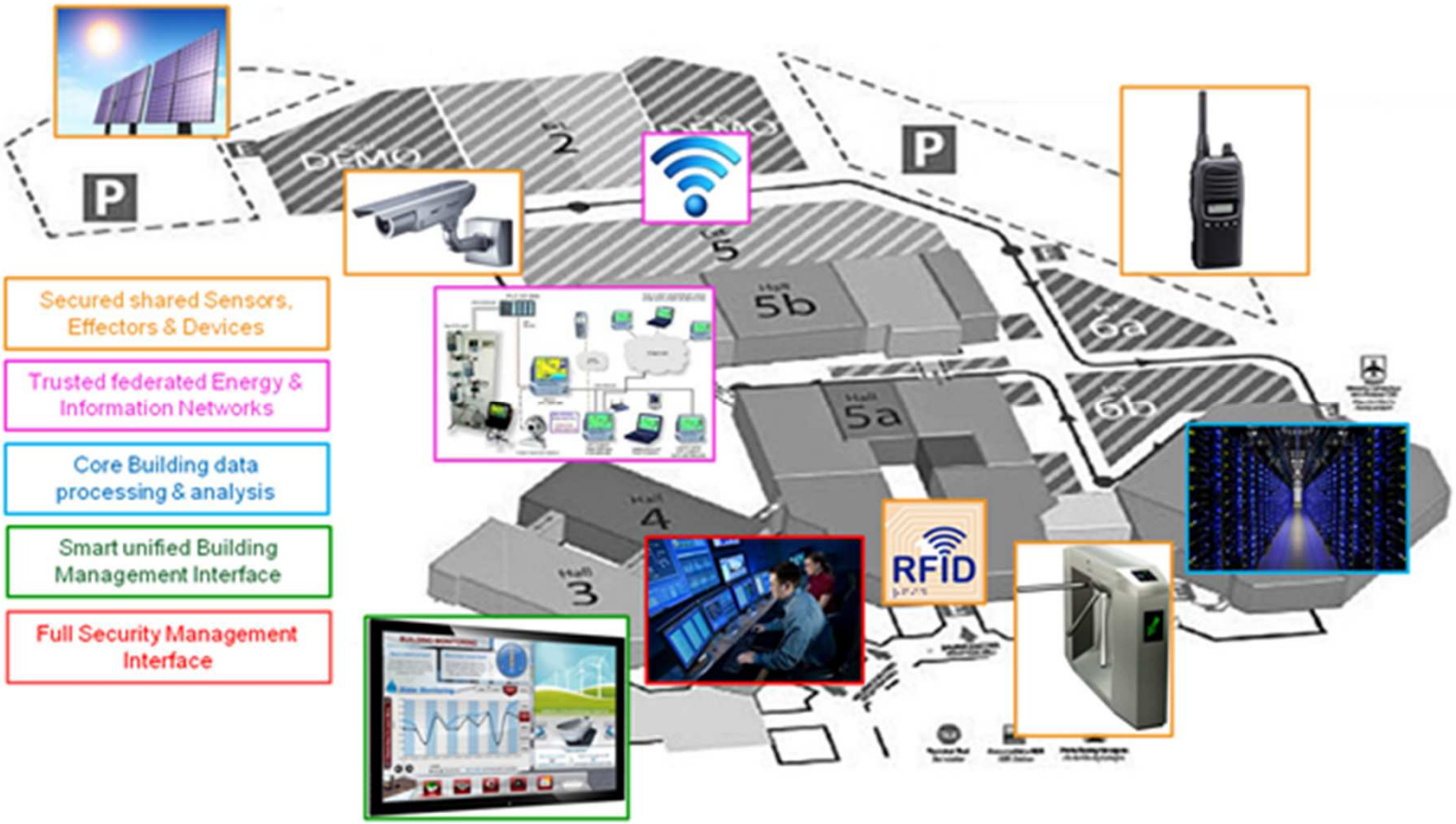


UC3: BMS SUPPORTING A TEMPORARY EVENT

ARC/EISIS (B. Istasse)

UC3: BMS supporting a temporary event

Use Case 3 stands for final FUSE-IT demonstrator with international impact,

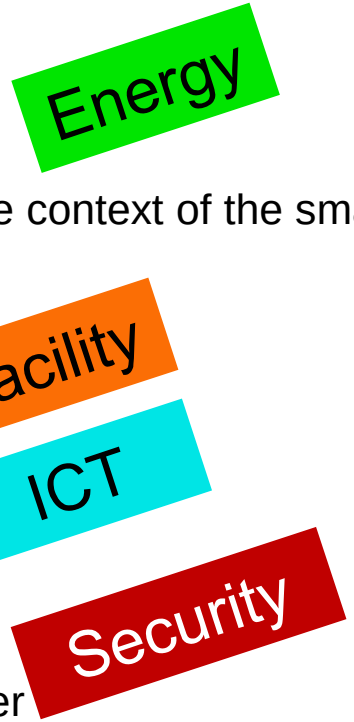


UC3: BMS supporting a temporary event

- **Focus**: smart secured and temporary equipment of a complex building for a big event.

- **Objective**: facilitate the deployment of systems and services for buildings that require frequent readjustments or organize events based on flexible configuration and reconfiguration of the facilities.

- **Key operational challenges**:
  - Changing operating conditions of the buildings in the context of the smart grid
  - Management of local energy sources
  - Load management in multi-agent environment
  - Heating, ventilation & Air conditionning
  - Self-reconfiguration of smart sensors
  - Self-authentication of smart sensors
  - Physical access management to restricted areas
  - Enforcement of anti-espionage policy
  - Interfaces between event organizer and booth-holder



Temporary event management: methodology

Event management

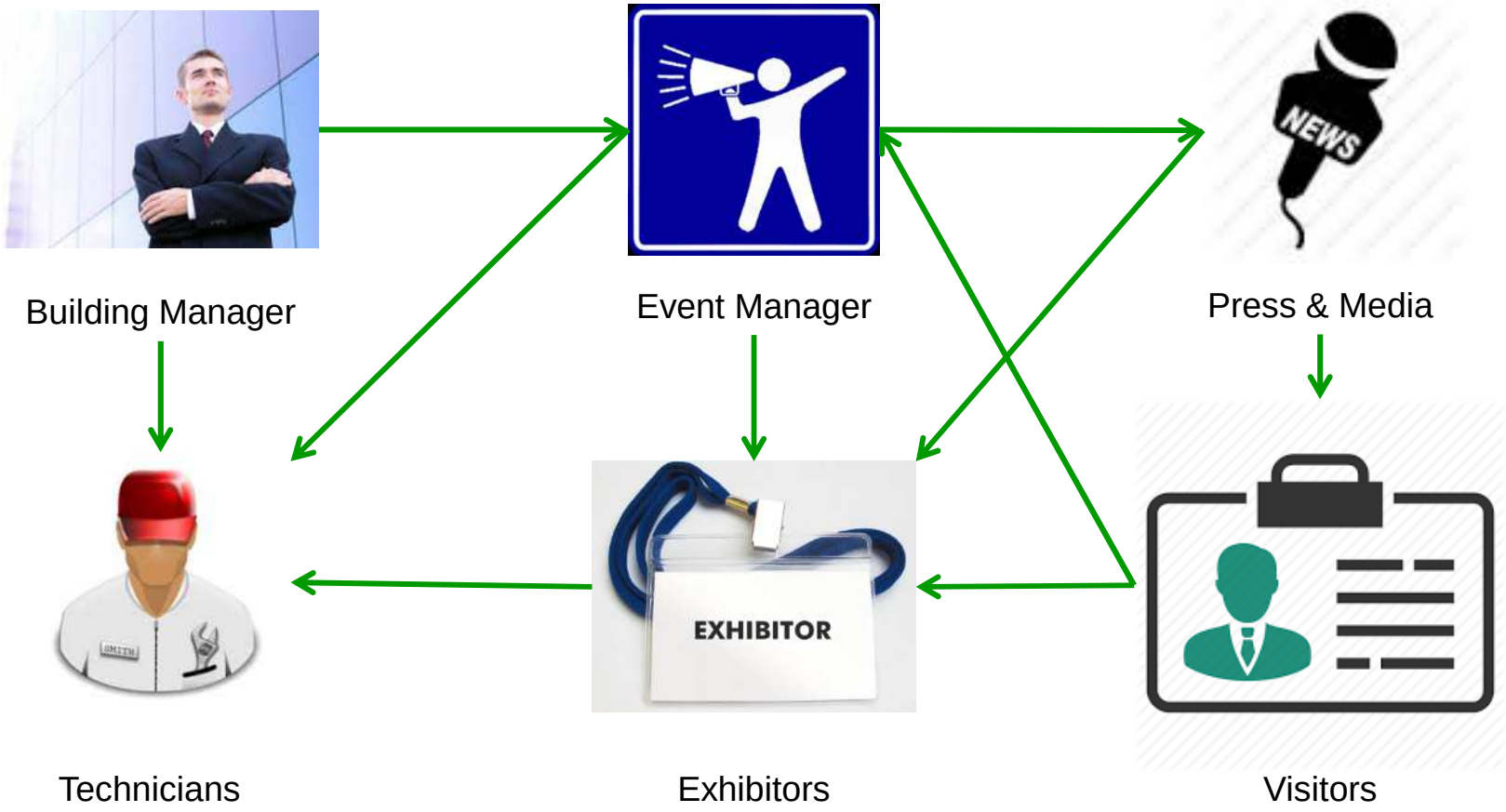
Type of Event (periodic event, independent event, …)

Type of building (from multi buildings and large buildings to small buildings, …)

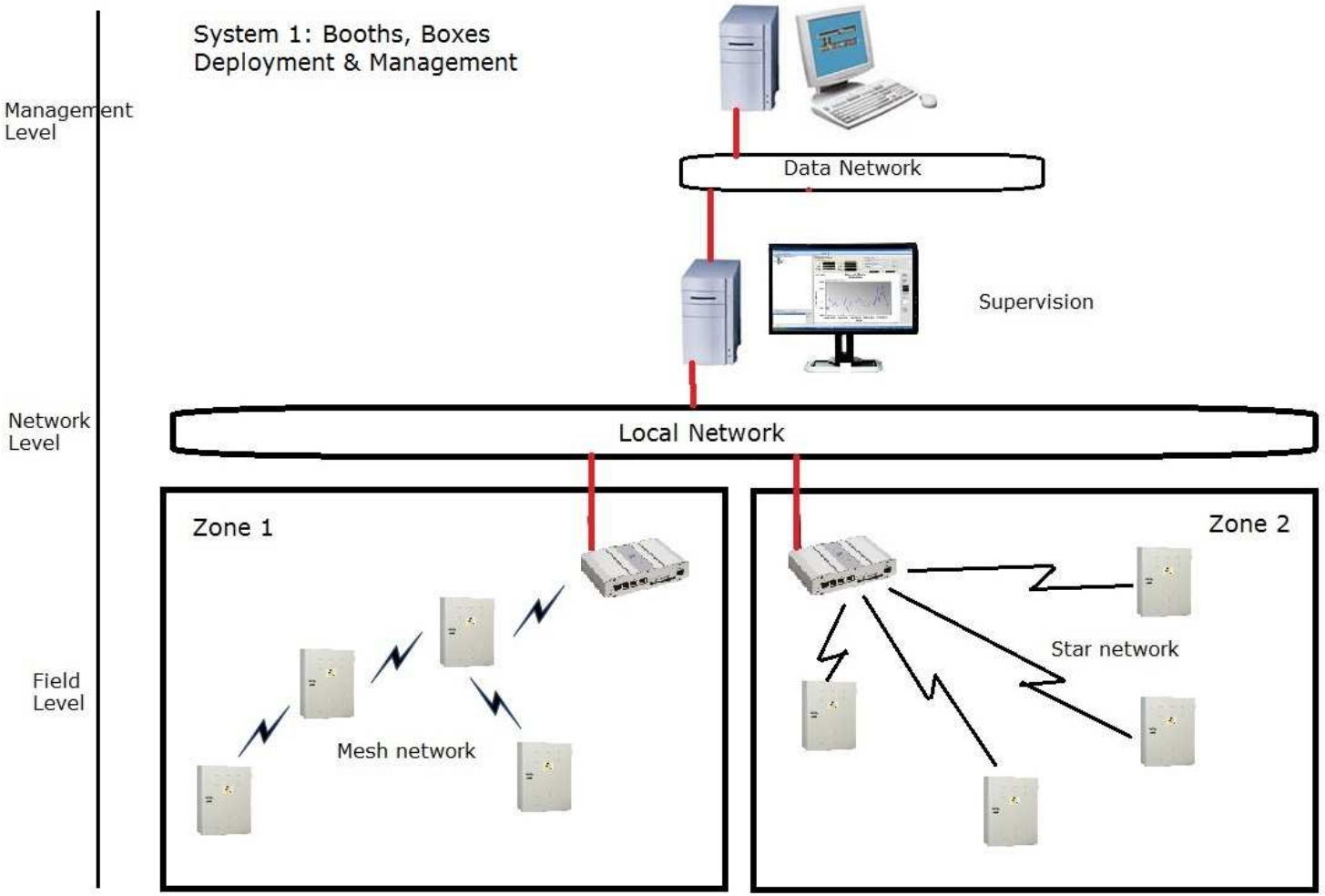
Type of managed resources
HVAC, Lighting, Lifts, Escalators, Security, Fire, Safety, Electrical, Water, …, ICT & sensors

Planning	Scheduling	Installation &Running	Dismantling
Resource Ident. • Historical data, previous event, New data (KPI, consumption, occupancy profiles, … • Actors prediction • Prediction (modeling, simulation,) Contract & Subcontract plan	Design, Integration, Configuration of existing installation (i.e.: space, zone and setpoint configuration) • Commissioning • Control & analysis	Supervision and Control •Management, •Monitoring •Abnormal operation •Analysis	Supervision and Control •Management, •Monitoring •Abnormal operation •Analysis
Horizon & Time Week(s), Month(s), Year(s)	**Horizon & Time** Day(s), Week(s), Month(s),Year(s)	**Horizon & Time** Days(s), Real time, Batch analysis	**Horizon & Time** Days(s), Real time, Batch analysis

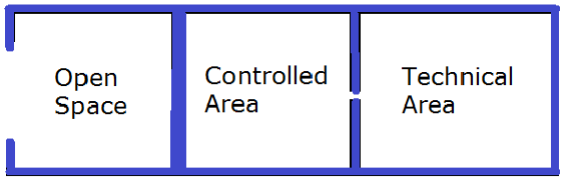
Actors

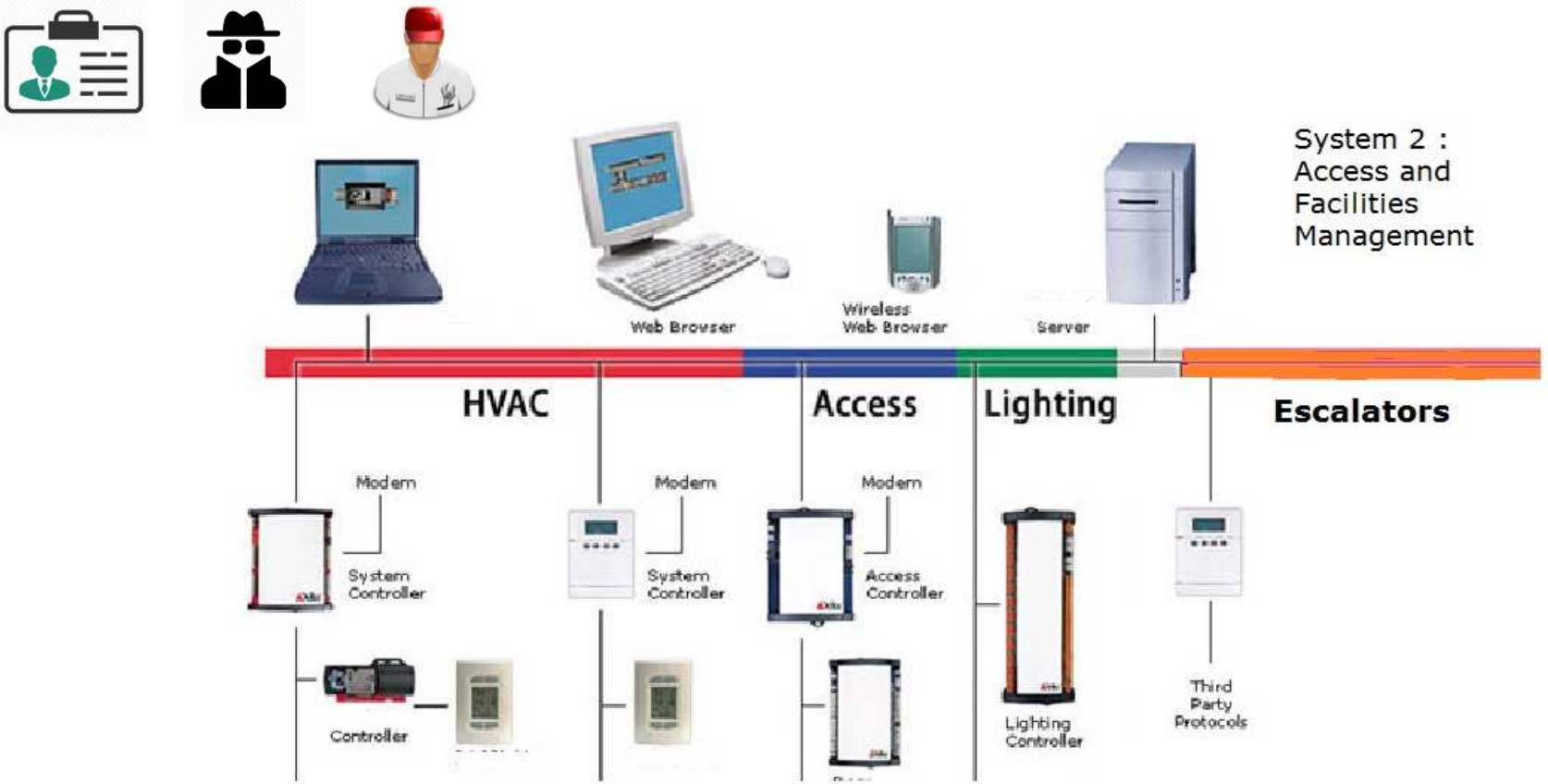

Building Manager
Event Manager
Press & Media
NEWS
EXHIBITOR
Technicians
Exhibitors
Visitors

SC1: Booths, Boxes Deployment & Management

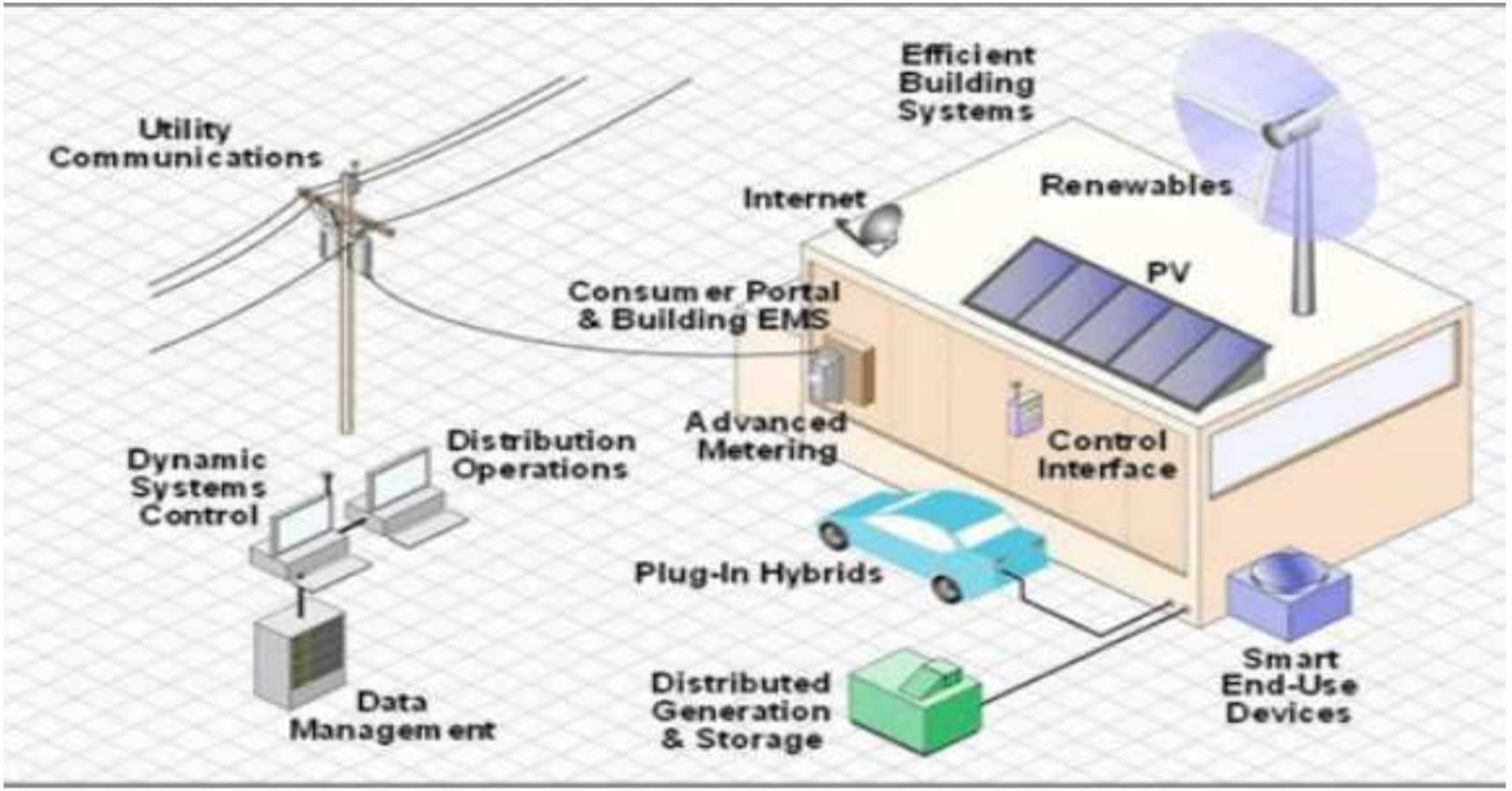


SC2: Access control and Facility Management





SC3: Control of Energy resources



Source: PIER - Public Interest Energy Research

UC3-SC1: BOOTHS & BOXES EXPERIMENT

SOGETI (D. Excoffier)

UC3: Booth & Boxes Experiment

A fully autonomous, secured & decentralized IoT Gateway

- **Challenge :** Creating the first fully autonomous, decentralized and secured gateway (for Boothes&Boxes, but not only).

- **Features: Create a new generation** of gateway able to:

- Be **a common building block**, able to evolve with any ecosystem of devices & datamodels (whatever the Use Case involved in).

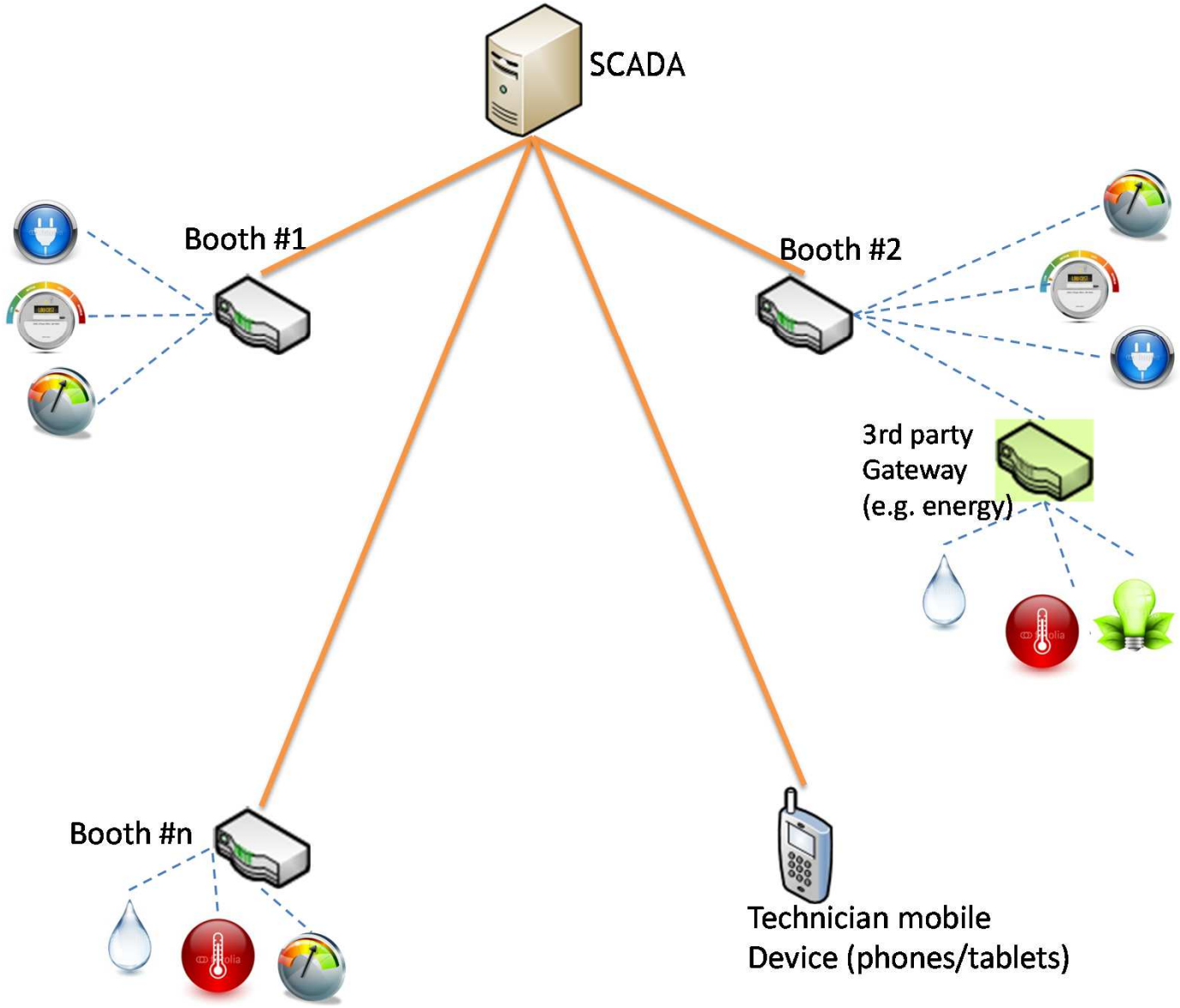
- Offer **full interoperability for all protocols and any kind of sensors**, actuators, or industrial devices (e.g. energy gateway) whatever protocols used (legacy, current, future).

- **Provide unification** of these heterogeneous ecosystem of devices (unification of data, services…)

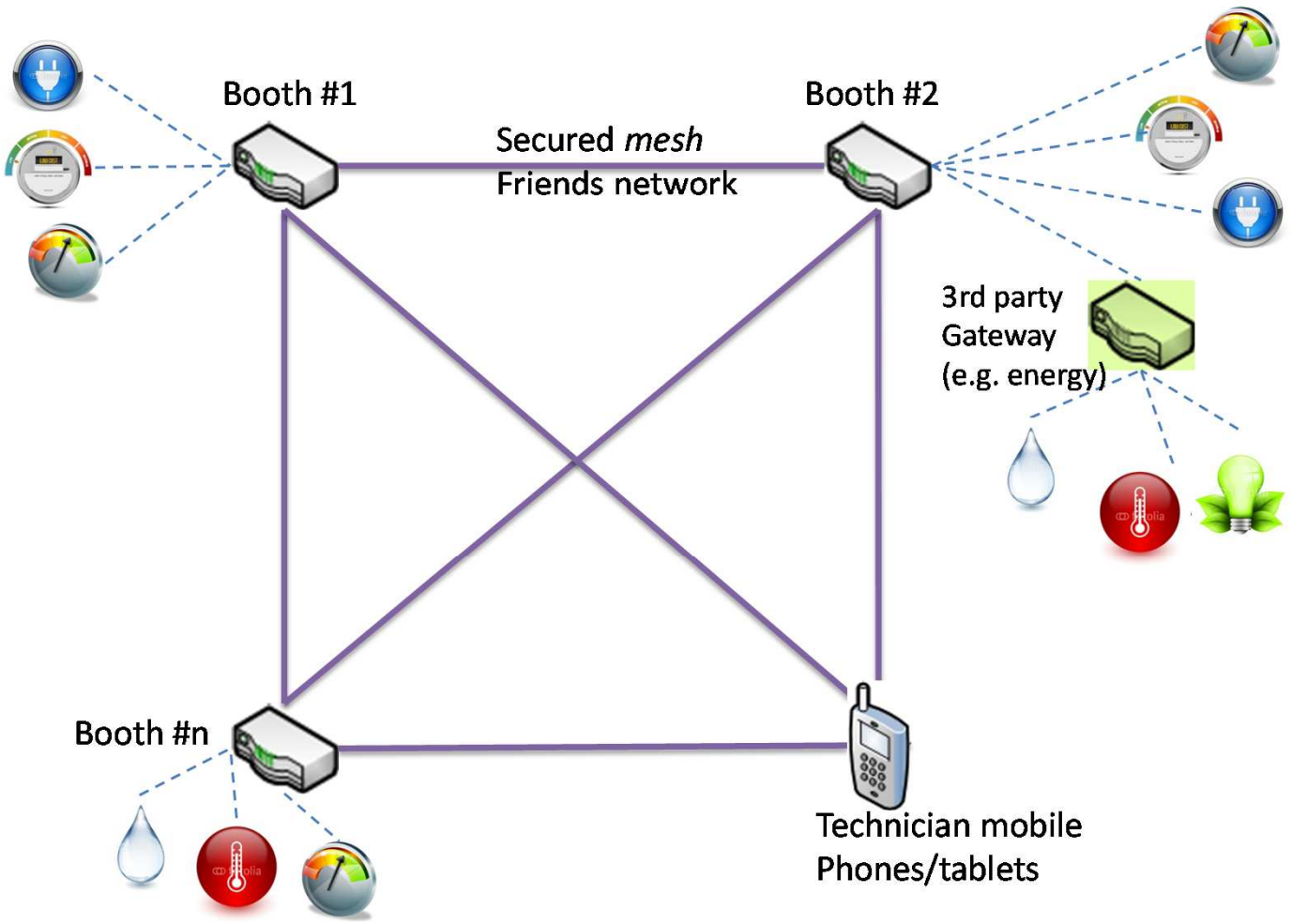
- **Allow real time data acquisition** from its ecosystem of sensors & devices

- **Communicate in a fully secured decentralized way** with a SCADA but also with all trusted "friends" devices (gateways, mobile devices, smart sensors,…):
  - Auto-discovery without no prior user config. of all other FUSE-IT gateways in the network.
  - Ensure that every discovered gateways are "friends" and have the right to communicate
  - Provide a decentralized way of communication: Does not rely on remote server(s).

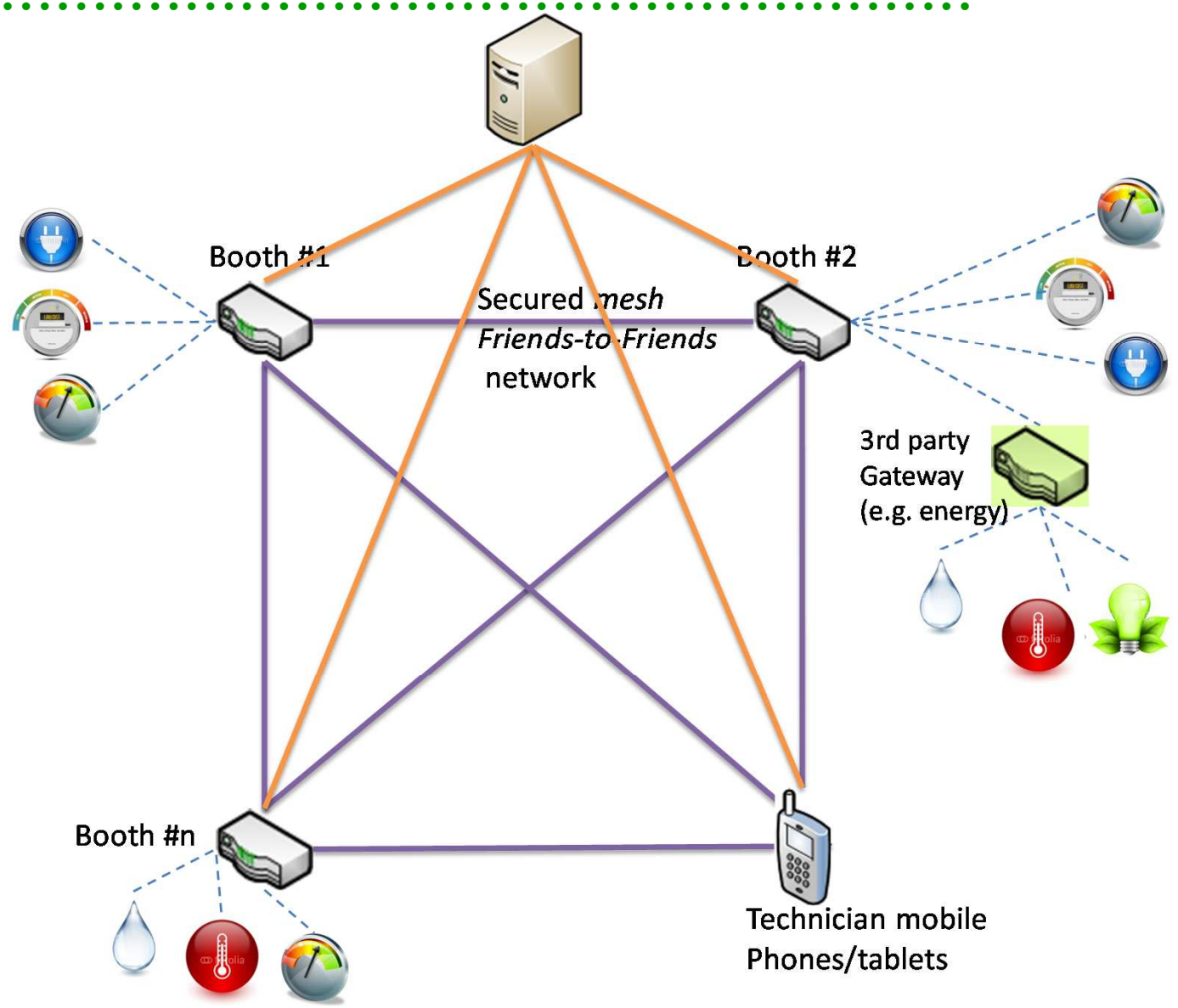
Creating IoT secure channel



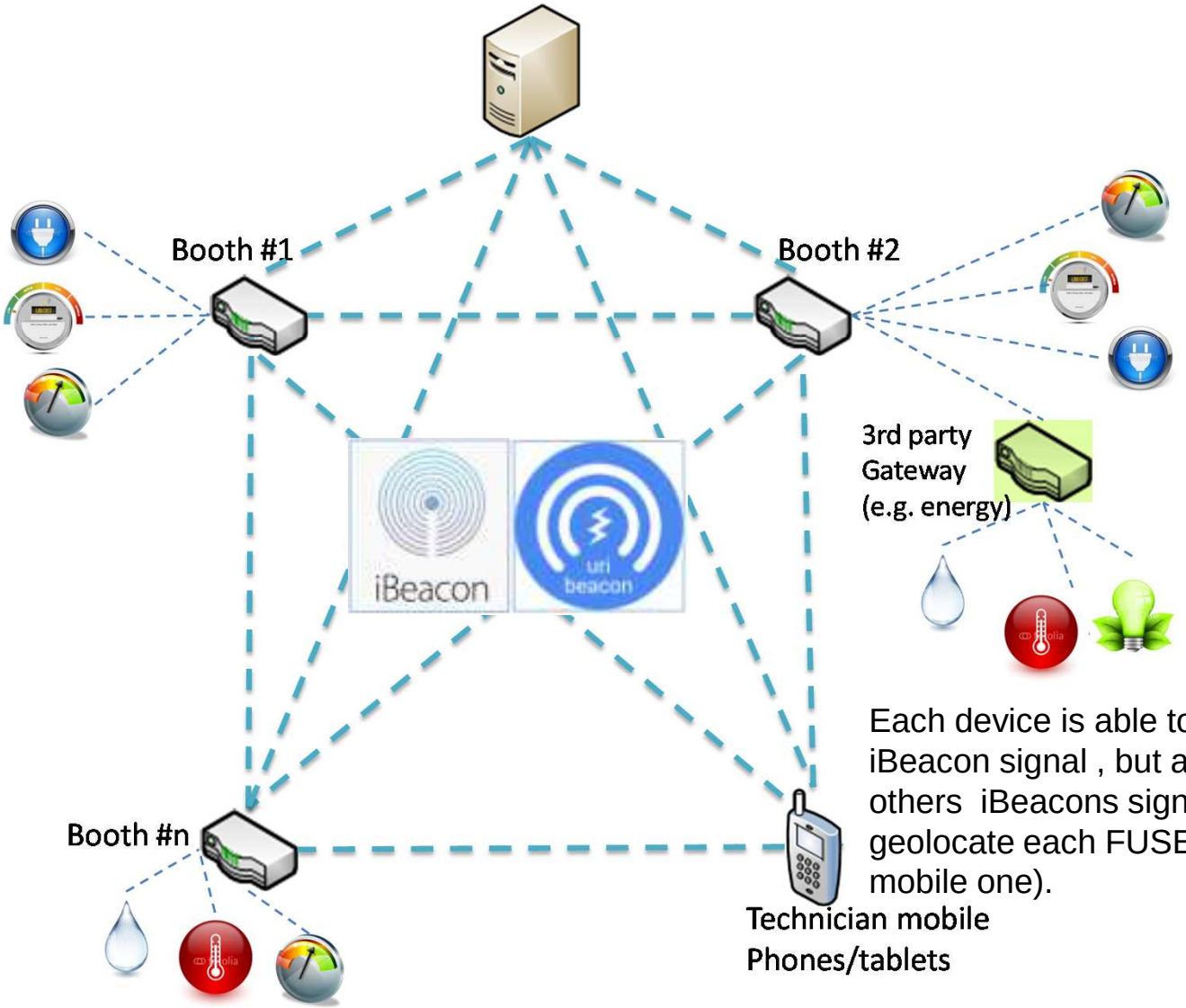
Create a fully autonomous decentralized secured network



Create a fully autonomous decentralized secured network

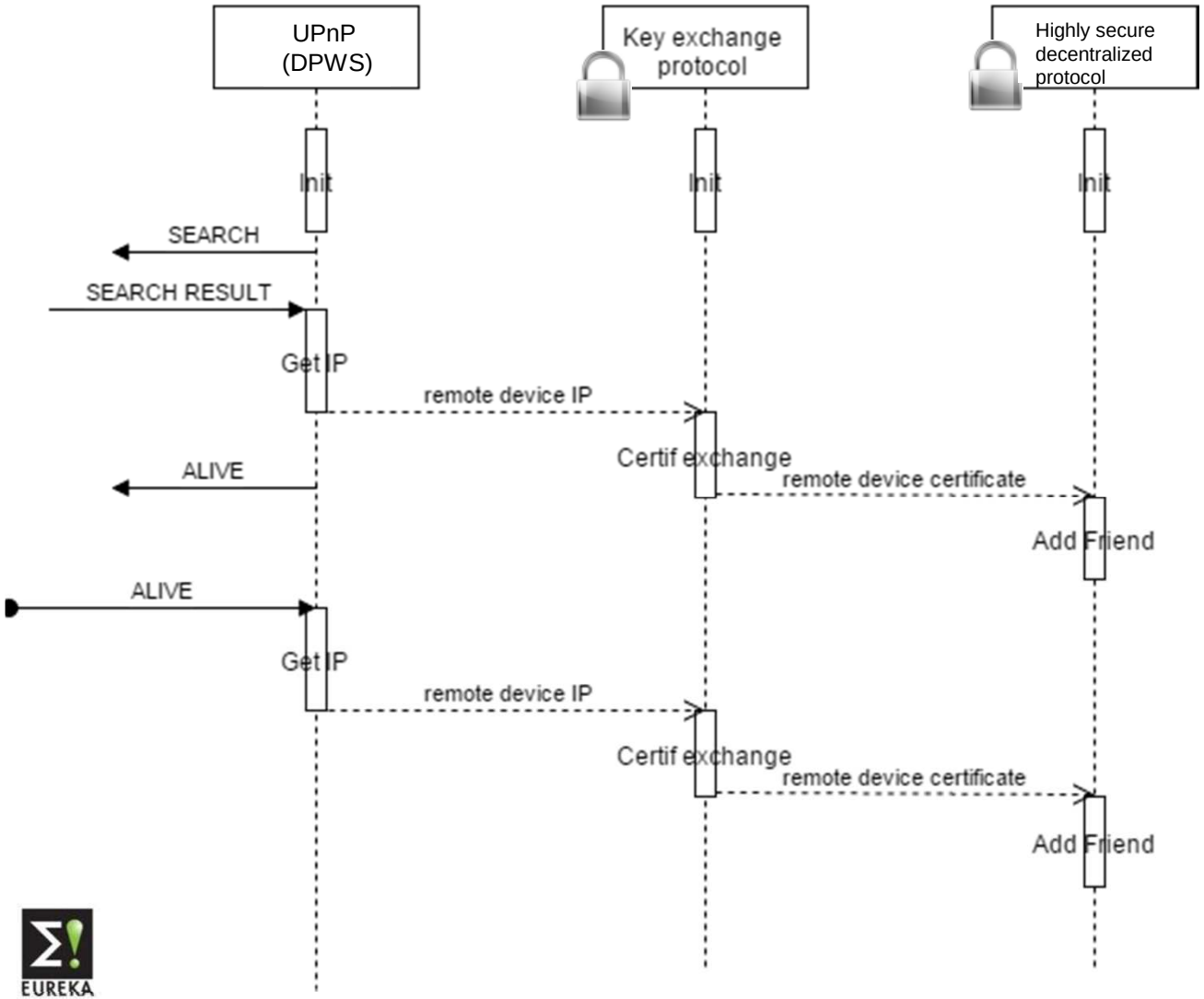


Indoor geolocation capabilities



Each device is able to send its own iBeacon signal , but also can receive all others iBeacons signals available, to geolocate each FUSE-IT devices (even mobile one).

Global flow-diagram



I. **Auto-discovery -** Autonomous devices discovery (SSDP discovery & UPnP device metadata exchange)

II. **Auto-configuration -** Secured Key exchange protocol

III. **Auto-adaptation –** RetroShare secured decentralized peer-to-peer communication (developed for PC, but used in this project in embedded system)

COMMON INFORMATION BASE & KPIS

EISIS (B. Istasse)

Common Information Base & KPIs

KB-based, Multi-Objective Optimization, Multi-Criteria Decision Aid, etc.

WP3 contributors

State of the art, Risk analysis, ETSI, SEAS, ISO31000, STRIDE, etc

High-Level Requirement matrix (D3.2)

UC 1 – Adaptive Energy Demand Response

UC2 – Reaction to a cyber-physical attack

UC3 – Temporary BMS supporting a major Event

WP2 contributors

Energy Management KPIs

Facility Management KPIs

Cyber and Physical Security KPIs

ICT KPIs

FUSE-IT Innovation

KPI Synthesis

Examples in the document, more to be defined in WP6/7

Common Information Base

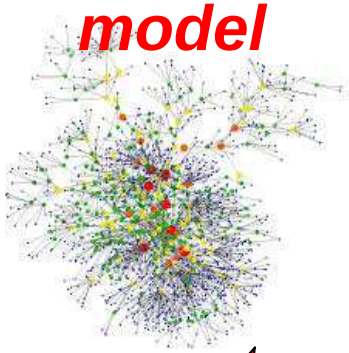
Project options for Ontologies

KPIs : metrics and data

- Energy Management
- Facility Management
- ICT Management
- Security Management

- FSGIM (Ashrae)
- SACM (ITEF)
- SEAS Data model (Sofia)
- OneM2M
- BIM model
- XORCISM
- ENISA

FUSE-IT Information model

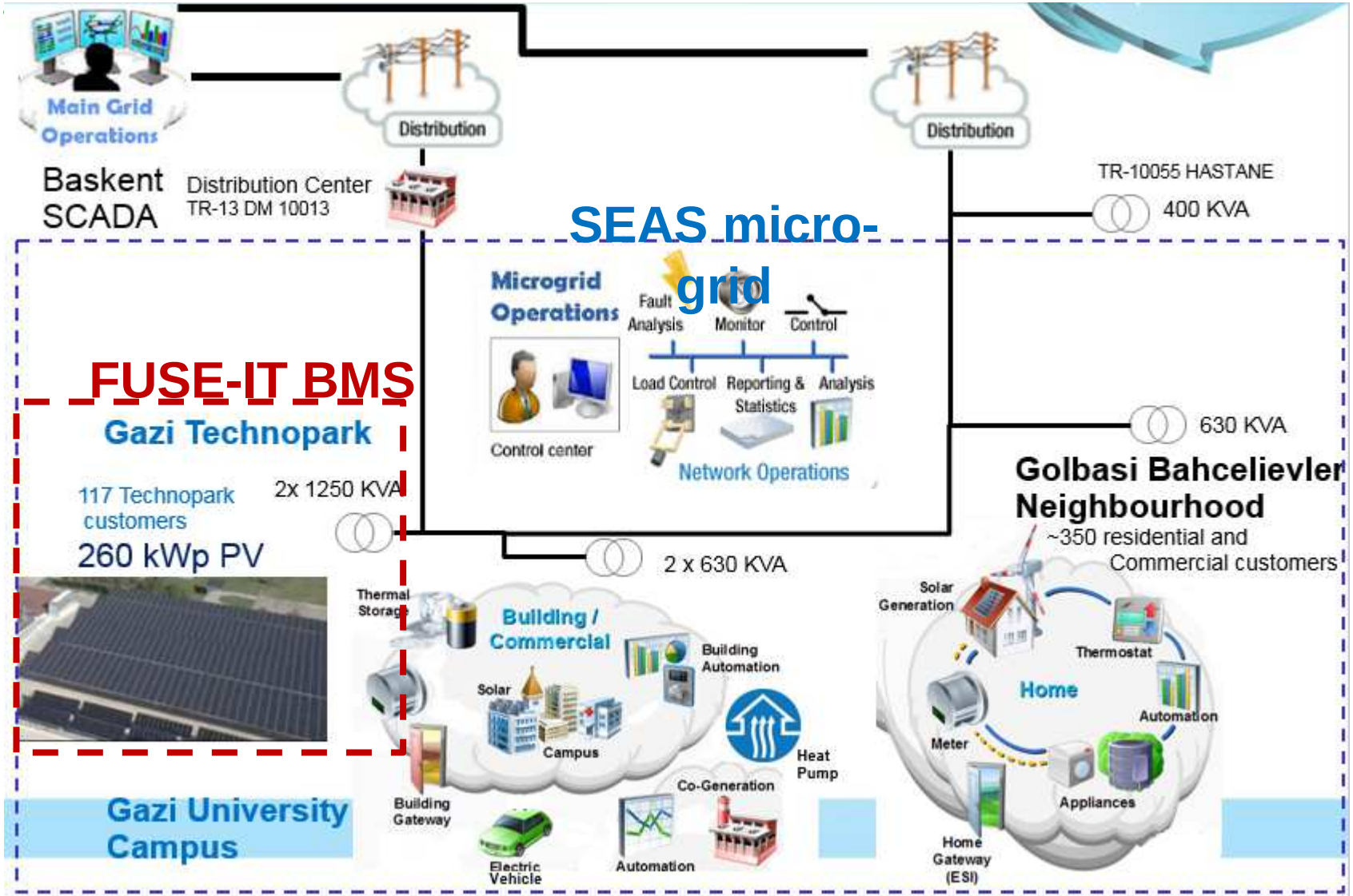


FUSE-IT November workshop

JOINT DEMONSTRATION WITH SEAS PROJECT ON GAZI TECHNOPARK

ICAM (L. Belhaj)

Joint Demonstration



Gazi Technopark

Validate and assess compliance with operational needs through use-case demonstration

One of the first and largest Installation producing electricity from solar energy

→ 118 companies/810 employees

Electric Vehicle Charging Station powered by Solar Energy.

Baskent (SEAS)
Energy Distributor

Capabilities Now

- ✓ **260 kW peak PVs already connected to grid** (PVs & inverters benchmark)
- ✓ **Feeding the campus area from two distribution transformers as a ring topology** (for islanding case- dispatching from two TRs)
- ✓ **Distribution transformers are already managed by SCADA**
- ✓ **117 techno park customers:** IT industry and etc.)
- ✓ **Eligible customers availability**

Microgrid Demonstration Center needs

→µCHP and additional PVs

→Storage units

→Smart protection relays

→Smart Meters and AMI

→Off-grid inverters

→Microgrid Control Center linked to the BMS

Useful for FUSE-IT Building Management System

Gazi technopark: Existing Equipment

- ✓ **230 kWp PVs already connected to grid**
  - ✓ **integration of additionnal 40 kWp**

Consumption: > 700kWp (peak)
- Week : production consumed locally
- Sundays: surplus sold to the grid

=> the PV is always connected to the grid.

- ✓ **Storage**

Installation of 20 – 25 kW storage, (ABB EssPro): **March / April 201**6

Gazi technopark: Confirmed Equipment

✓ EVs:

- 18 EVs rented for other project
- 1 charging point already implemented in the demonstration area

✓ AMI:

- 30 smart meters from “Silver Spring Network”, USA : free of charge - proof of concept - for the 3 buildings of Gazi Technopark
- 20 smart meters from Itron
- 200 old meters customized through Engie (LoRA, Sigfox…) mainly for the residential area
- 5 power quality devices from Schneider

Gazi technopark: available data

Single customer for distribution network for Enerjisa: monthly billing

✓ Sub-billing:

- Gazi divides bill for each company according to total monthly billing
- Gazi has sub-meter for each company

✓ PV Generation:

Gazi has data each 10 or 15 min for multiple inverters (SMA) for different arrays of different PV vendors

✓ Weather conditions measurements:

- Existing Meteorological measurement station in Gazi technopark.
- A startup company located in Gazi Teknopark, focusing on meteorological data and forecasting services.

Gazi technopark: ambition

✓ Gazi technopark islanding mode:

- Not legal (No regulation rules)
- Can be tried for the project
- Needs additional equipment: SCADA/RTU in Gazi Teknopark Transformation Substation, breakers, off grid inverters etc.

SCADA/RTU data:

- motion and door alarms,
- transformer faults (temperature, oil level),
- feeder switch positions,
- reactive/active power,
- voltage and current measurement etc.
- G.SHDSL (VPN solution) local telecommunication network between field and Main Control Center.

Gazi technopark: ambition

→ FUSE-IT additional components for BMS demonstration

- Access control system/cameras
- Smart sensors
- Cyber assets: servers, network devices

→ FUSE-IT demonstration objectives (Gazi-MOSBIT contract)

- Information model by using FUSE-IT user interfaces
- FUSE-IT KPIs by using information model
- Anomaly detection by using Cyber-Physical event correlation based on information model

QUESTIONS ?
COMMENTS ?