Nuevas Tecnologías de Ciberseguridad y Analítica de Datos para Subestaciones Eléctricas

SecureGrid

New generation of electronic equipment to build a more secure power grid

Iñaki Angulo (*Tecnalia*)

Madrid, 23rd November, 2018

Project supported by the Departament of Economic Development and Infrastructure of the Basque Government (HAZITEK Programme) and the European Regional Development Fund (ERDF).

EUSKO JAURLARITZA
GOBIERNO VASCO
EKONOMIAREN GARAPEN ETA LEHIAKORTASUN SAILA
DEPARTAMENTO DE DESARROLLO ECONÓMICO Y COMPETITIVIDAD

Europar Batasuna
Unión Europea

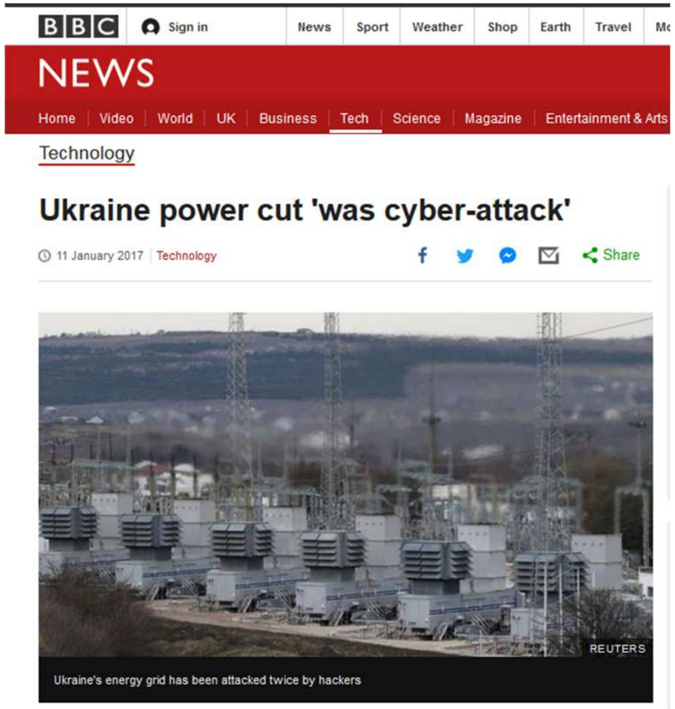
Fondo Europeo de Desarrollo Regional (FEDER)
"Una manera de hacer Europa"

Eskualde Garapenerako Europar Funtsa (EGEF)
"Europa egiteko modu bat"

ZIV · arteche · Ingeteam · ORMAZABAL velatia · GE · its · Cluster Energía BASQUE ENERGY CLUSTER · tecnalia Inspiring Business

Digitalisation is increasing vulnerability in the grid

- The number of external connection attempts has increased in the last years
- Regulation is confused
- The measures applied in other sectors are not directly applicable:
  - Availability versus confidentiality. We can not disconnect a system when we suspect an attack.
  - Response times.
  - Geographic and equipment dispersion



Technology

Ukraine power cut 'was cyber-attack'

11 January 2017 | Technology

Ukraine's energy grid has been attacked twice by hackers

SecureGrid

Nuevas Tecnologías de Ciberseguridad y Analítica de Datos para Subestaciones Eléctricas

- Funded by the Basque Government
- HAZITEK Programme (2016-2018)
- Budget: ~ 4M€
- Develop technology to Increase the security of the IEDs in electrical substations.
- Positioning the Basque Country as an international reference in cybersecurity for Smart Grids.

EUSKO JAURLARITZA
GOBIERNO VASCO
EKONOMIAREN GARAPEN
ETA LEHIAKORTASUN SAILA
DEPARTAMENTO DE DESARROLLO
ECONÓMICO Y COMPETITIVIDAD

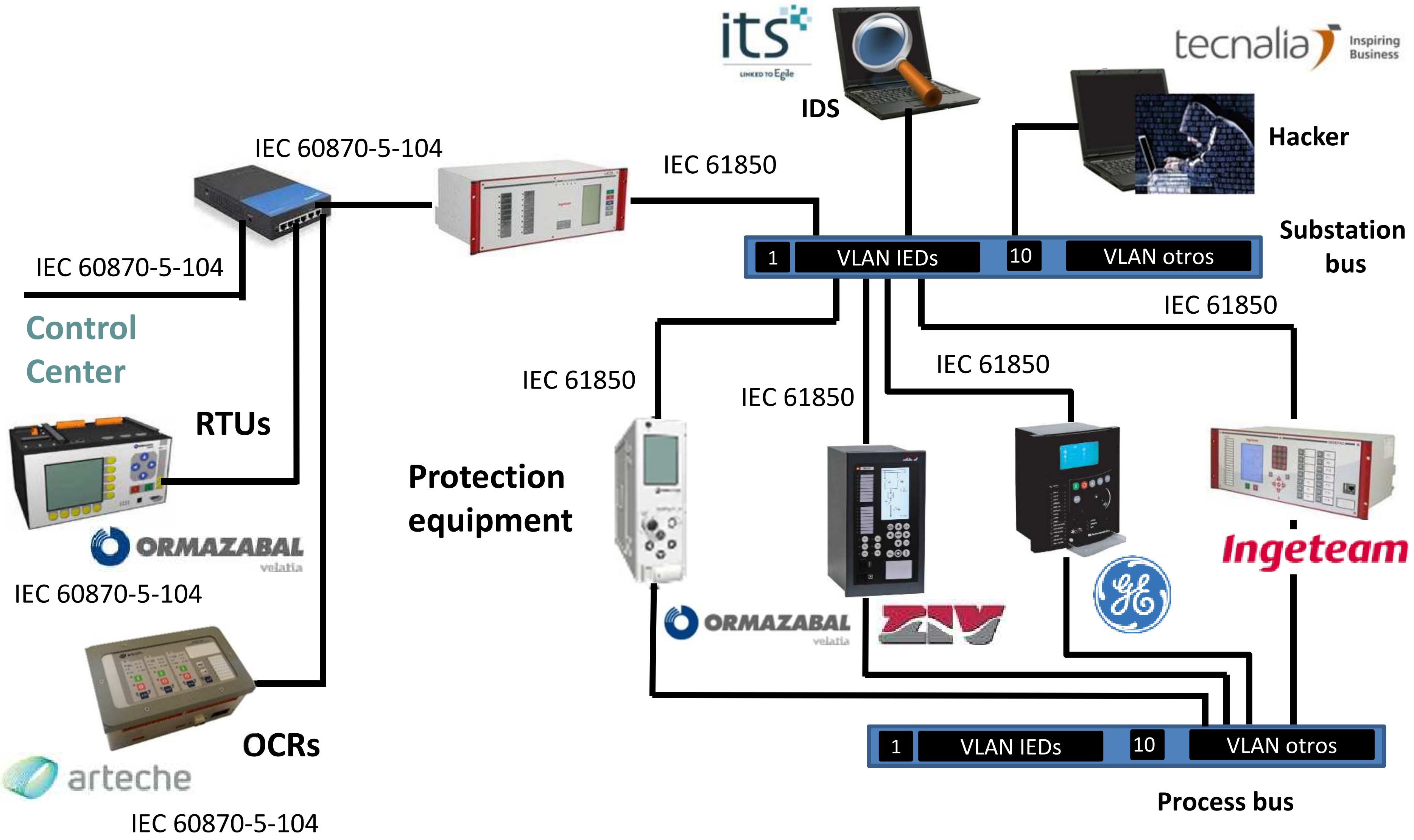
Europar Batasuna
Unión Europea

Fondo Europeo de
Desarrollo Regional (FEDER)
"Una manera de hacer Europa"

Eskualde Garapenerako
Europar Funtsa (EGEF)
"Europa egiteko modu bat"

ZIV arteche Ingeteam ORMAZABAL velatia

GE its LINKED TO Egile Cluster Energía BASQUE ENERGY CLUSTER tecnalia Inspiring Business



its

IDS

tecnalia Inspiring Business

Hacker

IEC 60870-5-104

IEC 61850

Substation bus

1 VLAN IEDs 10 VLAN otros

IEC 60870-5-104

Control Center

IEC 61850

IEC 61850

IEC 61850

IEC 61850

RTUs

ORMAZABAL velatia

IEC 60870-5-104

Protection equipment

ORMAZABAL velatia

ZIV

GE

Ingeteam

OCRs

arteche

IEC 60870-5-104

1 VLAN IEDs 10 VLAN otros

Process bus

Nuevas Tecnologías de Ciberseguridad y Analítica de Datos para Subestaciones Eléctricas

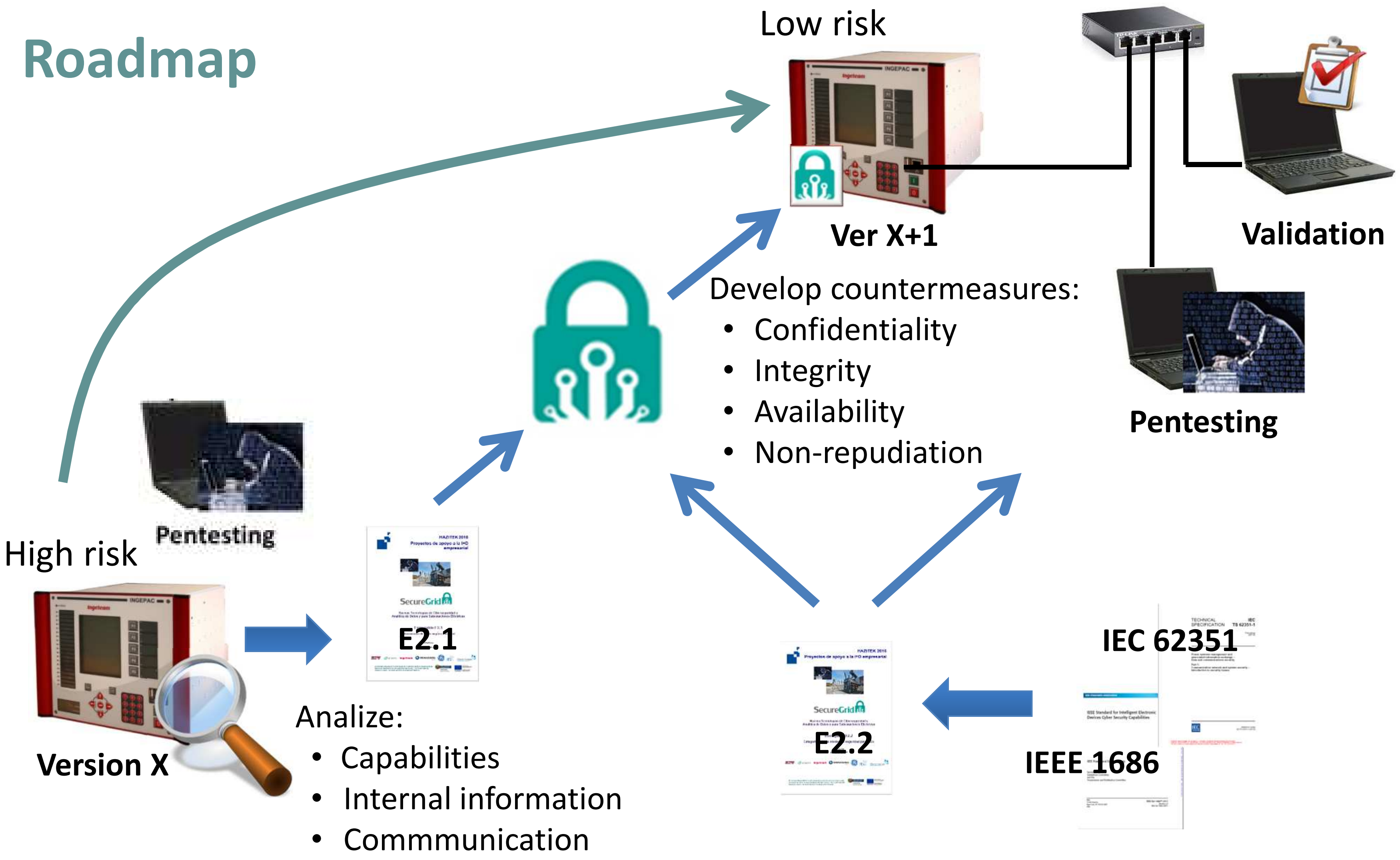
Regulation

- Which regulation should I apply?
  - IEC 62443. Evaluation of the safety of systems and equipment.
  - IEEE 1686. Security model for IEDs.
- How to apply it?
  - IEC 62351 (IEC 60870, IEC 61850)
    - Part 3 - IEC 60870-5-104
    - Part 4 to 6 - IEC 61850
    - Part 8 - RBAC
    - Part 10 – Architecture
- How to certify it?
  - Testbook of the IEEE 1686

SecureGrid Model – Specification IEEE 1686

High (A)	**5.4.x** – Communication encryption **5.5.x** – Firmware signing	**5.4.x** – Communication encryption **5.5.x** – Firmware signing	**5.5.x** – Role management in the config SW **5.5.x** – Firmware signing	**5.4.x** – Communication encryption
Medium (B)	**5.1.x** – Role management **5.5.x** – Role management in the config SW	**5.1.x** – Role management **5.5.x** – Role management in the config SW	**5.3.x** – Events and alarms monitoring **5.6** – Port activation and deactivation	**5.1.x** – Role management **5.2.x** – Audit record **5.3.x** – Events and alarms monitoring **5.5.x** – Role management in the config SW
Low (C)	**5.1.x** – Access control to IED **5.5.4** – Access control to config SW	**5.1.x** – Access control to IED **5.3.x** – Events and alarms monitoring **5.5.4** – Access control to config SW	**5.1.x** – Role management **5.2.x** – Audit record	**5.1.x** – Access control to IED **5.5.4** – Access control to config SW
Level / Req.	**Confidentiality**	**Integrity**	**Availability**	**Non-repudiation**

Roadmap



Low risk

Ver X+1

Validation

Pentesting

Develop countermeasures:

- Confidentiality
- Integrity
- Availability
- Non-repudiation

High risk

Pentesting

Version X

E2.1

Analize:

- Capabilities
- Internal information
- Commmunication

E2.2

IEC 62351

IEEE 1686

Improvements to the equipment

IEEE 1686

- Today, the equipment incorporate:
  - improved generation and management of passwords.

    Clauses 5.x.1
  - disconnection after a period of inactivity
  - role-based access systems
  - generation and management of an audit record containing basic information on events and alarms related to the security of the equipment

    Clauses 5.x.2
- Ongoing work:
  - monitoring of the activity related to security aspects

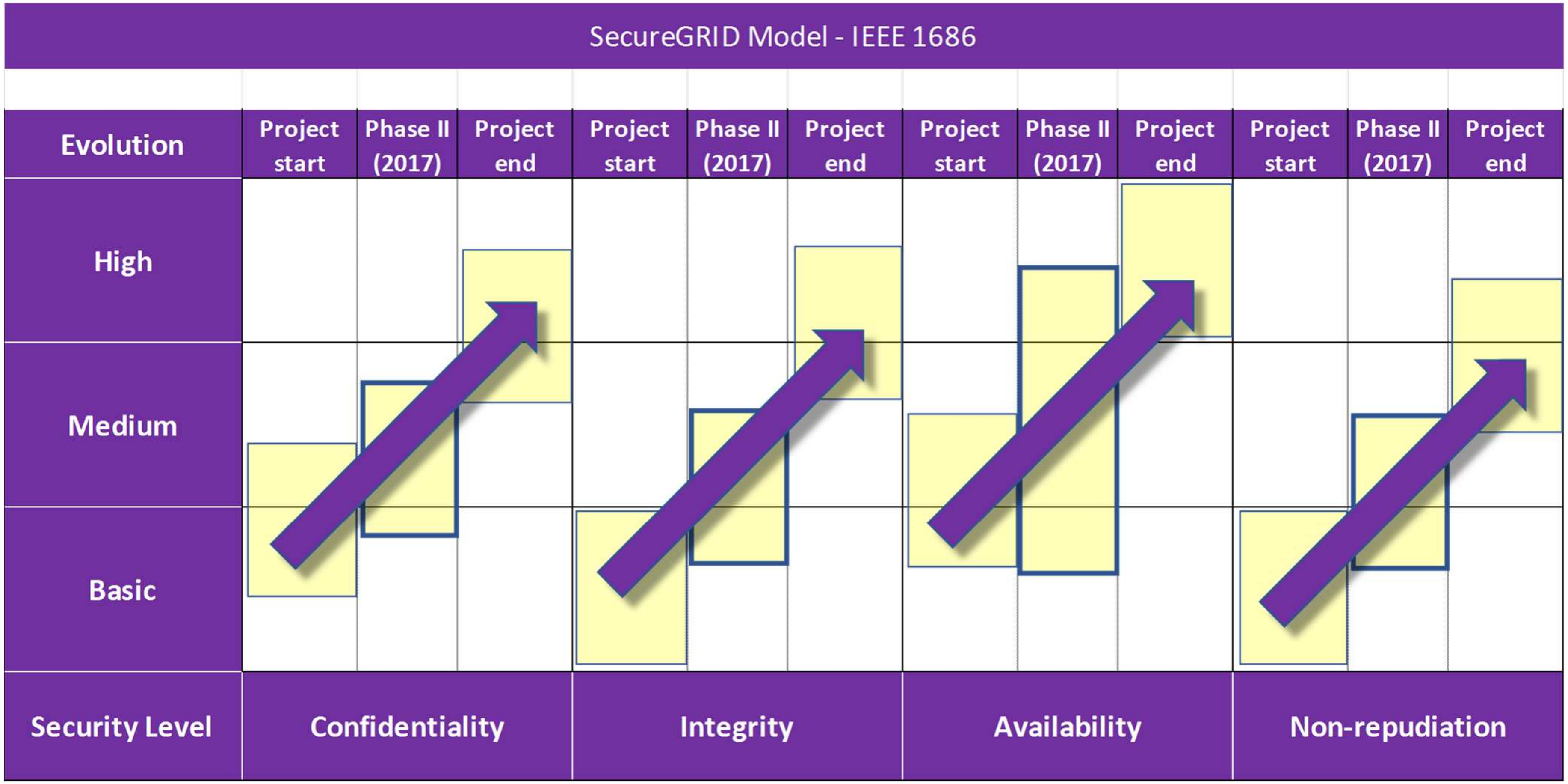
    Clauses 5.x.3
  - encryption of communications,

    Clauses 5.x.4
  - signature of the firmware and authentication of the configuration software

    Clauses 5.x.5
  - activation and deactivation of communication ports

    Clauses 5.6

Current situation - november 2018



SecureGRID Model - IEEE 1686

Evolution

Project start | Phase II (2017) | Project end

High

Medium

Basic

Security Level

Confidentiality

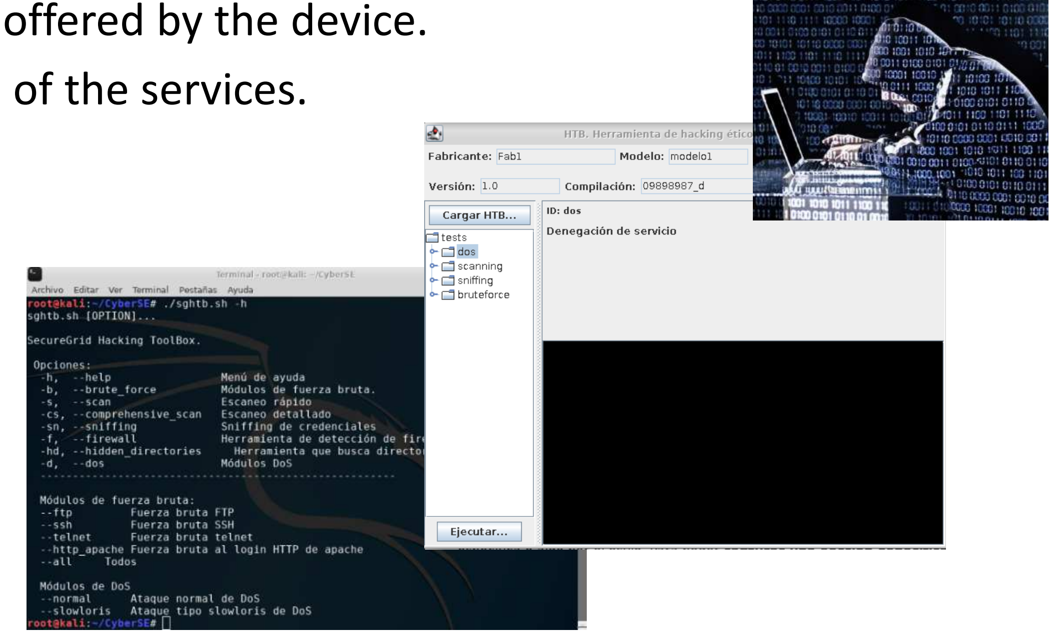
Integrity

Availability

Non-repudiation

Ethical hacking toolbox

- Allows to perform a set of penetration tests to discover the vulnerabilities that the device presents:
  - Discovery of the services offered by the device.
  - Obtaining the credentials of the services.
  - Denial of Service
- Integrated tools:
  - Nmap
  - Metaspoloit
  - W3af
  - Ettercap
  - Slowloris



```
root@kali:~/CyberSE# ./sghtb.sh -h
sghtb.sh [OPTION]...

SecureGrid Hacking ToolBox.

 Opciones:
  -h,  --help                 Menú de ayuda
  -b,  --brute_force          Módulos de fuerza bruta.
  -s,  --scan                 Escaneo rápido
  -cs, --comprehensive_scan   Escaneo detallado
  -sn, --sniffing             Sniffing de credenciales
  -f,  --firewall             Herramienta de detección de fire
  -hd, --hidden_directories     Herramienta que busca directo
  -d,  --dos                  Módulos DoS
  -----------------------------------------------------------

  Módulos de fuerza bruta:
  --ftp         Fuerza bruta FTP
  --ssh         Fuerza bruta SSH
  --telnet      Fuerza bruta telnet
  --http_apache Fuerza bruta al login HTTP de apache
  --all     Todos

  Módulos de DoS
  --normal      Ataque normal de DoS
  --slowloris   Ataque tipo slowloris de DoS
root@kali:~/CyberSE# 
```

Fabricante: Fab1 Modelo: modelo1

Versión: 1.0 Compilación: 09898987_d

ID: dos

Denegación de servicio

Conclusions

- Manufacturers are immersed in a process to improve the security of electrical equipment:
  - Make it more difficult to take control of the equipment from an external system, and avoid spreading to other equipment.
  - Registration of actions related to security.
  - Encrypted and signed communications.
  - Strengthen the equipment availability.
- Added value of collaboration between competitors.
- Ethical hacking as a tool applied to the improvement of security of IEDs during the manufacturing process.
- It is essential to combine the measures developed in the project (OT) with improved IT security measures.

There is still a lot to do…!

- Share and check the project results with utilities.
- Definition of technological lines for the project to evolve
  - Recovery from attacks
  - Honeypots
- Adaptation of electronic equipment to the evolution of regulation, which increasingly includes more security aspects.
- Tecnalia has a Cybersecurity Laboratory for Smart Grid:
  - It is part of the Cybersecurity Node of the "Digital Innovation Hub" of Advanced Manufacturing in the Basque Country.
  - It allows the simulation of new (and more complex) attack scenarios, as well as testing new equipment and attack detection systems.

Nuevas Tecnologías de Ciberseguridad y Analítica de Datos para Subestaciones Eléctricas

SecureGrid

Thank you!

inaki.angulo@tecnalia.com

http://www.clusterenergia.com/securegrid

Project supported by the Department of Economic Development and Infrastructure of the Basque Government (HAZITEK Programme) and the European Regional Development Fund (ERDF).

EUSKO JAURLARITZA
GOBIERNO VASCO
EKONOMIAREN GARAPEN ETA LEHIAKORTASUN SAILA
DEPARTAMENTO DE DESARROLLO ECONÓMICO Y COMPETITIVIDAD

Europar Batasuna
Unión Europea

Fondo Europeo de Desarrollo Regional (FEDER)
"Una manera de hacer Europa"

Eskualde Garapenerako Europar Funtsa (EGEF)
"Europa egiteko modu bat"

ZIV arteche Ingeteam ORMAZABAL velatia GE its LINKED TO Egile Cluster Energía BASQUE ENERGY CLUSTER tecnalia Inspiring Business