Jose Emilio Rico
Epoche & Espri
tech@epoche.es

EPOCHE & ESPRI

Smart Meters

Security Problem definition

Common Criteria

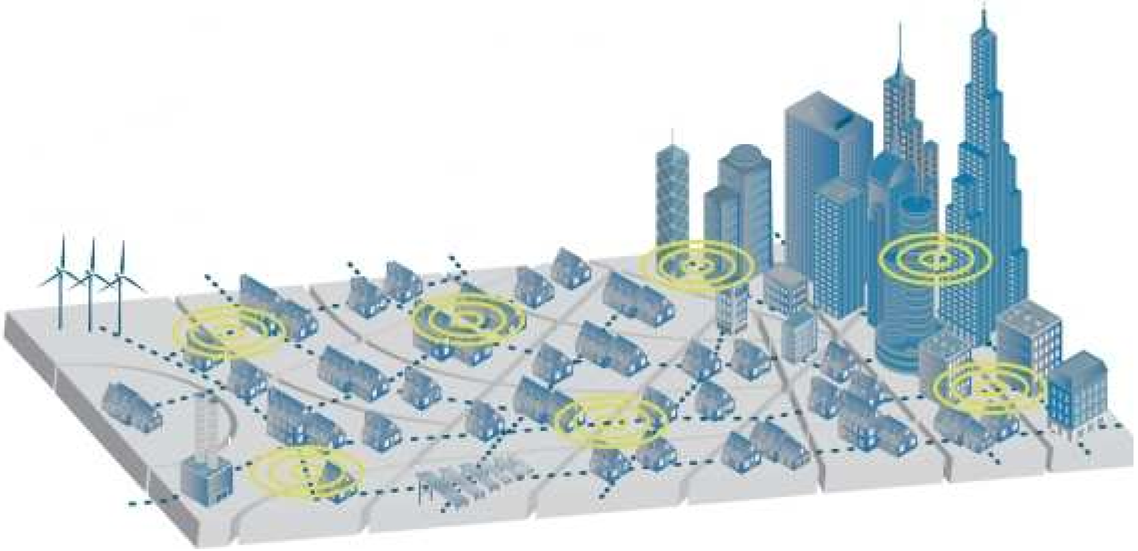
Agenda

EPOCHE & ESPRI

- ❑ Smart Metering System
- ❑ Supporting documentation
- ❑ TOE definition
- ❑ Security problem
- ❑ Security Capabilities
- ❑ Vulnerability analysis
- ❑ Conclusions

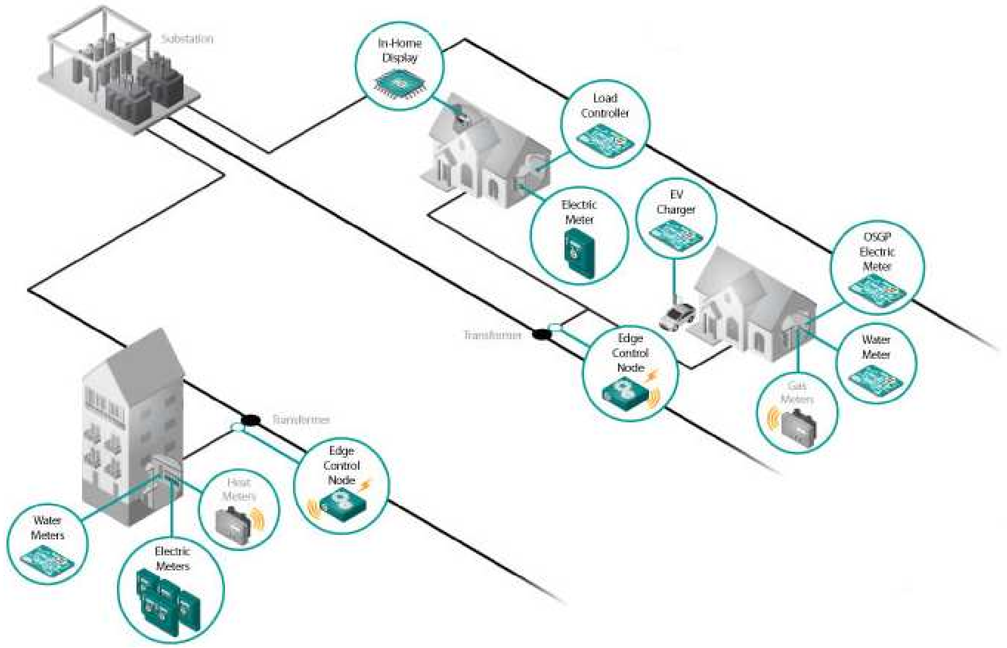
Smart Metering System

- A ***Smart Grid*** is a network that integrates the behaviour and actions of all entities connected to it in order to efficiently ensure a more sustainable, economic and secure supply of a certain commodities like electricity, gas, water or heat which is distributed from its generator to the consumer through the grid.



Smart Metering System

- ❑ An essential aspect of the smart grids is ***Smart Metering System*** that meters the production of the commodity at the consumer's side and supports sending the information to external entities.



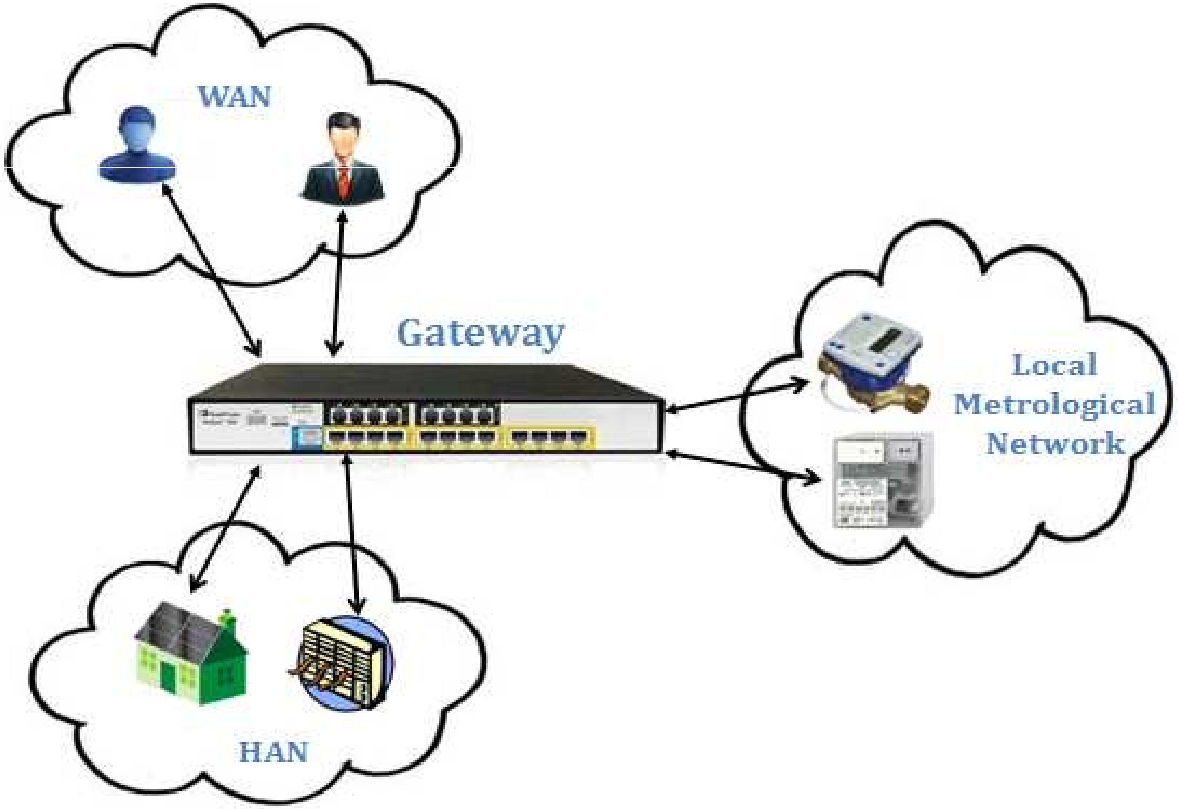
Smart Metering System

- ❑ The term ***METER*** refers to a unit for measuring the consumption or production of a certain commodity.
  - ✓ The meter device implements a **security module** to protect the data stored and to be sent.

Smart Metering System

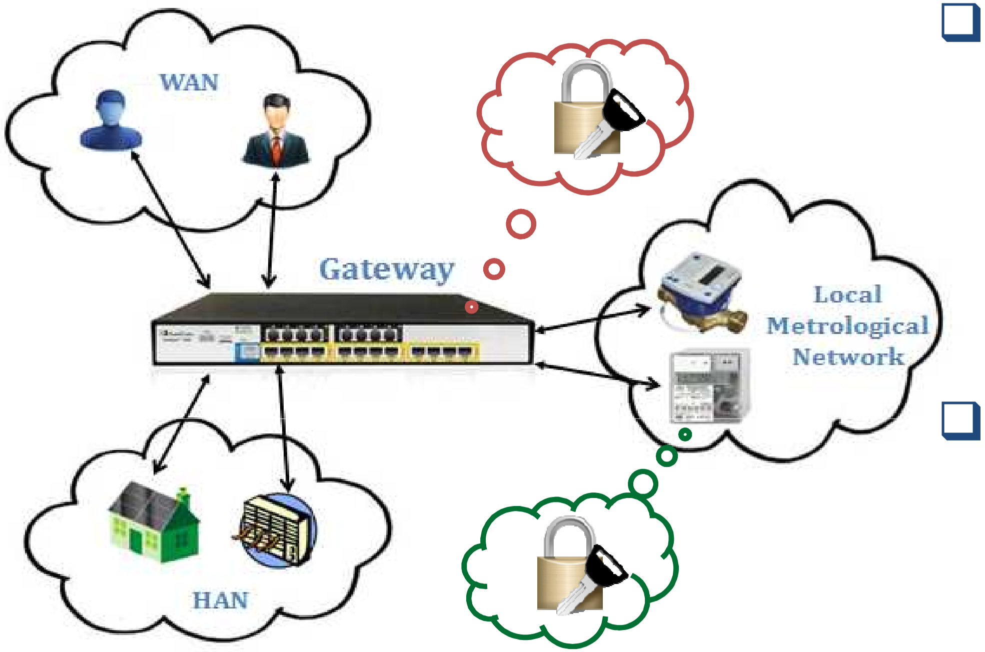
EPOCHE & ESPRI

- ❑ The **Smart Metering Systems** are supported by a communication infrastructure interconnecting the METERS providing connectivity to the external entity.



Smart Metering System

EPOCHE & ESPRI



- ❑ The **Gateway** serves as the communication component between the components in the LAN of the consumer and the outside world.

- ❑ **Controllable Local Systems.** power generation plants, controllable loads (air conditioned), applications in home automation, etc.

- ❑ The **Meter** records the consumption or production of one or more commodities (e.g. electricity, gas, water, heat) in defined intervals and submits those records to the Gateway.

Supporting documentation

EPOCHE & ESPRI

- ❑ Protection Profile for the Gateway of a Smart Metering System. BSI certified
- ❑ Protection Profile for the Security Module of a Smart Metering System (SM of the Gateway). BSI certified ....
- ❑ Non CC documentation .....
  - o ADVANCED METERING INFRASTRUCTURE ATTACK METHODOLOGY. An approach to security testing of different AMI architectures.
- ❑ .... EU directive .... as with a tachograph??

TOE definition

- ❑ What's a METER in CC terms?
  - o Physical: TOE with a security box
  - o Logical: Security module

TOE definition

❑ Physical Boundary

- The TOE comprises the hardware (SECBOX & circuitry) and the firmware that is relevant for the security functionality of the Meter device.
- Interfaces:
  - ✓ Interface between the Meter and the Gateway to send measures and also for meter configuration, FW upgrade.
  - ✓ Specific interface for meter configuration, FW upgrade, …..

TOE definition

- ❑ Logical Boundary
  - **Handling of Meter Measures**: confidentiality, integrity and authenticity protection (while sending to the Gateway, while temporarily stored in its volatile memory).
  - **Secure Storage** of Key Material and Certificates.
  - **Trusted channel** between the meter and an authorized Gateway.
  - **Management of security functionality**
  - **Audit**

TOE definition

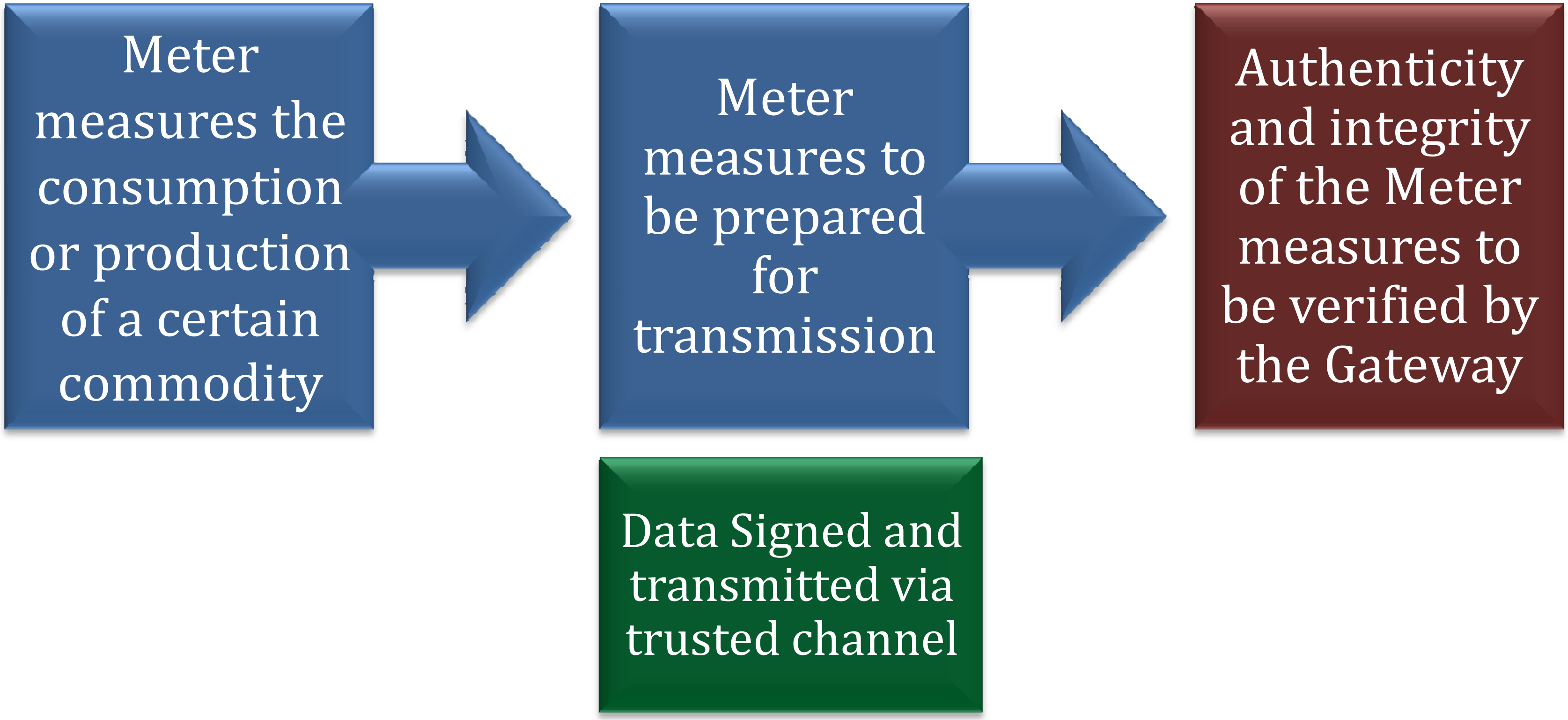
EPOCHE & ESPRI

- ❑ Logical Boundary
  - o **Cryptography.**

Aspect	Cryptography function
Trusted channel with the Gateway	Authentication of the Gateway Encryption Decryption Key Negotiation
Signature of Meter Data to be sent to the Gateway	Hashing Signature creation
Encryption of stored data	Encryption Decryption
Verification of FW upgraded	Hashing Signature verification

TOE definition

- ❑ Logical Boundary: Measures flow (meter to gateway)



Meter measures the consumption or production of a certain commodity

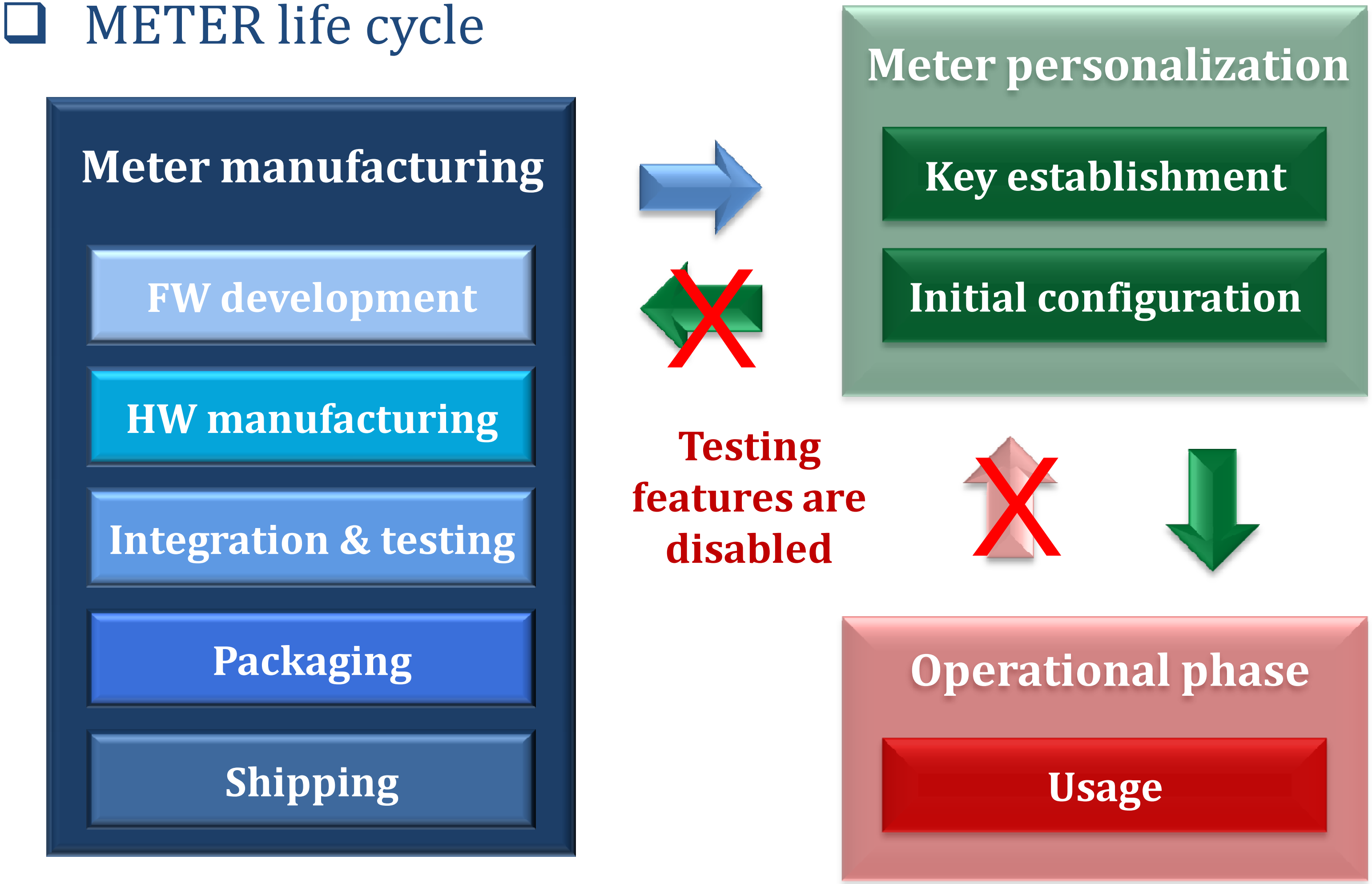
Meter measures to be prepared for transmission

Authenticity and integrity of the Meter measures to be verified by the Gateway

Data Signed and transmitted via trusted channel

TOE definition

- ❑ METER life cycle



Meter manufacturing

FW development

HW manufacturing

Integration & testing

Packaging

Shipping

Meter personalization

Key establishment

Initial configuration

Testing features are disabled

Operational phase

Usage

Security problem

- ❑ Threat model
  - o Meter Assets

Asset	Description	Value
Measures	Meter readings that will be processed later in the Gateway.	CIA
Meter time	Date and time of the real-time clock of the meter	IA
Conf. parameters	Configuration data of the Meter to control its behavior including the Meter identity and also status data.	CIA
Meter crypto material	• Private keys for signing meter data • Key material for trusted channel with the Gateway • Public key used for the integrity check for FW upgrade • Symmetric keys used to encrypt adm. commands • Symmetric key used to encrypt measures storage …..	CIA CIA IA CIA CIA
Meter FW	Meter firmware for updates	IA

Security problem

- ❑ Threat model
  - o Attackers.

Attacker	Description
Local attacker	They have physical access to the Meter. The attacker tries to compromise the confidentiality and/or the integrity of the assets while stored in Meter or while transmitted to the gateway or meter configuration data during the communication with the gateway.
Remote attacker	Located in the Local Metrological Network or link with the gateway trying to compromise the confidentiality and/or the integrity of the meter measures or meter configuration data during the communication with the gateway.

Motivation: supposed commensurate with high attack potential

Security problem

- Threat model
  - Threats.

Threats	Description
T.LocalData ➔ local attacker	Modify or disclose meter measures or alter the meter time stored in the meter. Try to modify the FW, key material or configuration parameters to circumvent security mechanisms or tries to get control over the TOE. Physical intrusive or non intrusive attacks and also attacks through the configuration interface.
T.RemoteData ➔ remote attacker	Modify or disclose meter measures or alter the meter time when transmitted between Meter and Gateway. Try to modify the FW, key material or configuration parameters to circumvent security mechanisms or tries to get control over the TOE. Try to impersonate a meter or the gateway.

Security problem

- Organizational Policies

OSP	Description
OSP.Audit	The TOE shall generate relevant log information and shall limit the access to this information to the meter operator or administrator. The system log may overwrite the oldest events in case that the audit trail gets full.

Security problem

- Assumptions

OSP	Description
A.LifeCycle	It is assumed that, during the whole life cycle of the meter (including personalisation and operational phase), the confidentiality, integrity, authenticity and quality of the key material is maintained.
A.TrustedAdmins	It is assumed that the meter operator or administrator is trustworthy and well-trained.
A.Network	It is assumed that the meters are connected only to the Gateway (in the Local Metrological Network). Meters may be configured through this interface or via a device connected with a direct cable which is supposed to be a trusted channel.

Security Capabilities

- ❑ Functional
  - o Logical security (SFRs + ADV_ARC)
    - ✓ Secure the communication with the gateway
    - ✓ Cryptography: trusted channel, signature creation & verification, data stored protection, verification of FW.
    - ✓ Meter configuration through the gateway interface according to an access control policy or through a dedicated interface (update keys, update FW, etc.)
    - ✓ Access control policy
    - ✓ Protection of the security functions against malfunctions and tampering (RIP, self-test, ADV_ARC)
    - ✓ Audit & Reliable time stamping

Security Capabilities

- ❑ Functional
  - o Physical security
    - ✓ **Tamper detection, evidence, response**. Provide mechanisms to resist manipulation of the TOE by physical probing on modifications against an attacker with high attack potential.
    - ✓ The TOE shall be able to **prevent leakage of information**, e.g., electrical characteristics like power consumption or electromagnetic emanations.

Security Capabilities

- ❑ Assurance
  - o EAL4 + AVA_VAN.5.

Vulnerability analysis

- Assumed an attacker with **high attack potential**

Considerations

1. The motivation of an attacker to the **full Smart Meter System** is high because of the full control of the smart grid.
2. The motivation of an attacker to a **single meter** would not be so high as the benefit would be for a particular user. However the easiness of taking control of a set of meters impersonating the gateway, would go beyond the interest of the end user.

Vulnerability analysis

- ❑ Attacks methods
  - o HW device with security box

1. Physical attacks: inspection (visual, X-ray…), removing materials, cutting/adding connections, probing a bus, reading memories…..
2. Overcoming sensors
3. Perturbation attacks and fault injection.
4. Side Channel Analysis
5. Software attacks

Conclusions

EPOCHE & ESPRI

❑ METER ➔

- A **security module** which provides security capabilities for the protection of the consumption measures
- **HW device with security box** falling in the SOGIS domain ➔ Attacks methods.
- PPs & EU directive ....
- Consideration of the requested assurance as part of the Smart Metering System : EAL4 +AVA_VAN.5

EPOCHE & ESPRI

Jose Emilio Rico
tech@epoche.es

Epoche & Espri, S.L.U.
Avda. de la Vega, 1
28108, Alcobendas, Madrid
Spain

Tel: +34 914-902-900
FAX: +34 916-625-344

Epoche & Espri Corporation
4000 Legato Road, Suite 1100
Fairfax, VA 22033
USA

Tel: +1 888-877-9506
FAX: +1 703-227-7189