Panel Energy: How Optimal Are The Current Energy Systems
From a security point of view

Chakib BEKARA
Fraunhofer FOKUS Institute
Berlin, GERMANY

Security Issues in the SG (1/4)

- The Smart Grid is a **Critical Infrastructure**. The use if **ICT** makes it a target to **Cyber-Attacks**
- Impact the **physical** power grid from the **cyber** world
- The SG aims to integrate commercial-of-the shelf hardware, non-owned network infrastructure and standardized protocols, even in the distribution and transmission parts of the power grid.
- Cyber attack?: Tuxnet virus which infected in 2010 an Iranian Nuclear Plant: the SCADA software of the plant running under Windows station
- Virus propagated through an infected USB key What happens if the SCADA system could be remotely accessed through a network?

Security Issues in the SG (2/4)

- The strictly and physically separation between the enterprise/IT network and the control (power) network could not be guaranteed.
  - If both networks share a portion of same communication infrastructure, or protections are not made to control moving from one to another, attacking the IT network leads to attacking the power network

- Control engineers awareness about security
  - Operating in isolated network in the past, control engineers were less concerned by security than IT engineers

- Several entry points to the SGs: smart meters, gateways, field sensors, etc.
  - Several potentials attacking points, with different consequences

Security Issues in the SG (3/4)

- A large amount of data will be exchanged in the future SG
- Data is the key success for the SG

- Impact of Data **Trustworthy** on the Smart Grid
- Sending fake low-prices during peak periods makes financial loss to customers, increases energy consumption, and may lead to energy outage.

- Performing a large-scale compromising attack against Smart meters/gateways by sending fake software update.

- Sending fake smart meters' measurements could result on financial loss for the energy provider, false load forecasting grid status estimation at the utility (under/over estimate energy consumption in the grid) and leads to energy outage.

Security Issues in the SG (4/4)

- Smart Meters introduce **Privacy** issues for the customer. The fine-grained measurements, allow the inference of new information:
  - Type and number of smart appliances in the customer's smart home
  - Energy consumption profile of the customer
  - Periods of presence/absence

- Controlling a Smart Meter or impersonating it, allow the control of the Smart Appliances in the Smart Home
  - Permanently running appliances (e.g., fridge) could be turned-off
  - Appliances critical for elderly persons or persons with special-assistance, could now be easily turned-off

Security Requirements for the SG (1/2)

- **Availability**
  - Systems and Data are available when required
  - E.g., Demand-response service availability
- **Authentication**
  - Ensure the **identity** that an entity claims to be/have
  - E.g., authenticate smart meters, gateways, utility, energy provider, etc.
- **Integrity**
  - Prevent transmitted/stored data from being illegally modified
- E.g., metering data and real-time prices integrity

Security Requirements for the SG (2/2)

- **Confidentiality**
  - Keep data **secret** from non-authorized parties
  - E.g., Individual energy consumptions should be accessible to the energy provider only

- **Customer's Privacy**
  - Ensure that **no data** related to a customer could be divulged or inferred without a prior and explicit approval from him
  - E.g., smart appliances inside home, local generation/storage capacity, presence/absence periods, etc.

Measuring energy efficiency of software applications

Luca Ardito

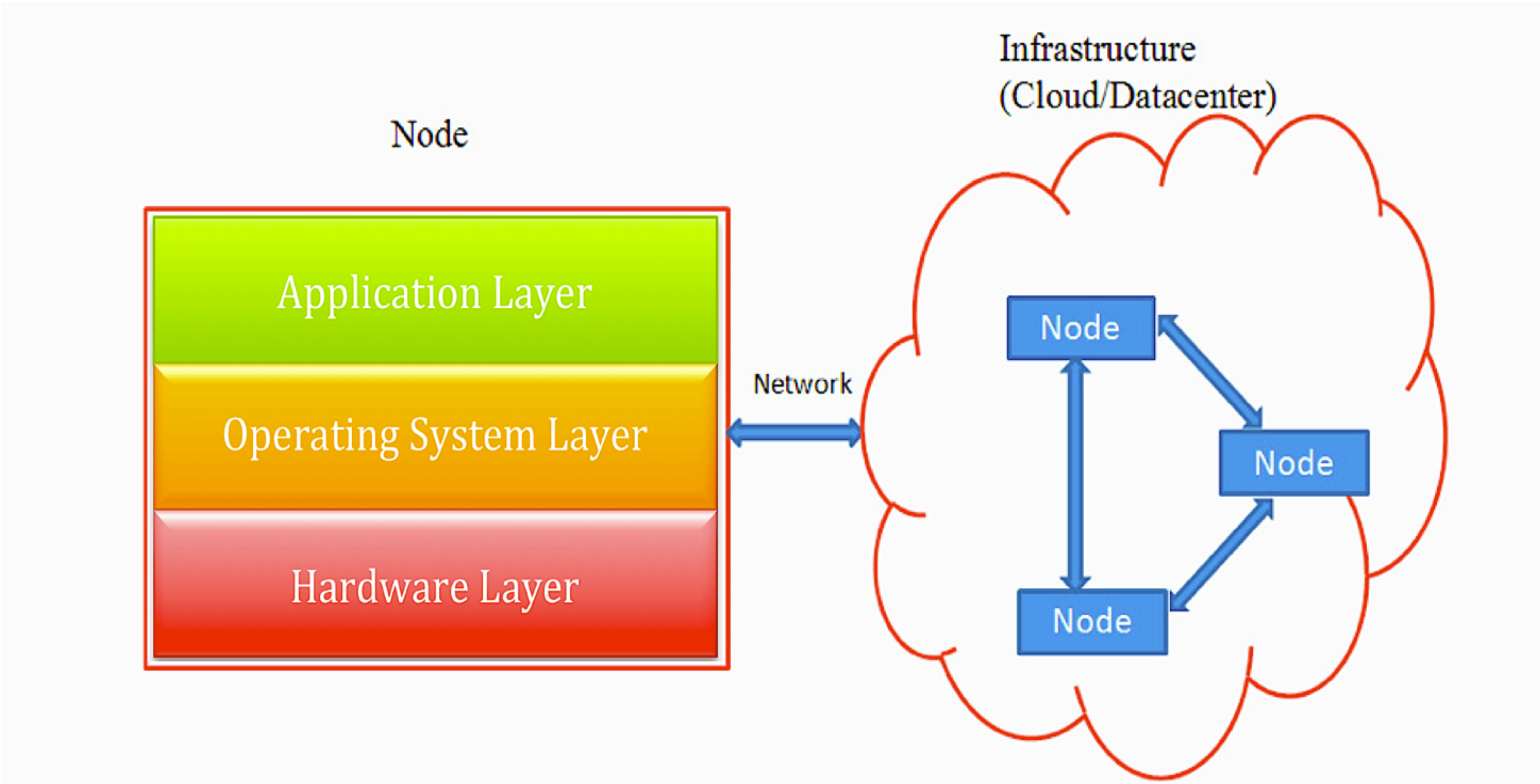
luca.ardito@polito.it

ENERGY 2012

Background

- The rapid growth and significant development of ICT systems has started to cause an **increase** of worldwide **energy consumption**
- In the field of ICT hardware manufacturers and designers have usually handled the problem, but recently **software energy efficiency** gathered the interest of industry and academic research.
- Writing **energy efficient software requires** proper **metrics** to evaluate it. The literature still lacks in defining energy related metrics.

Taxonomy



Node
Application Layer
Operating System Layer
Hardware Layer
Network
Infrastructure
(Cloud/Datacenter)
Node
Node
Node

Metrics

- We can summarize metrics into two broad categories:
  - **Efficiency**, as the **ratio** of useful energy and total energy used
  - **Productivity**, can be defined as **computational work done per resource** used. The resource is **energy**. Computational work needs to be defined at each level of the taxonomy. For instance: in a CPU, an example may be operations performed, in a network bits transmitted, in a web application hits managed, etc.

Modeling power consumption

- Can be done at **design level**:
  - Static analysis techniques to inspect the code
- Can be done at **run-time level**:
  - Energy Manager at OS Layer
  - Applications self adaptation
- **Need** to **define** and **validate** a comprehensive model capable of gauging the energy consumption of an application from the estimated usage of all components and devices, limiting the required instrumentation.

GREENS

Green and Sustainable Software

First International Workshop on Green and Sustainable Software

Workshop in conjunction with ICSE 2012

ICSE 2012

June 2-9, 2012

Zurich • Switzerland

http://greens.cs.vu.nl/

CHEMNITZ UNIVERSITY OF TECHNOLOGY

Panel Discussion

How Optimal are the Current Energy Systems?

– Energy Efficiency in Distributed Wireless communication Systems –

Dr. Matthias Vodel / Chemnitz University of Technology / Germany

vodel@cs.tu-chemnitz.de

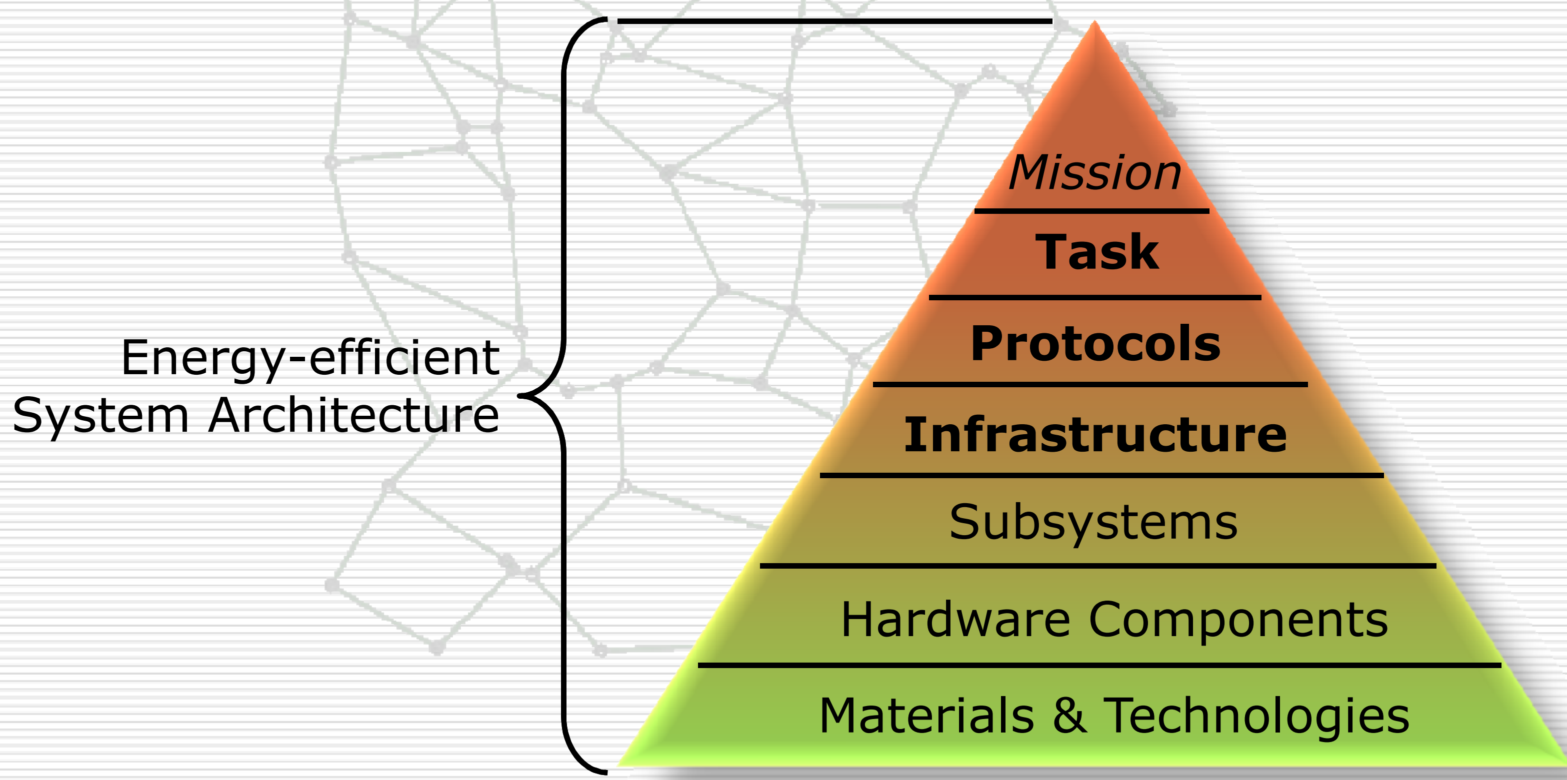
IARIA

- 2nd International Conference on Smart Grids, Green Communications and IT Energy-aware Technologies - ENERGY 2012

Let’s talk about “Energy Efficiency”

Differentiation: Product Life Cycle ⇔ System Runtime

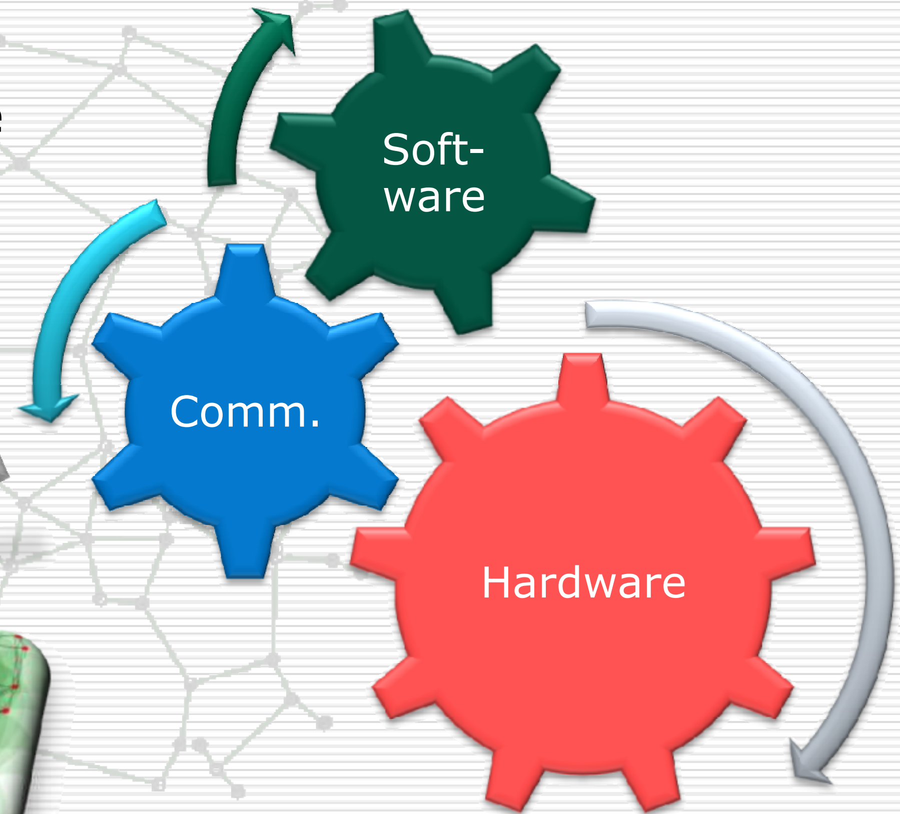
Definition & Level of abstraction (Distributed System):

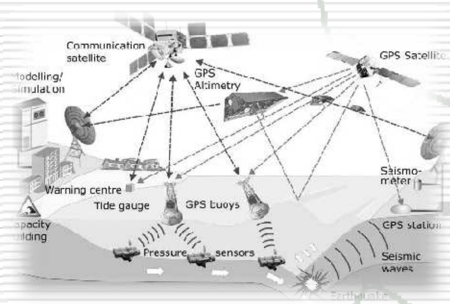


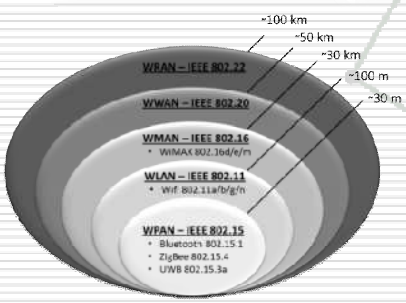
Approaches for Optimisation

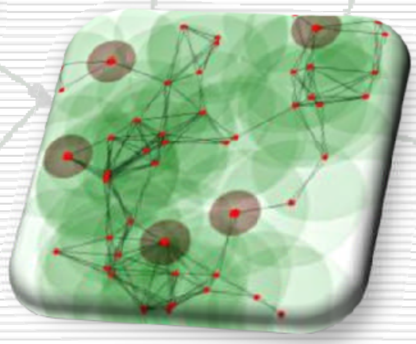
Focus on (suboptimal) communication aspects:

"Wireless challenges"
→ Trade-Off Security / Performance
→ Incompatibilities
→ Overhead / Inefficiency
→ Management & Scalability









“Pillars” of Energy Efficient Communication

- “Optimal” = Strongly application-specific
- “Optimal” = Trade-Off
- “Optimal” = Integration of different perspectives

➔ **“Optimal” ≠ “Optimal”**

Energy-efficient System Architecture

Communication Paradigms

Communication Technologies

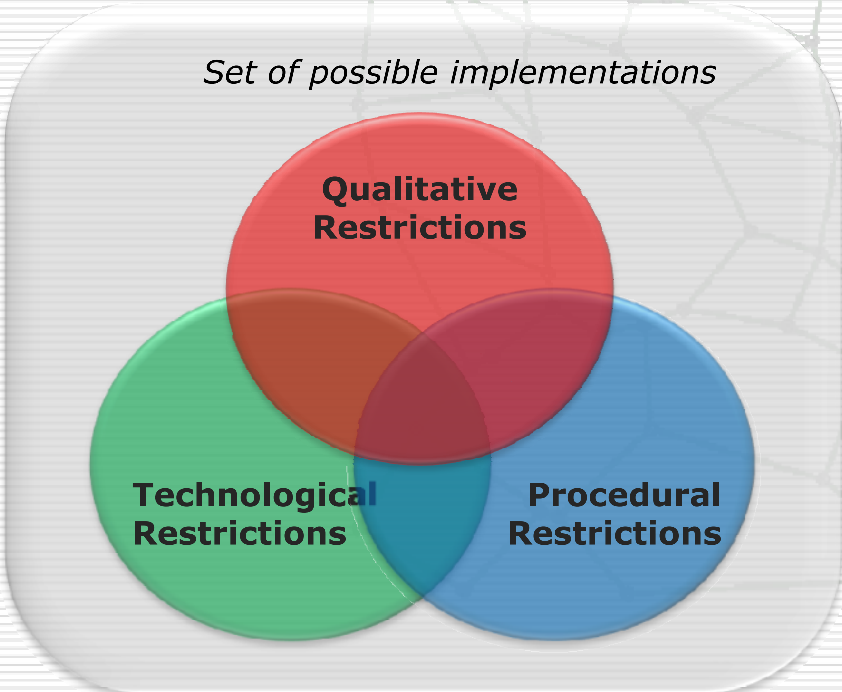
Communication Protocols

Basic Constraints & Requirements (functional & non-functional)

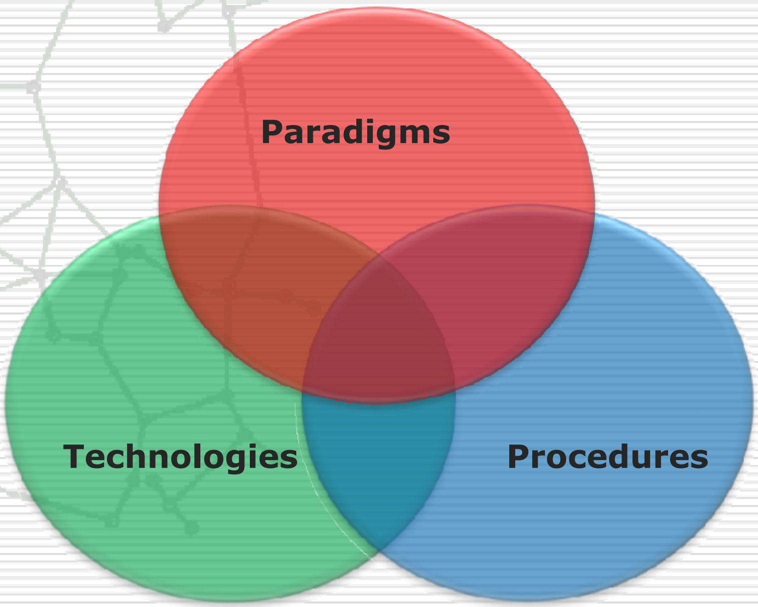
Energy-Efficient System Design

Design process is based on different principles:

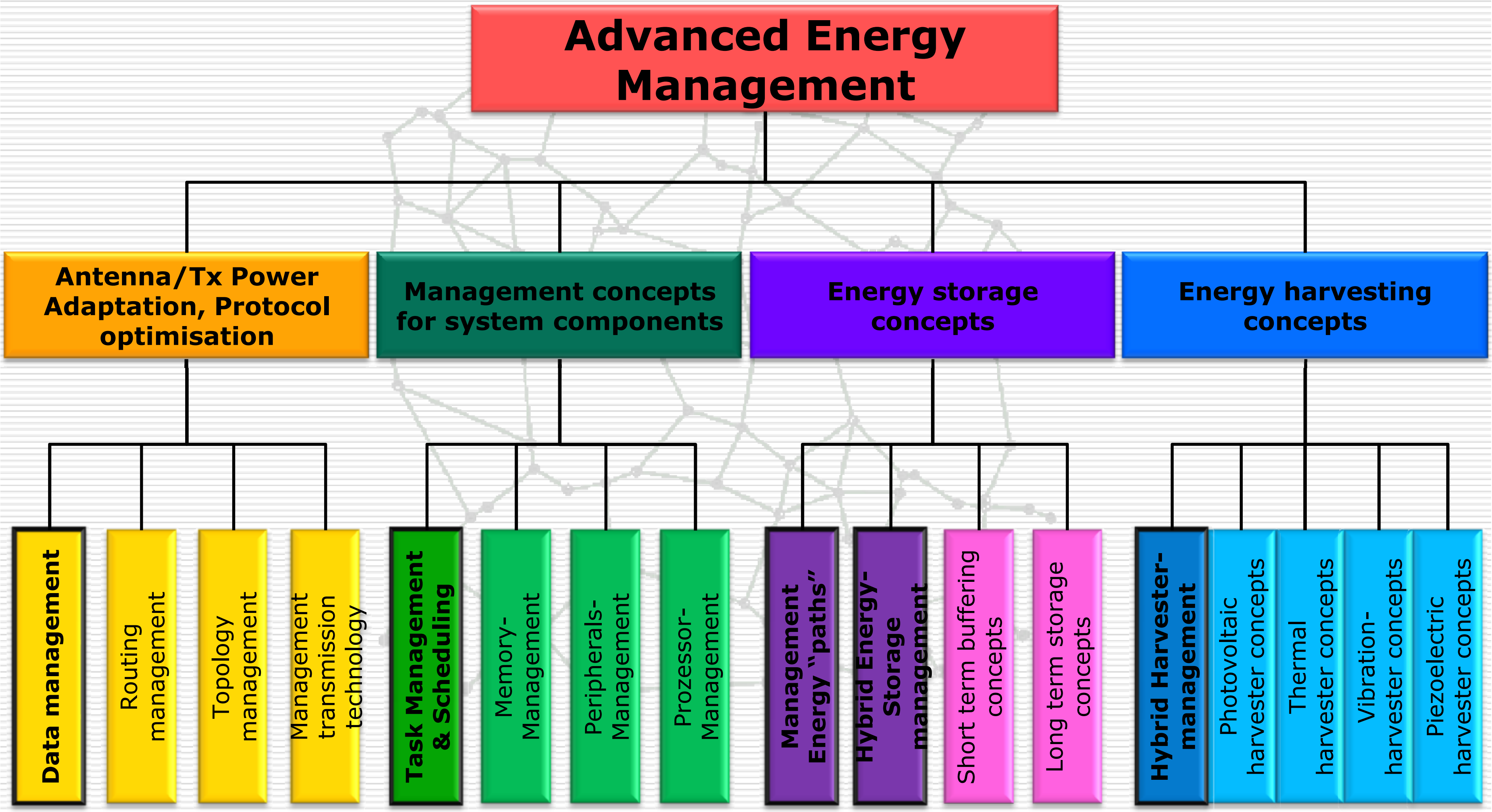
Narrow Down Approach



Build Up Approach



Research Objective & Vision



THANKS FOR YOUR ATTENTION

QUESTIONS …