CRITIS : Smart Grids Abdulhay Boydedaev | Christian Bauer | Hasan Güney Esendemir | Araz Rustamov | Uzezi Harry Adherioma

1. Business Model:

Smart grids are being used to create prosumers* by creating a supply chain system and network for energy resources to balance power generation with consumption. Our business is based on developing and selling smart grid appliances to create energy solutions and selling energy for houses and businesses.

2. Purpose:

Since smart grids work as a network based system and since it has become one of the main energy distribution systems, it has been a target for the malicious people. Purpose of the information security management system for smart grids is keeping devices, information and network secured and well-maintained in case of any possible internal or external threat to ensure keeping high availability by the user side for usage, high integrity by the company side for pricing data and safety of network and confidentiality for the privacy concern of end-users.

3. Existing Regulations:

-ISO 27019 based on ISO 27002 for process control systems specific to energy utility.

-Europe 2020 initiative, Energy 2020, a strategy fr competitive, sustainable and secure energy.

-Energy infrastructure priorities for 2020 and beyond.

-Energy efficiency directives for usage of more efficiently energy at all stages of energy chain : 2009/72/EC, 2008/114/EC, 2006/32/EC .

-Germany: The National Strategy for Critical infrastructure protection.

4. Assets:

Smart meters for homes (Lower Electricity Prosumers),

Smart meters for businesses (Higher Electricity Prosumers),

Software for smart devices,

Storage and Distribution Centers,

Wind Turbines and Solar Panels & Fields,

User Data,

Employee Data,

Development Data,

Energy Data,

Pricing Data,

Database Servers,

*Prosumer : Person who produces and consumes the product.

Backup Servers,

Software licenses, Patents, etc,

Distribution&Collection Cables,

Transformers.

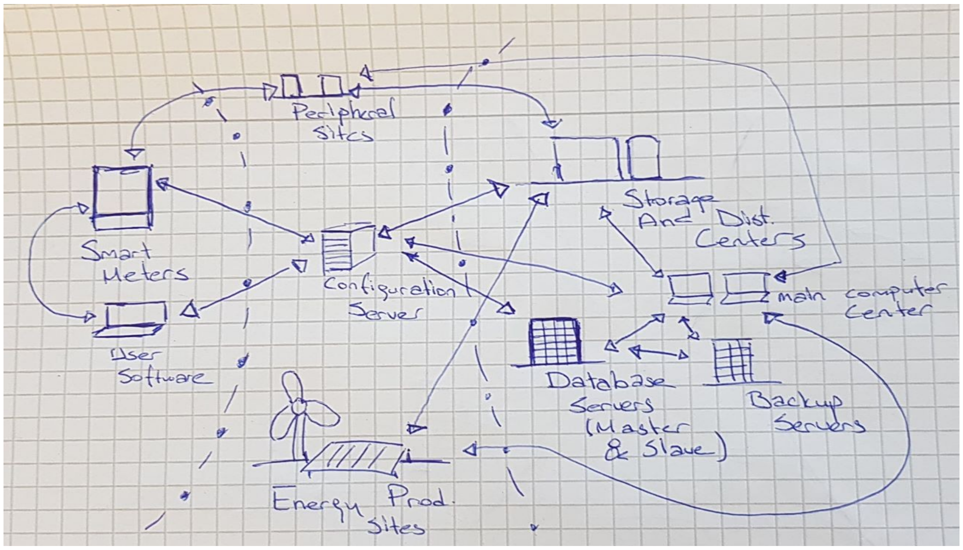
Peripheral sites and equipment

5. CIA Analysis:

Confidentiality	3
Integrity	5 (Customer Side) 10 (Business Side)
Availability	10

For the company availability is the most important thing. Our business has to track all production, consumption data and our customers should be able to use needed energy all the time. Integrity is also another important thing for the business side. Our production and distribution should be continuous for our customers, and it shouldn't be reached by third parties to prevent data breach, data changing (e.g pricing), uninterrupted distribution system management and for safety of production of storage areas. Confidentiality is only important for the privacy concerns and advanced metering infrastructure.

6. IT Architecture:



High Availability **Normal** **High Integrity**

In the IT-Architecture, customers with smart meters, and software connected to these smart meters. These should have high availability since they are needed continuously for our customers.

Storage-Distribution Centers which should have high integrity to maintain them correctly for safety of business and to keep its availability for our customers. It is also should be highly available but its availability comes from maintenance and safety.

Database servers for our user, employee, energy and billing data. They should have high integrity. Compromising these database servers are very risky for the business.

Backup servers are needed for maintenance and safety of database servers.

The energy production site should have availability and integrity at the same time. Our energy production should be able to fill our storage center when it is needed, it should be well maintained and secured to keep availability.

Our main computer servers should have high integrity to keep attackers outside of the system and to keep secure all network and distribution chain.

We need a configuration server between databases and other units to automate and secure data transactions.

7. ISMS Implementation:

ISMS implementation is done according to relevant ISO 27k documents (ISO 27001/27002/27019) by dealing the risks/vulnerabilities of:

- Reliably power providing,
- Faults and solutions,
- Impact of failures on customers.

The security measures are taken by ISMS includes:

- Monthly maintenance,
- Regular training and seminars for employees,
- Providing up-to-date policies, guidelines and safety protocols according to regulations.

7.1: Threat scenarios : (IT infrastructure, Human Internal, and Human external)

a) Cooling system breakdown of generators due to bad maintenance.

b) sabotage by employees

c) Vandalization/terrorist threat by 3rd parties

7.2 Concrete attack scenarios (Rx) for each Threat (Tx) including cause and course of events

R1 - IT Infrastructure (Internal Threat) : Security controls to avoid Cooling system failure due to bad maintenance:

1. ISO/IEC Control according to ISO/IEC 27019: 9.2.1 Equipment siting and protection*: Due to environmental factors such as dust, heat, cold, electromagnetic radiation, humidity, etc. The equipment should be suitably designed and constructed to operate in such conditions. Additional protections should be considered to reduce the influence of these environmental factors, such us dust protection covers, housing, shielding, etc. to guarantee reliable operation.

2. ISO/IEC Control according to ISO/IEC 27019: 9.2.4 Equipment maintenance: Following a regular maintenance cycle stationary equipment and appliances on company premises shall be checked by dedicated maintenance personal for its continued flawless operation within safety guidelines.

3. ISO/IEC Control according to ISO/IEC 27019: 9.3.1 Equipment sited on premises of other energy utility organizations*: If energy equipment needs to be installed on other energy utility organizations premises to provide better coverage and service, it should be ensured that the operational site where equipment is to be installed fulfils all necessary security requirements**.

R2 - Force majeure (External Threat) :

1. ISO/IEC Control according to ISO/IEC 27019: 9.2.2 Supporting utilities*: To avoid cyclic dependencies, all critical systems, communication servieces and other equipment required for system restoration after a major power outage should be designed and operated so that they are independent fo external services for an appropriate period of time. This applies in particular to external energy supplies**.

2. ISO/IEC Control according to ISO/IEC 27019: 9.2.3 Cabling security*: Due to the necessary extensive use of communication and power supply networks of cabling on ground which can’t be controlled by the power supply company and/or would be inaccessibly to maintain regularly additional protection shall be undertaking to protect existing cabling and provide fail-over networks of cabling to still be able to provide power in the event of incidents where cabling may become damage to to earth-quakes, fire, etc.

3. ISO/IEC Control according to ISO/IEC 27019: 9.1.2* Physical entry controls and 9.1.9* Securing peripheral sites: Authorized personal must identify themselves at the entrances and have their authorized access checked for example using a visible badge, smart (RFID) cards or access tokens. Entrance to peripheral sites where sensitive equipment is located need to be secured enough only using physical access control system. The entrances to these can be monitored so unscheduled entrance could notify the security at the company so personal can check the peripheral site for unauthorized access and/or damages.

Where a sufficient level of physical protection for peripheral sites is not attainable, the residual risk should be taken into consideration and mitigated by the application of appropriate countermeasures**:

a) In high-earthquake risk sites the peripheral site shall be proved against earthquakes and coinciding incidents such as water leaks, higher risk of fire, etc. corresponding to local and national standards.

b) Automatic fire control equipment could be installed if critical components are installed

c) Monitoring of component malfunction, power failure, fire, unauthorized entry, and if necessary to protect equipment, humidity, and temperature monitoring.

d) Adequate physically secure perimeter should be installed using, for example, secure fencing and automatic alarm system should be installed and monitored from a central location, where necessary**.

R3 - Sabotage (Human/External Threat):

1. ISO/IEC Control according to ISO/IEC 27019: 8.3.3 Removal of Access Rights: Upon termination of employment the employee must return their access tokens, badges or smart cards, their digital access be revoked and company property and/or clothing be returned to the company so the unauthorized access after unemployment can be stopped.

2. ISO/IEC Control according to ISO/IEC 27019: 9.1.1 Physical security perimeter: Security personal watches the premises for unauthorized entry of personal or 3rd parties. All authorized personal must be immediately identifiable and valid access must be visibly represented for example using a visible badge and company clothing.

3. ISO/IEC Control according to ISO/IEC 27019: 9.1.2* Physical entry controls and 9.1.9* Securing peripheral sites: (See R2.3)

7.3 Risk assessment

T1: Risk = damage high * medium

T2: Risk = damage high * low

T3: Risk = damage high * low

	Low Probability	Medium Probability	High Probability	Very high Probability
Damage Very high	🟥	🟥	🟥	🟥
Damage High	🟧	🟧 T1, T2	🟧	🟥
Damage Medium	🟨 T3	🟨	🟧	🟥
Damage Low		🟨	🟧	🟥

* Control is augmented by 27019

** Copied from control of 27019