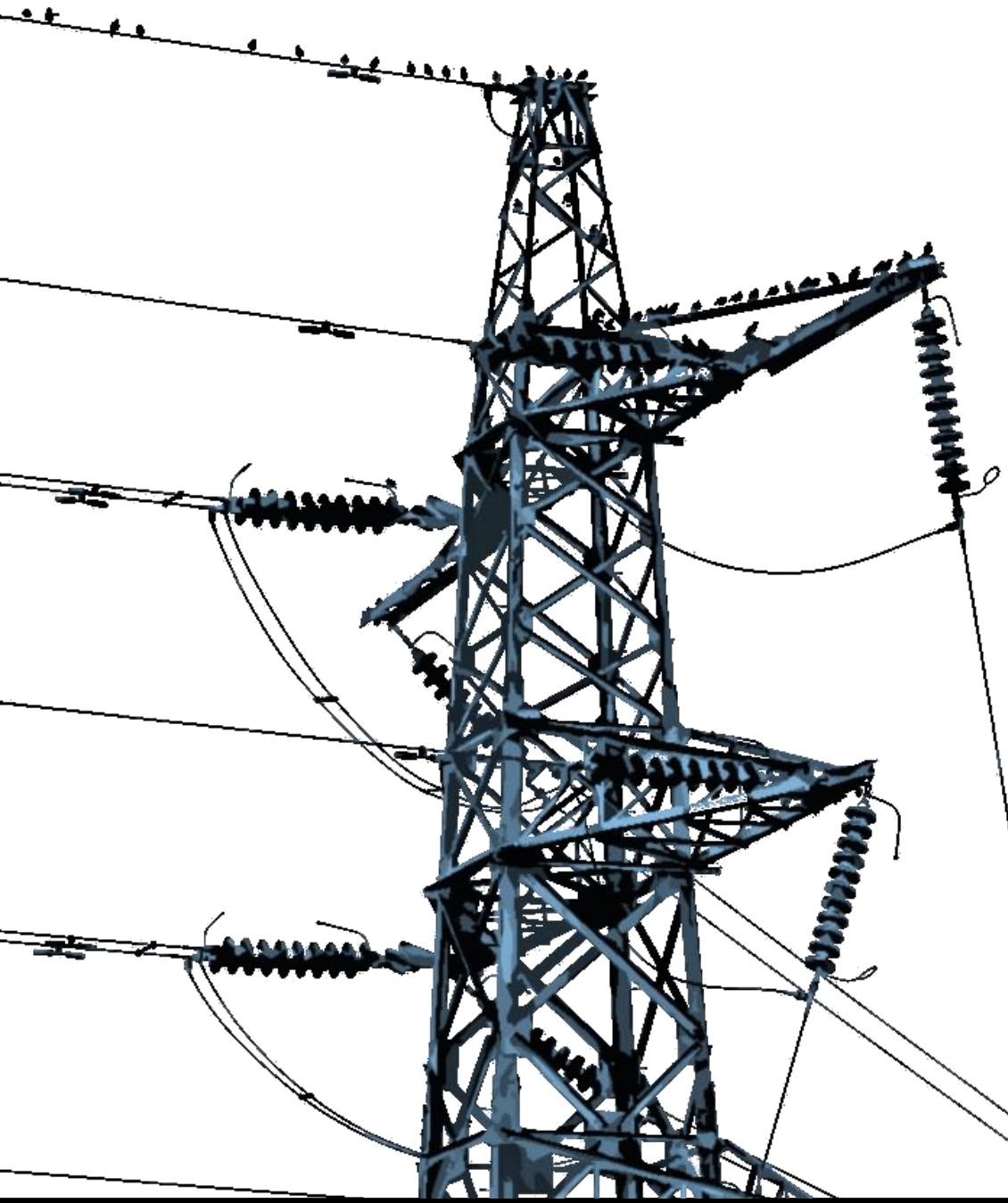
FASE, **F**ramework de **A**taque para **S**ector **E**léctrico

AFES, Attack **F**ramework for **E**lectric **S**ector

Author: Aarón Flecha Menéndez



Acknowledgements

To my family, friends, tutor and people who have trusted me. Special mention to:

Mildrey Carbonell Castro
Francisco Luis de Andres Perez
Rubén Ramón Sobrino

And to the company Estabanell Energia

Abstract

The main objective of this work is the development of a specific cyberattack framework for the energy sector named CAFFEINE, using a state of the art cyberattack methodology called CAT. The project focuses on the electricity sector in its distribution infrastructures, given the importance for other critical infrastructures. Throughout the work, the reader will be able to understand the basic concepts related to the electricity distribution networks, thanks to the description of devices, regulations, standards and communications protocols presented in this paper. Moreover, it will be developed a deep analysis about different cyber incidents with a clear impact into the electricity sector.

Once the main concepts of the electricity sector have been addressed, a comparative analysis of the state if the art strategic attack taxonomies, the proposed by Lockheed Martin (Cyber Kill Chain) and the CAT taxonomy. Moreover, using the Cyber-attack full stack model, CAFS as a reference, and selecting CAT taxonomy as the strategic layer, in the tactical and technical layers Mitre Attack will be used in order to complete the cyber-attack full stack modelling.

Finally, there will be an in-depth development of the CAFFEINE framework, which will come to light thanks to this work, since it is currently in the process of being evaluated by the new tactics and techniques. CAFFEINE framework intends to become the tactics and techniques layers incorporated to the CAT methodology for the electricity sector.

In order to demonstrate the applicability of this CAFFEINE framework a complete attack scenario will be presented so any network team could reproduce it, moreover, a full model of the GreyEnergy malware using the CAFFEINE framework as analysis instrument.

Key words

Cybersecurity, Electric Sector, Hacking, Industrial Control Systems, Red Team

Index

List of Illustrations

1 Introduction

Within industrial world, availability is the most important pillar ahead of confidentiality and integrity. This fact, coupled with other factors such as false sense of security due to industrial system isolation from Internet, made cybersecurity exercises in production or simply in these environments, unthinkable and practically unattainable.

As time goes by different pieces of malware were detected starting with Stuxnet (1) and following other ones like the last ones detected known as GreyEnergy (2). These advanced threats allowed different technologies to enter the industry thus improving both industrial network and device cybersecurity. Initially, only the most passive options began to be implemented given the initial complexity of industrial networks. Among these options can be found the deployment of probes for information collection or installation of agents running on industrial devices without much resource use.

Since threats, like technology implemented defensively, are constantly evolving, we face a new challenge in the industrial world and must go one step further to prevent future cyberattacks.

Following lessons learned from previous pieces of malware, some sectors, such as the Financial one, have opted for Red Team exercises in response to, in the form of training in the face of possible advanced attacks. This type of exercises is based on exploiting different vulnerabilities in production environments to:

- Detect vulnerabilities within elements located in a network.
- Get to know the real magnitude of cyberattacks.
- Procedure improvement and tasks to be executed before a real cyberattack.

Having said this, it appears that other industrial sectors are beginning to take action and seriously considering using Red Team exercises to analyze their systems. Among these sectors we can find the Energy one in which this whole project will be focused from now on.

Energy sector is one of the industrial sectors where researchers report most vulnerabilities. This is because it is the cornerstone of the sectors at industrial level and has cybersecurity budgets as well as professionals that focus their work and research in such sector.

1.1 Context and Work Justification

Based on Unified CyberKill Chain (4) document where different taxonomies and attack modellings are analyzed in depth, the necessity of a new taxonomy that covers existing gaps in those already considered in addition to an industrial cybersecurity focus can be assured and justified. The main objective pursued by this project is to create an attack framework for industrial environments that use Red Team in the electricity sector, specifically for distribution Substations in production. It is important to emphasize “production” because sectors such as

Financial are already starting to carry out this type of exercises on their product environments. Examples can be seen in TIBER-EU (3), TIBER-NL (5) or CBEST (6) frameworks in The United Kingdom. In this regard, it will also be important to emphasize pros and cons that red team squads will find when auditing production environments, how to solve potential problems, architecture types, use of regulations to base argument of some tests (NIST framework, IEC 27019, IEC 62443, etc.) and other features that can be taken into account when defending a test based on both, legal and technical level.

It will be important to narrow the scope in this project since energy sector, in particular electricity subsector (distribution) is one of the subsectors that is investing the most in cybersecurity. According to the latest INCIBE-CERT data, energy sector is one of the sectors where researchers discover most vulnerabilities.

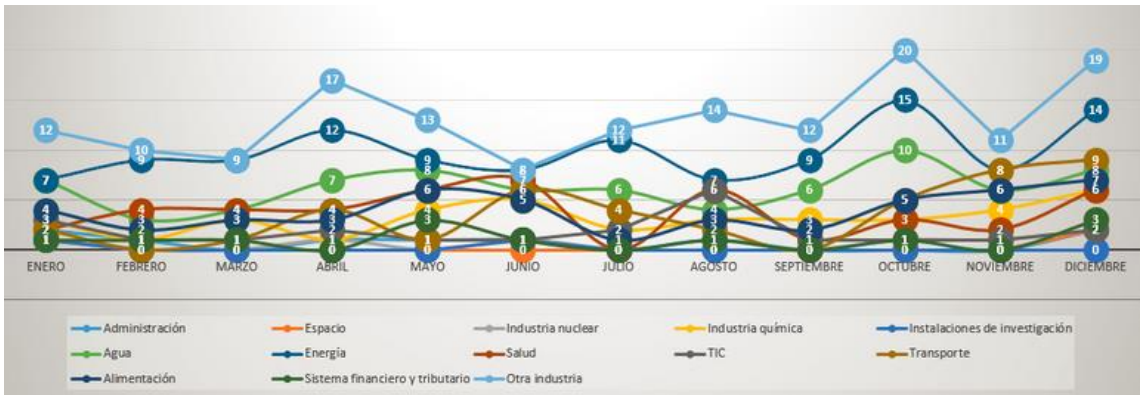


Illustration 1: Data extracted from INCIBE-CERT

To better understand the framework to be developed, cyberattacks that have affected electricity sector like BlackEnergy 3 or one of the latest, GreyEnergy will be analyzed. The objective here is to identify the steps executed by attackers in order to recreate the entire cyberattack to serve to incident response teams and red teams to run controlled tests. In summary, using well-known and documented cyberattack cases, aiming to reproduce them in a real industrial environment and checking if existing defensive measures could have prevented such cyberattacks (7).

1.2 Work Objectives

Among the different objectives of this project, the following should be highlighted:

- Creation of a cyberattack framework for electricity sector keeping in mind the availability problem and the specific case of electricity distributors.

- Enhance Cyber Attack Taxonomy (CAT) in industrial control systems. Such cyberattack taxonomy is being developed in open source format so that anyone can contribute and use it based on their needs. To achieve this goal an example will be developed using CAT taxonomy and cyberattack framework for electricity sector. This example will analyze a recent piece of malware that has affected the energy sector.

The achievement of this objective will be reflected by the project development itself and it will contain enough information to apply CAT taxonomy and specifically, framework oriented to industrial environments.

Parts of this project will be added to the official github account of CAT taxonomy.

- Comparison of the cyberattack taxonomy posed by Lockheed Martin (Cyber Kill Chain) and cyberattack modelling proposed by MITRE against Cyber Attack Taxonomy (CAT). This objective aims to show some of the deficiencies owned by cyberattack taxonomies and modellings like the one proposed by Mitre in "*insiders*" cases or other potential situations occurring in companies. Thanks to these deficiency simples and examples to be developed, it is intended to give a picture of both, CAT taxonomy and its application to industrial environments (created framework).

- Provide a series of key steps to be executed by Read Teams in production environments. These steps will focus on the electrical distribution part of the substations.

1.3 Focus and methodology followed

For development of the caffeine framework presented later in this project, use of CAT methodology was chosen. This framework will be defined within such methodology and will allow red teams to have specific tactics, techniques and tools available for testing in electrical distribution environments currently in production. Since CAT is not intended to be a substitute for attack modelling posed by MITRE or PwnWiki, it feeds instead on tactics, techniques, tools and resources owned by others. This choice will allow to perform both, modelling and developing different red team exercises in a clearer and more efficient way, technically and visually.

In summary, since *caffeine* framework will be defined into CAT, within this framework there will be techniques, tactics and tools specific to electricity sector (distribution) as well as inherited from CAT, MITRE or PwnWiki among others.

1.4 Work Planning

Since this Project has been posed by the student, the first task performed was to collect documentation and send arguments to the person responsible for security area in operating systems. After an email Exchange and Project explanation it was proceeded to project planning itself. The different deliveries contemplated with the content included in each one, are as follows:

- **PEC 1**
  - Work planning and Project introduction
  - Scope and Project objectives
  - Project Argumentation
  - Methodology used
  - Project content

- Documentation Organization. At this point using of document managers like nuxeo, alfresco or Google drive itself was considered.

- **PEC 2**
  - **Introduction** – Brief description of the current cybersecurity state in industrial environments and specifically in the electricity sector (distribution).

    - **Context and Work Justification –** Work starting point (What is the need to cover? Why is it a relevant issue? How is the problem being resolved currently?) and the contribution made (Which result do we want to obtain?).

    - **Work Objectives –** List of work objectives.

    - **Approach and method followed –** Discuss possible strategies to carry out the Project and indicate the chosen one (develop a new product, adapt an existing one, …). Assess why is the most appropriate strategy to achieve the objectives.

    - **Work Planning –** Description of the resources needed to carry out the project, tasks to be performed and a time schedule of each task using a Gantt chart or similar. This planning would have to mark partial milestones for each PEC.

    - **Brief summary of obtained products -** No need to get into detail: in-depth description will be made in the other chapters.

    - **Brief description of the other memory chapters –** An explanation of the contents of each chapter relative to the entire work.

  - **Electricity Sector, distribution –** Introduction to the electricity sector.

    - **Devices –** Different devices that can be found in a substation network and its communication with the control center.

    - **Communications –** Architectures commonly found in an electrical distribution substation and protocols used (IEC104, DNP3, 61850, etc.).

    - **Regulations –** Discuss different regulations to be considered that will serve to develop the attack

framework. At this point, ISO/IEC 27019, IEC 62351, IEEE 1686-2013, NERC CIP and 62443 standards will be addressed in particular.

- **Cyberattacks –** Comment upon the most famous and recent malware cyberattacks on electricity sector (BlackEnergy, GreyEnergy, etc.).

- **PEC 3**
  - **ICS Cyber Kill Chain and Cyberattack Taxonomies –** Introduction to the Cyber Kill Chain attack taxonomy developed by Lockheed Martin (CKC) and specifically the one suited to industrial environments. After discussing such taxonomy, an in-depth CAT taxonomy description and Mitre modelling with its matrixes incorporating TTPs will be made.

- **PEC 4**
  - **Cyberattack Framework for Electricity Sector –** Development of the main idea.
    - **Temporary acting spaces**
    - **Explanation of the environment created for testing**
    - **Applying CAT to the tests**
    - **Tests executed, results and recommendations**
    - **Tools**
    - **…**

- **Final delivery**
  - **Incorporation of all corrections and improvements detected by both the tutor and the student himself.**
  - **Add following sections:**
    - **Final Conclusions –** Explanation of the conclusions drawn after finishing the project and its improvement possibilities.
    - **Glossary –** Description of the different terms used in this document.
    - **Bibliography –** Description of the material used.
    - **Annexes –** The use of annexes will depend directly on work's development.

Different diagrams and tables collecting all planning in a more visual way have been added. This material can be found in Annex I – Planning Diagrams.

1.5 Brief summary of obtained products

The development of *caffeine* framework has provided different contributions in the Project that CAT has on github with new tactics and techniques specific to

the industrial sector and in particular for the electricity sector (distribution). Such tactics and techniques will be published based on community's review. In addition, it will be the starting point for other professionals in the sector who want to model an attack or plan new cyberattack scenarios for red teams.

1.6 Brief description of the other memory chapters

Content of each section and its importance in this project are described below:

- **Introduction** – Brief description of the current cybersecurity state in industrial environments and specifically in the electricity sector (distribution). State of industrial cybersecurity art and some data of interest.

- **Electricity Sector, distribution** – Introduction to electricity sector. This chapter allows to position the reader and focus the terms that are going to be discussed. Devices, communications, regulations, standards and cyberattacks affecting directly the electricity sector will be described.

- **Cyberattack taxonomies, Cyber Kill Chain and CAT –** This chapter will describe both cyberattack taxonomy proposed by Lockheed Martin (Cyber Kill Chain) and the taxonomy on which the framework development for the electricity sector CAT (Cyber Attack Taxonomy) will be based.

- **Cyberattack Framework for Electricity Sector –** Development of the main idea, the framework. Examples of new tactics and techniques specific to the electricity sector and a modelling of the GreyEnergy incident will be included.

- **Final Conclusions** – Explanation of the conclusions drawn after finishing the project and its improvement possibilities.

- **Annexes –** The Project has 2 annexes. In the first one it is shown graphically with tables and charts a more in-depth planning of the work performed and the second annex, a technical view of the cyberattacks suffered by Venezuela in its electricity sector.

2 Electricity Sector, distribution – Introduction to electricity sector

The electricity sector supports many others and allows, among other actions, to provide energy to settlements. If energy supply is compromised in a settlement, revolts could arise given the importance of electricity in people's lives nowadays. One of the most recent cases, where this problem is discussed, can be consulted in Annex 2 – Cyberattack on Venezuela, technical review.

Within a Power Grid, electricity must pass through different phases or stages before reaching our homes. This Project will focus on the distribution phase however the other phases will be listed and briefly commented to better understand how a power grid looks like.

1. **Generation**. The origin of electrical energy derives from different primary elements such as water, wind, sun, etc. Thanks to an adequate treatment provided by generating plants (hydroelectric, wind farms, solar, etc.) these elements generate electricity.

   In many cases, power plants do not comply with proper regulations and can damage the environment so it is very important, in addition to generating electricity, to do so in a sustainable and efficient way.

2. **Transport**. Energy generated in the initial phase has to be transformed previously by transformer stations. The mission of these stations is to change the output voltage level of the generating plants to an adequate value (in Spain, between 220 and 400 Kv) to obtain greater efficiency in electric transport and avoid energy losses due to Joule Effect (8).

   To achieve the transport phase main objective, elements like electricity pylons and high-voltage cables that transport electricity over large expanses are commonly used.

   In Spain, Red Eléctrica de España (REE) is the company in charge of managing the transport network, since Law 17/2007 (9) became effective, which granted it the status of sole electricity Carrier.

3. **Distribution**. Once transported, electricity must be distributed to the different populated areas or areas with a specific need. To achieve this goal, reducing transformer substations change voltage levels from high to medium voltage and from medium to low voltage before reaching the final customer, populated areas or specific locations.

   The distribution network starts from reducing transformer substations and by means of rings surrounding the large consumption centers reach distribution transformer substations. Usual voltages are 25, 30, 45, 66, 110 or 132 kV. Second stage is the medium voltage distribution network, which is a radial network that links distribution transformer substations with processing centers. Voltages used: 3, 6, 10, 11, 15, 20, 25 or 30 kV.

Our research will be focused in this phase to reduce the scope and show greater technical detail.

4. **Commercialization**. This is the final phase of electricity in which companies sell electricity to final consumers through a competition regime, at least in Spain. These companies have previously had to buy the electricity from generating companies.

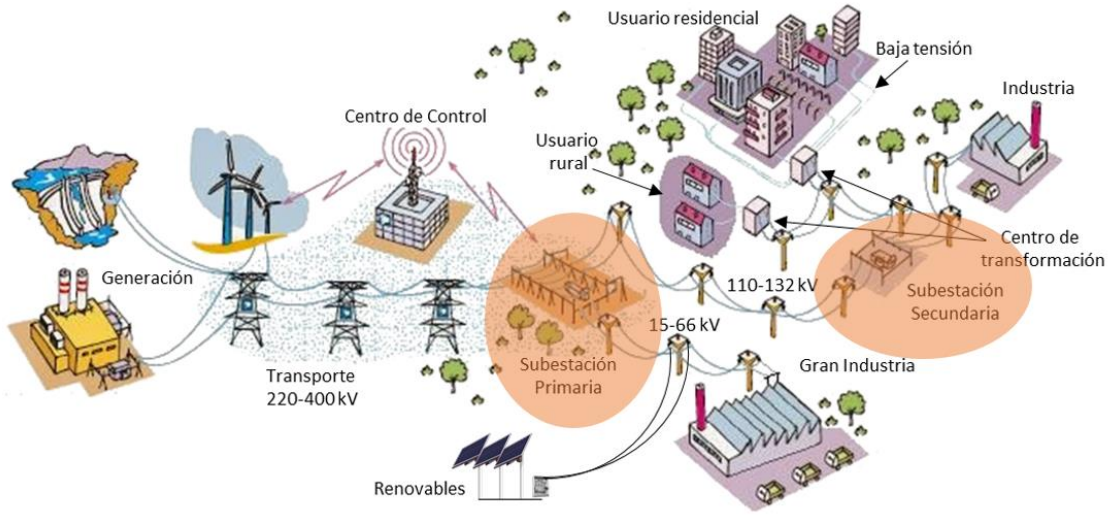


Illustration 2: Explanation of an electrical grid and specifically distribution part, source: Red Eléctrica Española (REE)

2.1 Devices and Systems

Within an electrical distribution substation, different devices of industrial scope can be found, standing out the following:

2.1.1 Gateway

The Gateway allows to translate protocols used in internal communications of the substation to protocols used between the control center and the substation itself (IEC 104). In this case, it can be a fully independent device or a function included in another device.

Some of the most widely used translations at industrial level in the electricity sector are:

- Modbus TCP to IEC 104. (Classic distribution Substations that have undergone a digitization process)
- IEC 61850 to IEC 104. (More modern distribution Substations

2.1.2 HMI – Human Machine Interface

They display process status information for operators to coordinate and control the actions to be performed. Sometimes they allow to adjust the process or to modify its variables.

2.1.3 RTU – Remote Terminal Unit

It is a device that allows to obtain data input from processes and transmit such data to a remote site for further processing. It is found mainly in substations without an electrical automation system and has as many cables as signals are exchanged with its control center.

2.1.4 IED – Intelligent Electronic Device

Devices that handle information extraction. Commonly this information is usually voltage and intensity values that helps to control the electrical substation.

2.1.5 SCADA – Supervision Control and Data Acquisition

These systems carry out real-time monitoring, control and information management within an electrical substation. In addition, they centralize signals generated by one or more industrial processes (alert control) and have the ability to communicate with a multitude of devices located in control networks (PLC, RTU, HMI, etc.).

2.1.6 Industrial switch

Network element that allows communication between devices. Industrial switches, in addition to being ruggedized due its working conditions, also possess the capabilities of more standard switches located in more corporate environments. One of the most commonly used capabilities, besides VLAN creation (802.1Q), is PRP capability for network traffic redundancy.

2.1.7 CSU

The central substation unit centralizes orders and signals from all local control units in every substation position.

2.1.8 Industrial firewall

Cybersecurity devices that manages communications with functionalities such as DPI (Deep Packet Inspection) and DPBI (Deep Packet Behavior Inspection) among others focused on the industrial world. These functionalities allow in-depth inspection of protocols used within substations and in communications with the control center, commonly implemented under IEC-104 protocol.

2.2 Communications

For devices to interact with each other, there must be a series of communications that enable relevant information to be sent on the control and monitoring side. The most prominent protocols that can be found in the electricity sector and specifically in a substation are described below.

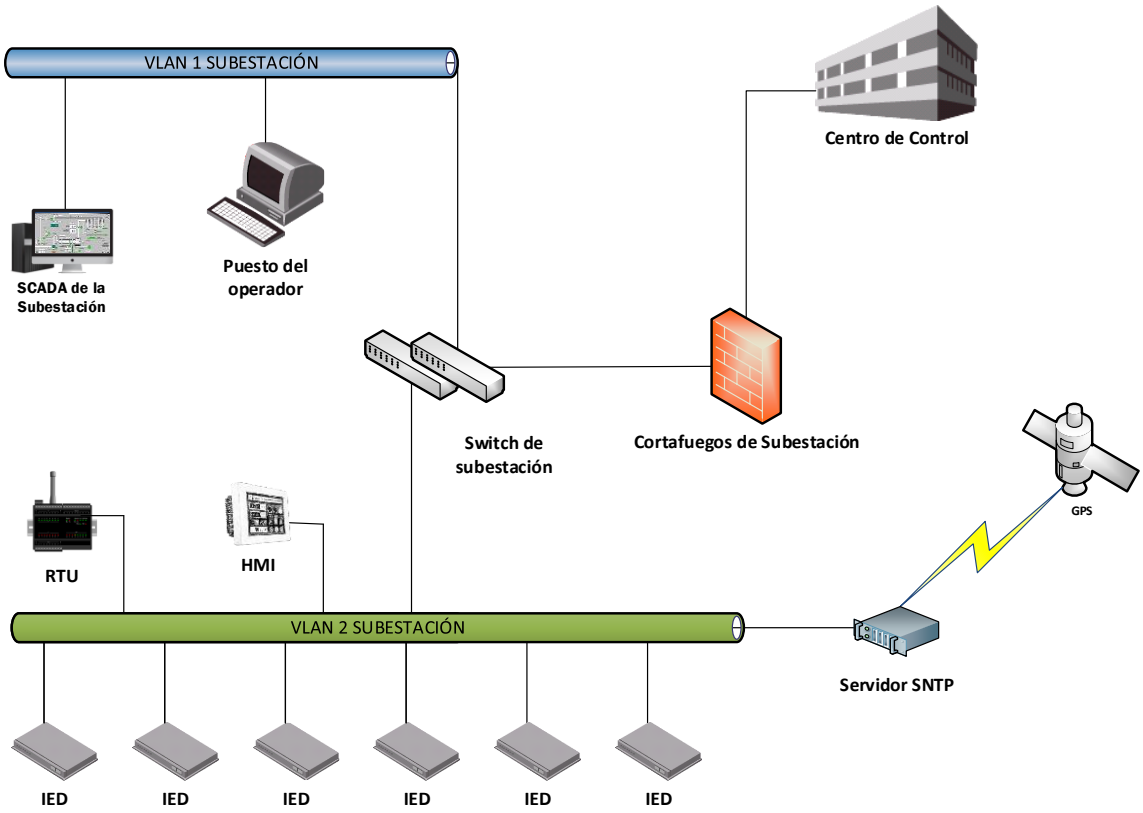


Illustration 3: Example, Distribution Substation Network

2.2.1 IEC 60870-5-104

This protocol is used for communications between substation and control center. It is considered an extension of IEC 101 protocol working on serial communications. Therefore, IEC 104 implements service changes at different levels of the OSI layer (transport, data link and physical), thus getting TCP/IP implementation.

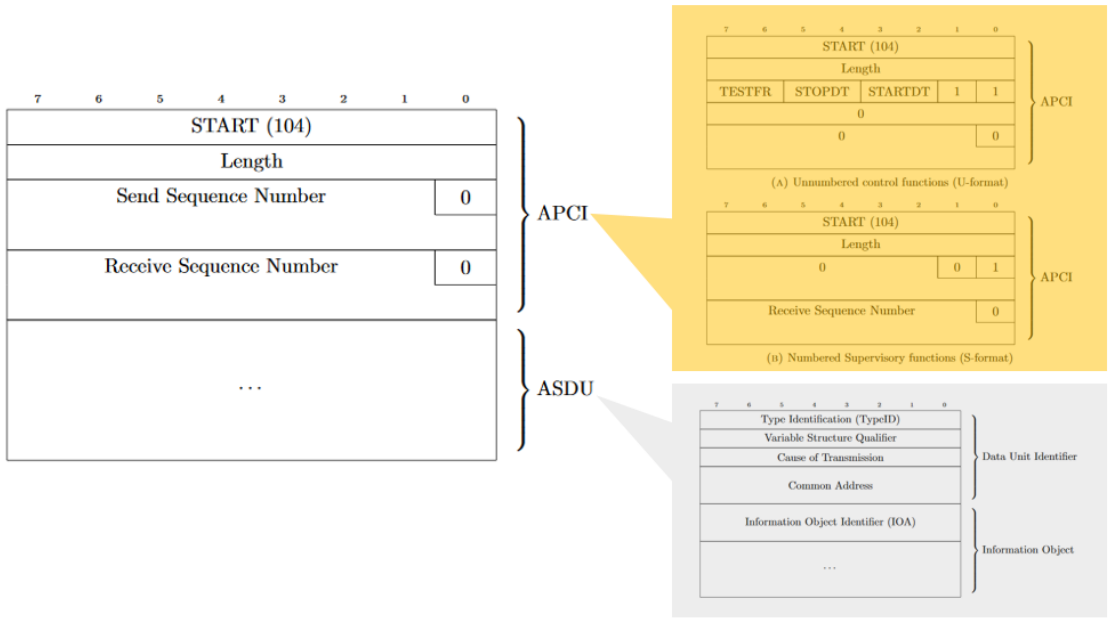


Illustration 4: IEC-104 Protocol Header and Data Section

2.2.2 DNP3 – Distributed Network Protocol v3 (10)

Communication protocol developed in 1993 and commonly used in the USA and Canada. DNP3 is an industrial protocol designed for communications between intelligent equipment (IED) and control stations. Its presence in Europe is scarce due to alternatives such as IEC-60870-5-101 or IEC-60870-5-104.

DNP3 is a three-layer protocol according to the OSI model: Data Link, Application and Transport Layer that does not actually meet all OSI model specifications, and so it is often referred to as Transport pseudo-level. For this reason, it is often mentioned as a two layer or tiered protocol.

Layered or tiered structuring follows the next scheme:

- **Application level messages are called Fragments**. Maximum size of a fragment is set to 1024 bytes.
- **Transport level messages are called Segments**.
- **Data Link level messages are called Frames**. The maximum size of a DNP3 frame is 292 bytes.

2.2.3 Standard Protocol 61850 (11)

IEC 61850 standard is the first of the standards considered as a global solution to the problem between proprietary protocols and different manufacturer devices unable to communicate with each other. This standard defines aspects such as interoperability, protection, monitoring, control and automation of different devices individually and between them. One of the most important objectives in its definition was interoperability, but another very important aspect was cost reduction. For example, it works under a LAN network, which implies reducing cabling and therefore its cost.

The standard is divided into many parts, which cover topics such as communications, data modelling or compliance tests, but none of them about cybersecurity technical aspects. In fact, security related to IEC 61850 is delegated to another standard, specifically IEC 62351.

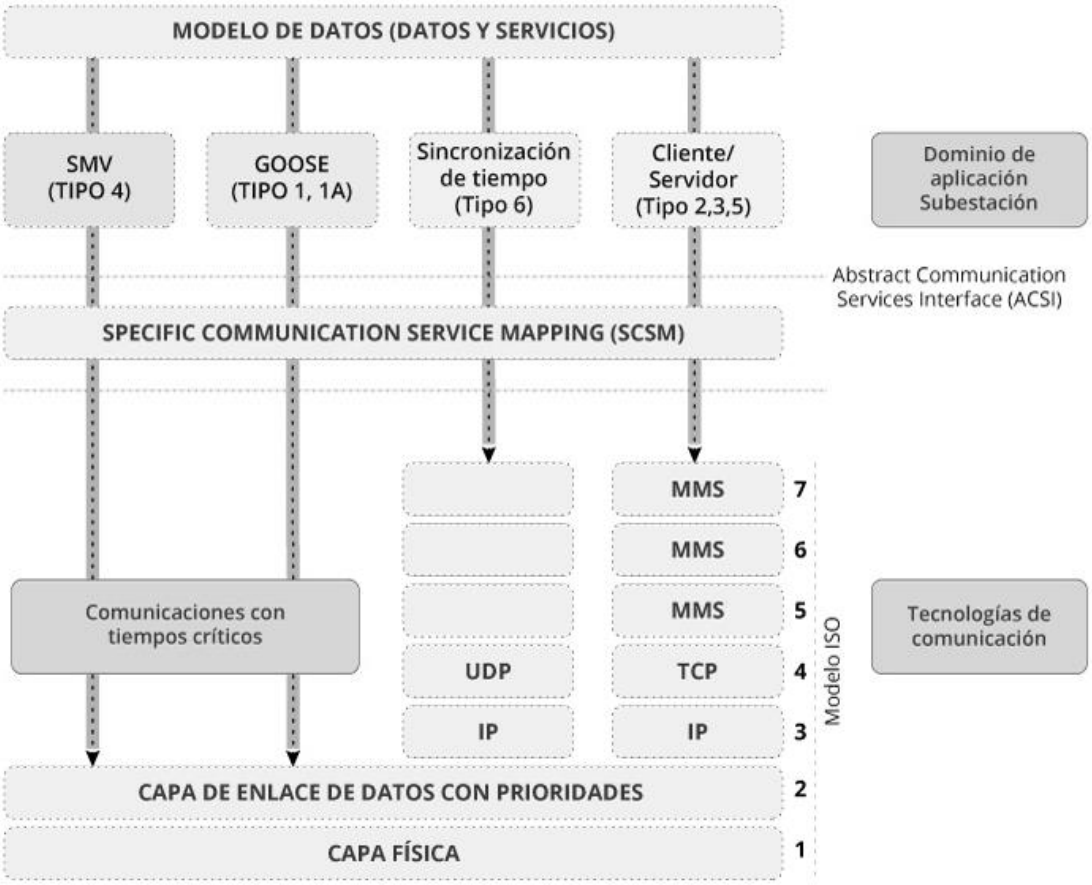


Illustration 5: Standard 61850 Layer Model, source: INCIBE-CERT (11)

- **Sampled Measured Values** is used to provide fast communication of measurement, protection and control values. It works over Ethernet (OSI Layer 2) and messages are encapsulated as multicast, following a Publisher-subscriber structure, where the publisher sends data to all computers on the network and each computer subscribes to the data to access it.

- **GOOSE** is used for real-time transmission of critical events and works, like Sampled Measured Values, via Ethernet multicast messages (OSI Layer 2). GOOSE operating model also follows Publisher-subscriber structure.

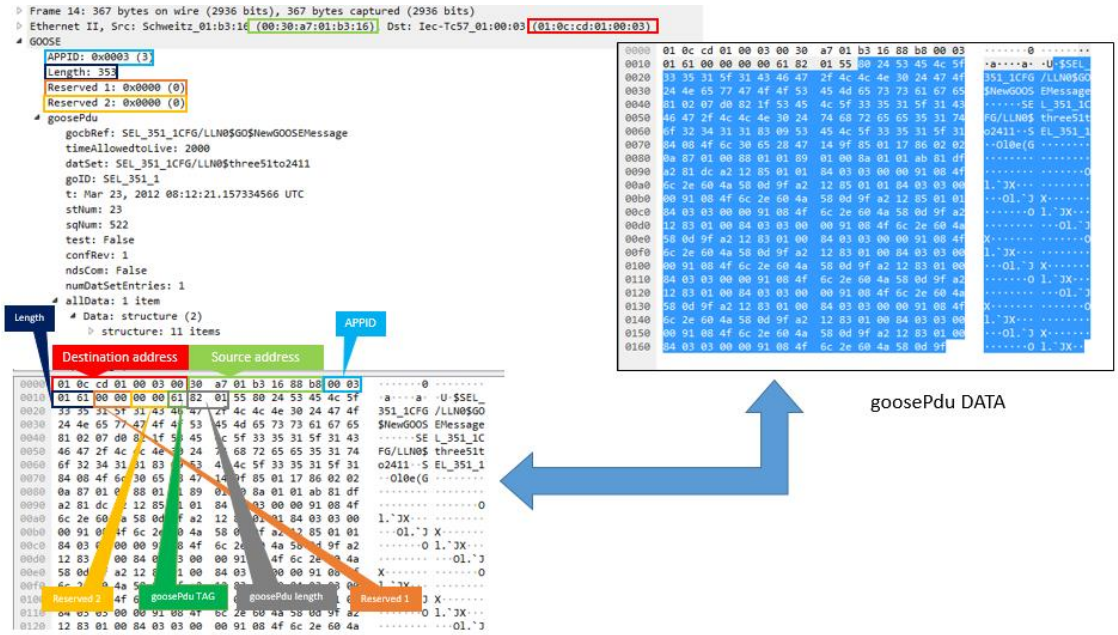


Illustration 6: GOOSE protocol (wireshark) dissector explaining every field defined in such protocol

- **SNTP** protocol is used for time synchronization of the devices. As its name implies, it is a simplified version of the NTP protocol, used on devices that do not need the full functionality protocol. UDP protocol (OSI Layer 4) is used for transmitting SNTP messages.

- Finally, **MMS** protocol is the basis for application data communications in IEC 61850 standard. This protocol sends its messages over TCP connections (OSI Layer 4) and is used for client/server communications. Thus, its purpose is to exchange application data, as well as device configuration parameters or monitoring data.

2.3 Regulations and Standards

In electricity sector as much as other sectors, there are regulations relating to cybersecurity. At this point the most well-known regulations and standards with great maturity in its application to electricity sector are listed below.

2.3.1 ISO 27001

ISO 27001 standard covers different types of organizations whether they be small or large companies, non-profit or governmental organizations, etc. It is therefore not a specific standard only for Energy sector, but it can be drawn several ideas from it when developing some of the controls that will be written on this document.

This standard was developed to show a model when implementing an Information Security Management System (ISMS) in companies following a “Plan-Do-Check-Act” (PDCA) model.

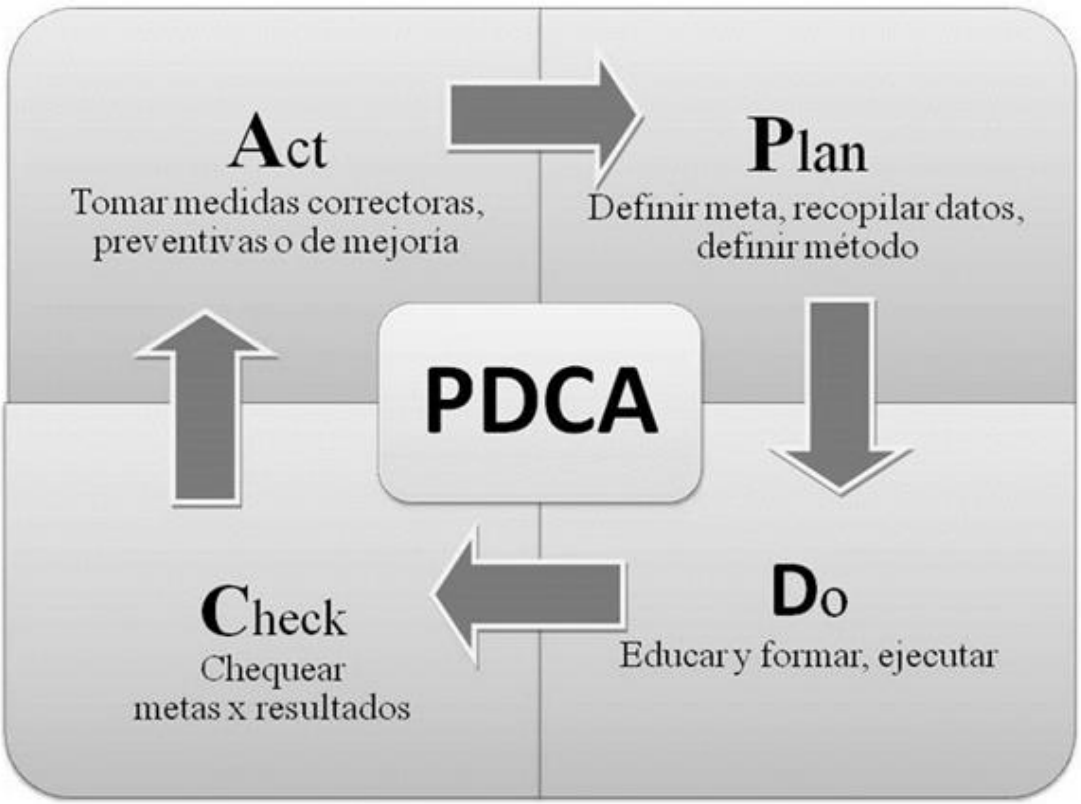


Illustration 7: "Plan-Do-Check-Act" Model

The objective of creating an ISMS is to ensure the three elemental characteristics when protecting information within organizations:

- **Confidentiality**. Information should only be seen by those who have permission to do so, it should not be able to be accessed by personnel without the corresponding authorization.

- **Integrity**. Information may be modified only by those with appropriate right to change it

- **Availability**. Information must be available every time authorized users require access to it.

2.3.2 ISO 27002

ISO/IEC 27002 (formerly ISO 17799) is a standard that provides recommendations for applying a series of best practices in information security management to all people concerned and those responsible for initiating, implementing or maintaining an Information Security Management System (ISMS).

In its new 2013 release, ISO 27002 is presented with 14 domains, 35 control objectives and 114 controls.

Among the new features to highlight that appear in this new version compared to the 2005 one based on 11 domains, 39 control objectives and 133 controls, there can be found a section change of everything related to mobile devices and teleworking associated to Access Control in the 2005 version and to section 6 “Corporate Security Management”. The Access Control section itself includes access to operating systems, applications and information. New domains such as Cryptography (section 10) appear with all the suggested cryptographic controls for an organization. Finally, another change to keep in mind is that disaster recovery cases are in section 17.

In addition, it should be noted that there are specific versions of the ISO/IEC 27002 standard, focused in different types of companies: health care sector (ISO 27799:2016), energy sector (ISO 27019 described in the next point), cloud services (ISO/IEC 27017:2015), among others.

2.3.3 ISO 27019

IEC 27019 standard comes from an information system base (IEC 27002) and provides specific principles and controls for electrical control systems. The objective of ISO/IEC TR 27019:2013 is to extend ISO/IEC 27000 series to the domain of automation and control processes in the electricity sector thus supporting the electricity industry in the implementation of an information security management system.

This standard covers the process of controlling and monitoring power generation, transmission, storage and distribution, in combination with support process control. It includes controls for the following applications and components:

- Control center: IT and monitoring system, as well as automation system.
- Automation components and digital controllers such as PLCs, including actuators and sensors.
- All other IT systems used in domain process control.
- Set of communication technologies used in the control of power supply process (networks, telemetry, remote control applications).
- Remote measurement in the last mile.
- Digital protection and security systems (in products such as PLC for example).
- DER (Distributed Energy Resources) distribution components prepared for future supply connections.
- Software, firmware and applications installed on the aforementioned systems.

Both purely electrical systems (or electromechanical) and telecommunication system are excluded from this standard.

2.3.4 IEC 62351

The action scope of IEC 62351 standard is security in energy sector control operations. Its main objective is to undertake the development of security standards for communication protocols defined by IEC TC 57, specifically IEC 60870-5 (IEC101, IEC104, etc.), IEC 60870-6 (ICCP), IEC 61850 (MMS, GOOSE), IEC 61970 and IEC 61968.

IEC 62351 is divided into 11 separate documents, the first being the introduction to the standard, second one the term glossary and the rest a set of security measures, applied by protocol families. The latest documents attached to the standard define the implementation of measures such as Role Based Access Control (RBAC), key management, secure architecture definition or cybersecurity measures to use with XML files.

Service	Applied Protocol (s) or Applications	Recommendations for security controls
Remote desktop	RDP	Use VPN or IPSec option. RDP has built-in encryption (RC4) and authentication from Windows operating system.
Web-monitor	HTTP	Application of HTTPS for secure Web access.
Web-monitor	Java Applets/Servlets	Application of HTTPS for secure Web access.
Reporting / MMS	IEC 61850	IEC/TS 62351-4 encompasses IEC 61850 and provides end-to-end security for IEC 61850. Alternatively a VPN may be deployed.
Time synchronization	NTP	NTPv3 offers security. Can be deployed using auto-key for key management
Substation – control center communication	IEC 60870-5-104	IEC/TS 62351-4 encompasses IEC 61850 and provides end-to-end security for IEC 61850. Alternatively a VPN may be deployed.
Control center communication	IEC 60870-6 TASE 2 (ICCP)	IEC/TS 62351-4 encompasses IEC 61850 and provides end-to-end security for IEC 61850. Alternatively a VPN may be deployed.
Control center and substation – control center communication	DNP3	Application of DNP3 security measures.
Network management	SNMP	Application of SNMPv3 security measures, support of IEC/TS 62351-7 defined NSM objects, SNMPv2 should only be allowed for monitoring.
File transfer	FTP	Use secure variants like SFTP instead of FTP.

Illustration 8: Cybersecurity approaches to communication protocols in energy sector.

2.3.5 IEC 62443

IEC 62443 standard, developed by TC65 group of the IEC, emerges as an evolution of ISA 99 standard, with the intention of supplementing it and expanding its acting capabilities. One of the main security objectives of IEC 62443 is in-depth defense, deepening the concepts posed by ISA 99 and extending security to other areas from manufacturers to operators.

Cybersecurity in industrial networks is marked by the different levels of the automation pyramid (ISA-95). This standard created the basis for IEC 62443, evolution of the ISA 99, specifically IEC-62443-3-2 “Standard addresses security risk assessment and system design for IACS”, where concepts like “zones” and “conduits” for secure segmentation of industrial networks applying in-depth defense (12) (13) are introduced.

- A **Zone** is defined as the logical or physical grouping of industrial assets (such assets can be physical, applications or information) which share the same security requirements.

- A **Conduit** is a particular type of zone responsible for grouping communications that allows information to be transmitted between different zones.

This standard consists of a total of 13 documents, some of them already officially published and the rest in draft status. In turn, documents are divided into 5 technical reports, 1 technical specification and 7 guides, grouped into four blocks according to their content: General, Policies and Procedures, Systems and Components.

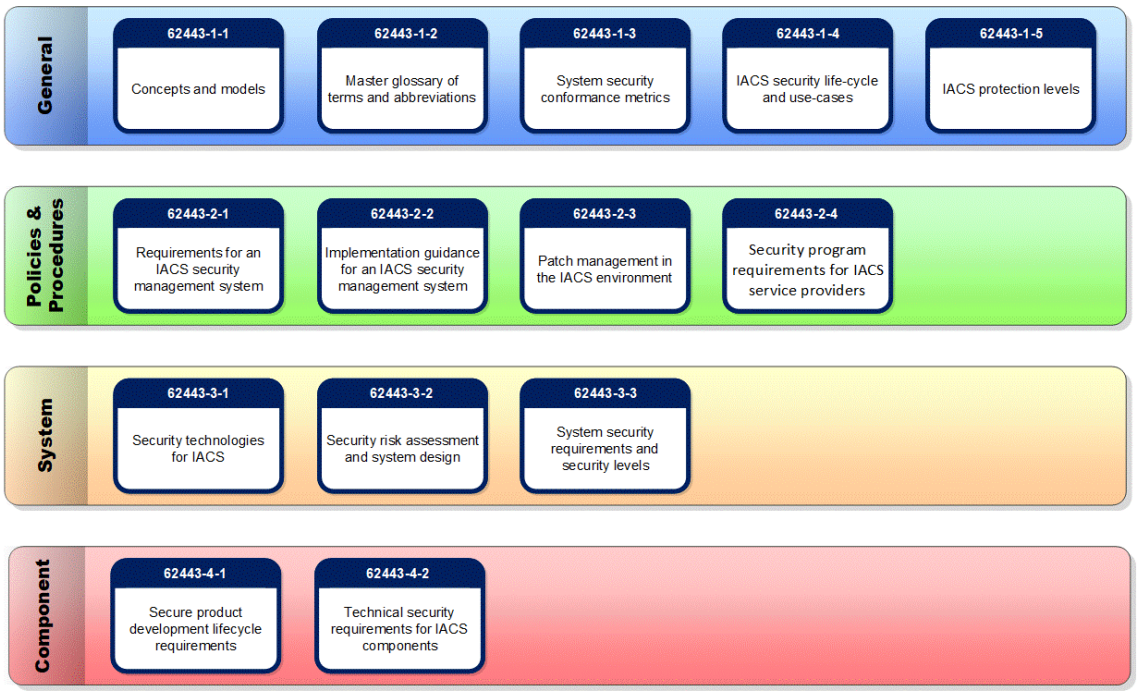


Illustration 9: IEC 62443 Documentation

2.3.6 NERC CIP

NERC is the regulatory body for the U.S. Energy sector. This agency created a series of mandatory guides to assess the security of facilities and the sector in general. Nine guides were created originally, all but the first related to cybersecurity, subsequently expanding total number to 12. Version 5 is currently in effect meanwhile version 7 is being developed.

This standard recognizes the different roles of each entity in the operation of the electrical system, criticality and asset vulnerabilities that make them up and the risks they are exposed to.

Among the types of organizations that must obey this standard, there are distribution companies that have within their networks assets considered in this standard, therefore directly affecting the objectives pursued by this document.

2.4 Threats in electricity sector

The incorporation of new technologies that allow better monitoring of industrial networks and the different defensive solutions that are being incorporated in the industrial world, facilitate malware detection. Following Stuxnet infections, different industrial companies have begun to develop and incorporate cybersecurity measures to their networks in order to prevent new infections.

The challenge of defending against a potential advanced threat is quite complex as attackers use fairly advanced tactics to prevent the detection of anomalous behaviors.

Recently, a number of industrial-level pieces of malware targeting the electricity sector have been detected. Among other actions, pieces of malware detected performed information exfiltration, transmitting control frames with industrial protocols, etc. It should be noted that after the analysis of these pieces of malware, a rather professional development was detected since some of them were modular and these modules were loaded by communication with the C&C (Control Center).

2.4.1 Actors and attack vectors in industrial environments

Among the different actors that can cause an industrial incident resulting from some motivation such as revenge, terrorism, industrial espionage, sabotage, etc. the following can be found:

- **States or Nations**: Their objectives are fully studied and attacks are caused for specific reasons as happened in the Stuxnet case, to stop the Iranian nuclear program.

- **Insiders:** Disgruntled employees seeking mainly economic benefits by using their knowledge of the internal network, devices, etc. of the company they work for. These employees may act on their own or motivated by third-party companies offering money in exchange for information or sabotage.

- **Terrorists:** Their main objective is to generate social panic through attacks targeting critical infrastructures used by a large part of the population. An example of such attacks occurred in The United Kingdom in 2018 when The Islamic State, Daesh, attempted to modify the parameters of a water treatment plant.

- **Cybercriminals:** The goal that such actors are looking for is an economic Benefit through attacks such as using ransomware to demand a ransom for encrypted data or cause anomalies within industrial networks. Sometimes these groups are motivated by political ideals or simply infect industrial networks after a large network infection campaign.

With some of the most important actors in industrial-level attacks already presented, it is time to learn about the most commonly used attack vectors in malware campaigns, where APT (Advanced Persistent Threat) is mostly used:

- **Malicious attachments:** Virtually all of the latest malware detected in industrial control systems possesses an email with malicious attachments as its attack vector. Much of these attachments need features such as Office macros or JavaScript activation in documents to infect the target.

- **Spear phishing:** a phishing variant that involves sending messages, usually specific and personalized emails to a particular group of people, in order to obtain sensitive information or infect the device used by the victim. This is the main difference from traditional email phishing, which involves sending the same email in bulk and at random to millions of users.

- **Watering hole:** this technique consists in conducting a study of the profile or organization to attack, in order to detect which websites are often used by their victims. Once detected, these websites will be scanned for vulnerabilities that can be exploited to compromise the website and thus being able to infect its visitors through different existing resources, malicious URLs, etc.

- **Large Attack Surface:** this attack vector is often accompanied by a lack of knowledge of the published networks and services that some organizations have, increasing their exposure level on the Internet. In other cases, such as GreyEnergy with its web servers, the organization is aware that its services are public and accessible from the Internet, but do not apply the appropriate cybersecurity measures regarding to segmentation or hardening of hosts providing public services.

2.4.2 BlackEnergy 3

Since its first detection in 2007, from being a trojan in its beginning, whose objective was none other than infecting computers to create a botnet and perform distributed denial of service attacks, BlackEnergy has evolved into an Advanced Persistent Threat (APT).

In 2014, variations arise that limit kernel mode only for its malicious upload or directly disabling it by loading it with rundl32.exe process, this version is known as BlackEnergy Lite

In 2015, BlackEnergy added Win32/KillDisk.NBB, Win32/KillDisk.NBC and Win32/KillDisk.NBD variations remaining its final version as the one used it in the attack suffered by Ukraine at the end of this year.

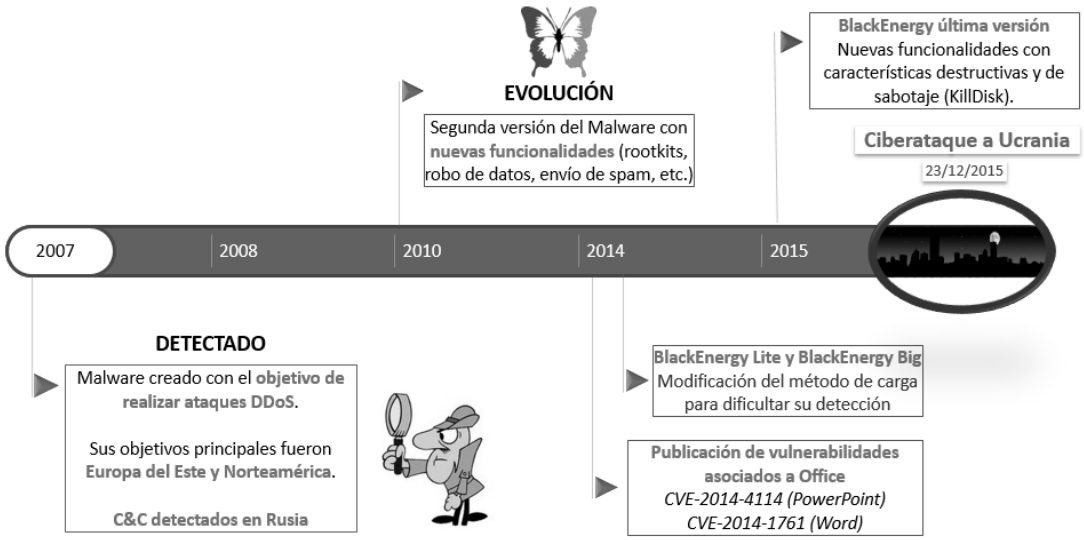


Illustration 10: BlackEnergy evolution over time until the attack in Ukraine

The infection vector was originated thanks to a spear phishing simulating Ukrainian government entities that sent emails with malicious attachments. This attachment had an Excel worksheet with a macro that ran if macro options were enabled rebuilding an executable file associated with this malware.

The dropper's malicious upload is a DLL executed by rundll32 and creates an LNK file allowing persistence after a reboot. In the upload, process a connection to the C&C server is performed.

Once its target was infected, the malware spread to the control network where it caused an anomalous behavior by opening and closing electrical switches with IEC-104 commands and eventually causing an electrical substation breaking down in the middle of winter (14).

2.4.3 CrashOverride/Industroyer (15)

It is a modular malware focused on organizations that use IEC101, IEC104, IEC61850 and OPC protocols. This specialization already implies a clear objective on the electricity sector. At operational level, CrashOverride used features previously detected in the three main control system malware that have appeared to that date (end of 2017).

- It imitates STUXNET in the way it understands and represents industrial process knowledge, coding it to interrupt operations.
- System Architecture is mapped using OPC protocol, just as HAVEX/Dragonfly did.
- It also follows in the wake of BlackEnergy2 when it comes to reviewing HMI libraries and configuration files to understand the environment and try to connect to the internet when possible.

Among other capabilities, CrashOverride was able to (16):

- Send commands directly to RTUs using industrial protocols, including opening and closing breakers (substation switches) quickly and continuously just like BlackEnergy.

- Block serial ports on Windows computers, preventing communications from legitimate devices to affected computers.

- Perform network Discovery using OPC protocol and greatly improving its success probability through a port scanner.

- It has the ability to exploit a known vulnerability of Siemens SIPROTEC relays, which can lead to a denial of service.

- Includes a wipe module (deletes logs and any other file that can be tracked or specific files) that leaves Windows systems useless and requires a rebuild or backup to get them running again.

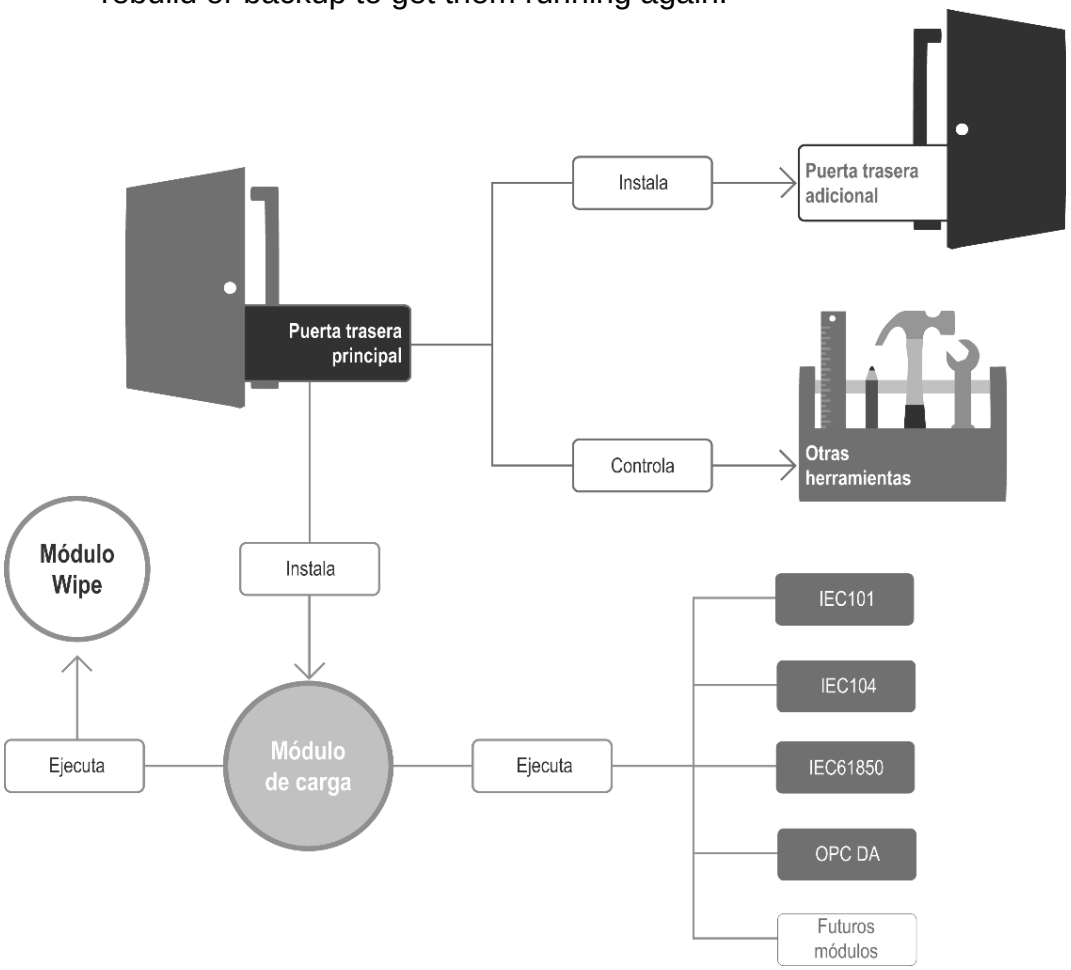


Illustration 11: CrashOverride functioning

2.4.4 DragonFly 2.0

Dragonfly 2.0 was an industrial-level malware campaign aimed at infiltrating in infrastructures in the energy sector. In this campaign, cyberattackers used different attack vectors to gain access to energy companies that included sending malicious emails (phishing) with trojanized attachments. In addition, they used

backdoors that allowed continuous access to industrial infrastructures being able to modify the infected devices due to the Control Centers (C&C) they used.

2.4.5 GreyEnergy

This piece of malware is considered an evolution of BlackEnergy, hence its name. Its attack vector used was the sending of custom emails with infected attachments (spear phishing), besides as a novelty, they also compromised company websites to be able to carry out, among others, watering hole attacks.

After an initial infection with a mini dropper called GreyEnergy Mini, it opened the way to perform new infections and afterwards downloading the malware in its entirety, GreyEnergy.

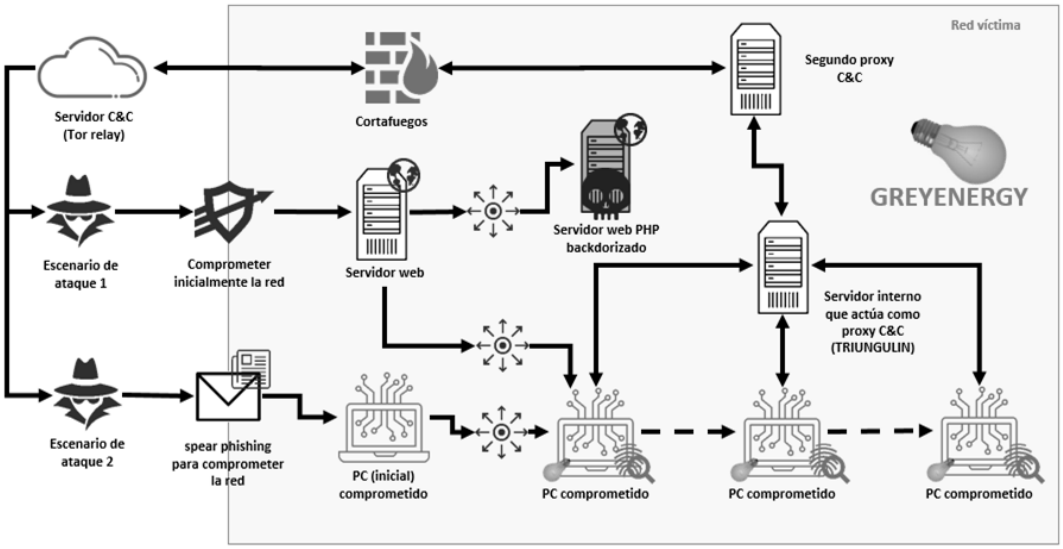


Illustration 12: GreyEnergy Infection Process

An ESET investigation (17) on this piece of malware did not observe any Industrial Control System (ICS) module. However, it was detected that GreyEnergy attackers had been strategically targeting workstations related to ICS environments running SCADA software. These stations or servers are typically critical systems that are meant to be never disconnected, except in maintenance cases.

3 Attack Taxonomies, Cyber Kill Chain and CAT

An attack taxonomy can be described as a set of phases or stages that allow to analyze a cyberattack suffered by a particular environment. This in-depth analysis allows incident response teams to act based on cyberattack severity and actions executed within it.

3.1 Cyber Kill Chain (CKC)

Among these taxonomies, Cyber Kill Chain (CKC) (18), designed by Lockheed Martin Corporation, stands out. This taxonomy consists of a seven phased sequence, which characterize the different phases of an advanced attack. This model identifies the steps that adversaries must complete to achieve their goal, focusing on the network, data exfiltration and how to maintain organization resilience.

Since all intrusions leave some kind of trace behind, it is important to detect them and classify all actions in order to be able to learn from all of them. At forensic level, there is a well-known principle called “Locard’s Exchange Principle”, such principle holds that in any crime its perpetrator will introduce an element and take something from it. Therefore, both elements will serve as evidence. By extrapolating this principle to a cyberattack, attackers will leave evidence (logs, communications, log modifications, etc.) and quit with information or other elements that will later betray them.

Once these concepts are known and returning to Cyber Kill Chain taxonomy, these are the phases that such chain possesses:

- **Reconnaissance:** Search, research, identification and selection of the objective(s). This phase may consist of recognition with passive open source analysis techniques or active recognition of Internet-accessible systems for potential vulnerabilities.

- **Weaponization:** Include or mask malware to allow remote access to attackers and also loading of exploits or modules that will be used in the exploit phase. Office suite or malicious PDF documents are typically used to achieve this goal.

- **Delivery:** Sending and receiving the payload it is an important phase in this taxonomy. The most commonly used delivery routes are usually email with attachments, malicious websites or removable media such as USB devices.

- **Exploitation:** The exploit executes the payload, previously sent to the victim. Such phase can point to a specific vulnerability, specific features of an application or operating system used, etc. Exploitation can also involve social engineering techniques to attack a very specific target directly.

- **Installation:** Installing a Trojan or backdoor to remotely access the system allows the attacker to maintain a certain presence in the attacked environment. In this phase, persistent memory techniques are often used to prevent losing communication if the compromised system is rebooted.

- **Command & Control:** Outbound communications from a server controlled after an infection with internet connection, directly or indirectly, to establish a Command and Control (C&C) channel. Such channel will allow attackers to have remote access to the compromised systems, load modules improving the persistent threat, etc.

- **Actions on Objectives:** The last taxonomy phase in which concrete actions such as extraction of confidential data, information modification, compromising additional systems, network lateral movements, etc. will be performed.

There are different variants to the previously mentioned chain. One of them is the extended version that includes:

- **Internal Reconnaissance:** Phase in which attacker has access to a device deployed on the internal network of the attacked organization. Thanks to such access the attacker can analyze local files, network traffic, browser history, stored passwords, etc. Its goal is to find out how the infected device could help to map organization's internal network and allow it to attack more interesting targets.

- **Internal Exploitation:** Using information obtained from the victim system, attackers can take advantage of a lack of patches against specific vulnerabilities used in protocols or specific applications, etc. to perform lateral movements between networks or devices on the same network, scaling privileges or manipulating systems.

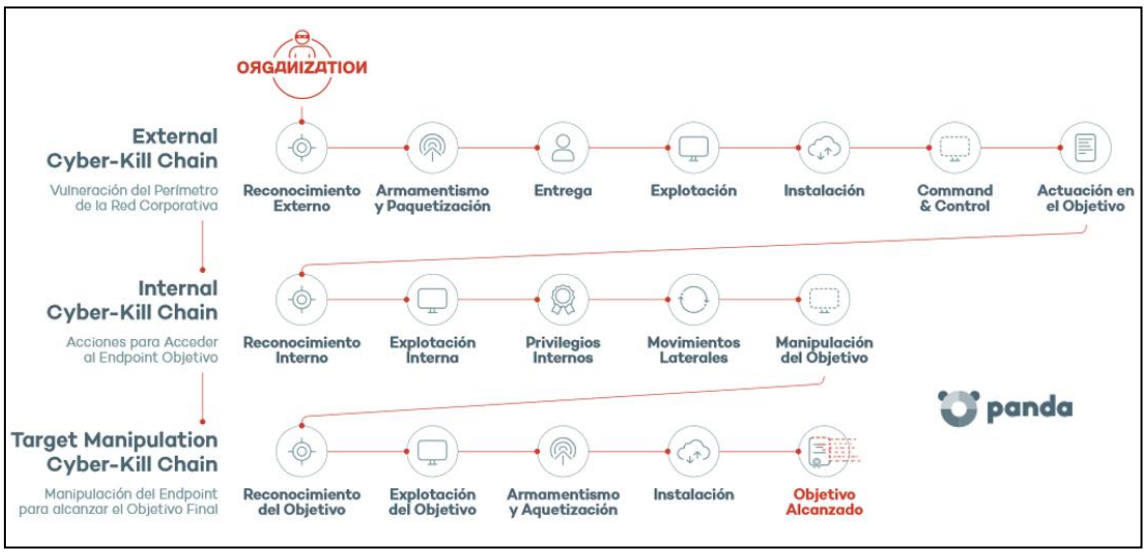


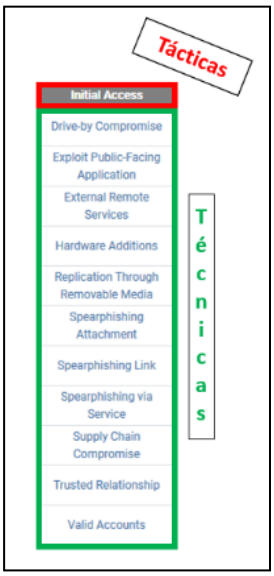
Illustration 13: Extended Cyber-Kill Chain Taxonomy (19)

In a

In addition to the Lockheed Martin Corporation taxonomy, there are other models that allow a better understanding of these attack, all of them with its particularities and stages.

#	Unified Kill Chain	Cyber Kill Chain® (CKC)	Lalliberte	Nachreiner	Bryant	Malone	MITRE ATT&CK™	UKC after literature study	UKC after Red Team C1	UKC after Red Team C2	UKC after Red Team C3	UKC after Red Team KC	UKC after APT28 C4 & KC
1	Reconnaissance	1	1	1	1	1		1	1	1	1	1	1
2	Weaponization	2	3	3	3	2		2	2	2	2	2	2
3	Delivery	3	5	5	6	3		7	7	3	3	3	3
4	Social Engineering	5	6	6	11	5		3	3	4	4	4	4
5	Exploitation	6	8	8	14	6		5	4	5	5	5	5
6	Persistence	8	14	9	18	8	6	6	5	6	6	6	6
7	Defense Evasion	18	18	14	16	10	11	8	6	7	7	7	7
8	Command & Control			18		5	7	9	8	8	8	8	8
9	Pivoting					11	13	11	9	9	9	9	9
10	Discovery					14	10	10	11	11	11	10	10
11	Privilege Escalation					17	14	14	10	10	10	11	11
12	Execution					18	12	12	14	14	14	12	12
13	Credential Access						15	13	12	12	12	13	13
14	Lateral Movement						16	17	13	13	13	14	14
15	Collection						8	15	17	17	17	17	15
16	Exfiltration							16	15	15	15	15	16
17	Target Manipulation								16	16	16	16	17
18	Objectives												18

Illustration 14: Different models developed or derived from CKC taxonomy, source: The unified kill chain



One of the most used models nowadays that many companies are starting to incorporate into their incident response exercises when modelling some attacks is called MITRE ATT&CK (21), developed by MITRE (20). This model is bases on an array (Enterprise) that contains current tactics and techniques used by cyberattackers when developing persistent threats. It is important to note that, although it is called matrix, it is simply a series of columns whose initial row contains the tactic's name and subsequent rows including techniques.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data Staged	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data from Removable Media	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-Stage Channels		Runtime Data Manipulation
	LSASS Driver	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	SSH Hijacking	Screen Capture	Multi-hop Proxy		Service Stop
	Launchctl	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Stored Data Manipulation
	Local Job Scheduling	Create Account	Launch Daemon	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation
	Mshta	DLL Search Order Hijacking	New Service	DLL Side-Loading	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking	Path Interception	Deobfuscate/Decode Files or Information	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		

Illustration 15: Part of the MITRE (Enterprise) matrix where techniques and tactics of adversaries can be observed

Besides Enterprise matrix, MITRE currently offers:

- **PRE-ATT&CK** (22): This matrix is a summary of the tactics and techniques described in the PRE-ATT&CK model. It visually aligns individual techniques under the tactics in which they can be applied. Some techniques cover more than one tactic because they can be used for different purposes.

Priority Definition Planning	Priority Definition Direction	Target Selection	Technical Information Gathering	People Information Gathering	Organizational Information Gathering	Technical Weakness Identification	People Weakness Identification	Organizational Weakness Identification	Adversary OPSEC	Establish & Maintain Infrastructure	Persona Development	Build Capabilities	Test Capabilitie
Assess KITs/KIQs benefits	Assign KITs, KIQs, and/or intelligence requirements	Determine approach/attack vector	Acquire OSINT data sets and information	Acquire OSINT data sets and information	Acquire OSINT data sets and information	Analyze application security posture	Analyze organizational skillsets and deficiencies	Analyze business processes	Acquire and/or use 3rd party infrastructure services	Acquire and/or use 3rd party infrastructure services	Build social network persona	Build and configure delivery systems	Review log and residu traces
Assess current holdings, needs, and wants	Receive KITs/KIQs and determine requirements	Determine highest level tactical element	Conduct active scanning	Aggregate individual's digital footprint	Conduct social engineering	Analyze architecture and configuration posture	Analyze social and business relationships, interests, and affiliations	Analyze organizational skillsets and deficiencies	Acquire and/or use 3rd party software services	Acquire and/or use 3rd party software services	Choose pre-compromised mobile app developer account credentials or signing keys	Build or acquire exploits	Test ability evade automate mobile applicatio security analysis performed app store
Assess leadership areas of interest	Submit KITs, KIQs, and intelligence requirements	Determine operational element	Conduct passive scanning	Conduct social engineering	Determine 3rd party infrastructure services	Analyze data collected	Assess targeting options	Analyze presence of outsourced capabilities	Acquire or compromise 3rd party signing certificates	Acquire or compromise 3rd party signing certificates	Choose pre-compromised persona and affiliated accounts	C2 protocol development	Test callba functionali
Assign KITs/KIQs into categories	Task requirements	Determine secondary level tactical element	Conduct social engineering	Identify business relationships	Determine centralization of IT management	Analyze hardware/software security defensive capabilities		Assess opportunities created by business deals	Anonymity services	Buy domain name	Develop social network persona digital footprint	Compromise 3rd party or closed-source vulnerability/exploit information	Test malwa in various execution environmen

Illustration 16: Matrix covering early phases of a cyberattack

- **Mobile** (23): These are 2 device-specific ATT&CK matrixes, one for tactics and techniques related to device access, and the other one for network originated effects that can be used for attackers without access to such devices.

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Effects	Collection	Exfiltration	Command and Control
Deliver Malicious App via Authorized App Store	Abuse Device Administrator Access to Prevent Removal	Exploit OS Vulnerability	Application Discovery	Abuse Accessibility Features	Application Discovery	Attack PC via USB Connection	Encrypt Files for Ransom	Abuse Accessibility Features	Alternate Network Mediums	Alternate Network Mediums
Deliver Malicious App via Other Means	App Auto-Start at Device Boot	Exploit TEE Vulnerability	Disguise Root/Jailbreak Indicators	Access Sensitive Data in Device Logs	Device Type Discovery	Exploit Enterprise Resources	Generate Fraudulent Advertising Revenue	Access Calendar Entries	Commonly Used Port	Commonly Used Port
Drive-by Compromise	Modify OS Kernel or Boot Partition		Download New Code at Runtime	Access Sensitive Data or Credentials in Files	File and Directory Discovery		Lock User Out of Device	Access Call Log	Standard Application Layer Protocol	Standard Application Layer Protocol

Illustration 17 Matrix related to device access

Network Effects	Remote Service Effects
Downgrade to Insecure Protocols	Obtain Device Cloud Backups
Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Exploit SS7 to Track Device Location	
Jamming or Denial of Service	
Manipulate Device Communication	
Rogue Cellular Base Station	
Rogue Wi-Fi Access Points	
SIM Card Swap	

Illustration 18: Matrix related to effects caused by a network attack (devices)

This model, like many others, is oriented towards Information Technology world and therefore not entirely suitable for industrial control systems, due to the system nature and attack typology. However, there are adaptions that allow its application in industrial environments.

Like the model developed by MITRE, Lockheed Martin Corporation attack taxonomy was designed for IT world. However, at the end of 2015, SANS institute published a report (24) adapting the Cyber Kill Chain model to control systems. Such report details the expansion phase of the original Intrusion Kill Chain to better suit industrial environment characteristics, as well as splitting it into two stages.

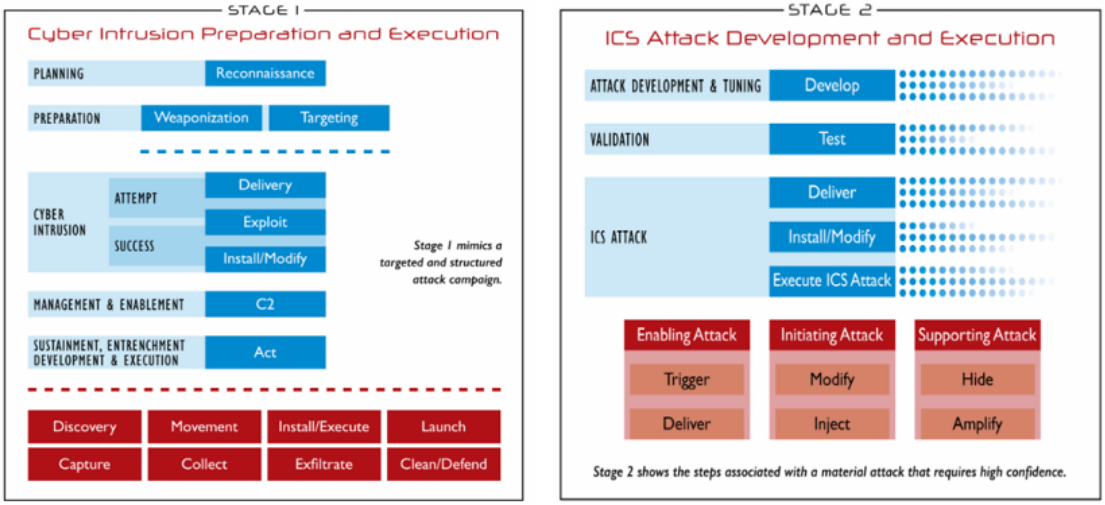


Illustration 19: Adapting CKC model to control systems, source: SANS

First stage, quite similar to the original model previously explained, corresponds to what has traditionally been classified as espionage or intelligence operations.

For its part, in the second stage, knowledge collected in the first stage is taken advantage of to develop a targeted attack, not requiring an immediate succession after first stage, there may be a delay between both stages. The typical phases of this industrial environment oriented Cyber Kill Chain scenario are:

- **Attack development and tuning:** With this phase begins the second stage, in which the attacker tries to create a new capability (procedure, tool, method, etc.) that specifically affects the targeted control system. The development of this attack will possibly be performed thanks to the exfiltrating data and information collected over a long time about the victim industrial environment. For this reason, there are delays in malicious operations to be executed.

- **Validation:** This phase aims to certify the new capability in an environment similar to or equal to the one intended to attack. Typically, the attacker acquires specific hardware to carry out this phase. Within this stage, an attacker performs simulations of the attack to be carried out. This is a major challenge, given the complexity of simulating an entire industrial control system.

- **Attack on the industrial control system:** Last phase consists of the attack on the industrial control system itself. Here, the attacker tries to distribute the developed capacity, install it or modify the system's behavior to be exploited and execute the attack. Common consequences of an attack on control systems are data loss, denial of service and data manipulation, visualizations, etc.

Like Cyber Kill Chain attack taxonomy, Enterprise matrix developed by MITRE also has an adaptation for industrial environments. Such adaptation consists of techniques and tactics drawn from some attacks at industrial level like those defined in *"Threats in electricity sector"*. These advanced threats allow to specify techniques and tactics only used in industrial environments when developing an attack. However, some techniques are shared with more corporate environments since, in the industry, similar or directly same technologies can be found but adapted to industrial environments.

An example of such matrix can be seen below with CrashOverride malware:

Persistence	Privilege Escalation	Defense and Operator Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control	Disruption	Destruction
External Remote Service	Exploitation of Vulnerability	Alternate Modes of Operation	Brute Force	Account Enumeration	Default Credentials	API Interaction	Automated Collection	Automated Exfiltration	Commonly Used Port	Alternate Modes of Operation	Alternate Modes of Operation
Firmware	Loadable Module	Block Comm Port	Create Account	Control Process	Exploitation of Vulnerability	Alternate Modes of Operation	Data Staged	Data Compressed	Communication Through Removable Media	Block Comm Port	Block Command Message
Interactive Service	Valid Accounts	Block Reporting Message	Credential Dumping	File and Directory Enumeration	External Remote Service	Command-Line Interface	Data from Local System	Data Encoding	Connection Proxy	Block Command Message	Block Reporting Message
Loadable Module	Web Shell	Code Signing	Credentials in Files	I/O Module Enumeration	Man in the Middle	Exploitation of Vulnerability	Data from Network Service	Data Encrypted	Custom Command and Control Protocol	Block Reporting Message	Command-Line Interface
Modify Control Logic		Exploitation of Vulnerability	Default Credentials	Local Service Enumeration	Remote File Copy	Graphical User Interface	Data from Network Share	Data Transfer Size Limits	Custom Cryptographic Protocol	Command-Line Interface	Device Shutdown
Modify System Settings		File Deletion	Exploitation of Vulnerability	Location Identification	Replication Through Removable Media	Interactive Service	Data from Removable Media	Exfiltration Over Alternative Protocol	Data Encoding	Device Shutdown	Exploitation of Vulnerability
Module Firmware		Inhibit Security Tools/System	Input Capture	Network Connection Enumeration	Taint Shared Content	Loadable Module	Screen Capture	Exfiltration Over Command and Control Channel	Data Obfuscation	Exploitation of Vulnerability	Firmware
Non-Interactive Service		Man in the Middle	Intercept Multi-Factor Authentication	Network Enumeration	Third-party Software	Modify System Settings	Video Capture	Exfiltration Over Other Network Medium	Exfiltration Over Command and Control Channel	Firmware	Man in the Middle
Rootkit		Masquerading	Modify Account	Network Service Enumeration	Valid Accounts	Non-Interactive Service	Web Service	Exfiltration Over Physical Medium	Fallback Channels	Man in the Middle	Masquerading
Scheduled Task		Memory Residence	Network Sniffing	Network Sniffing	Virtual Terminal Services	Scheduled Task		Scheduled Transfer	Multi-Stage Channels	Masquerading	Modify Control Logic
Valid Accounts		Modify Control Logic	Password Manager	Role Identification		Scripting		Virtual Terminal Services	Multiband Communication	Modify Control Logic	Modify Parameter
Web Shell		Modify Event Log	Private Keys	Serial Connection Enumeration		Third-party Software			Multilayer Encryption	Modify Parameter	Modify Physical Device Display
		Modify Event Log Settings				Virtual Terminal Services			Remote File Copy	Modify Physical Device Display	Modify Reporting Message
		Modify HMI/Historian Reporting				Web Shell			Standard Application Layer Protocol	Modify Reporting Message	Modify Reporting Settings
		Modify Parameter							Standard Cryptographic Protocol	Modify Reporting Settings	Modify Tag
		Modify Physical Device Display							Standard Non-Application Layer Protocol	Modify System Settings	Module Firmware
		Modify Reporting Message							Uncommonly Used Port	Modify Tag	Rootkit
		Modify Reporting Settings							Virtual Terminal Services	Module Firmware	Spoof Command Message
		Modify Security Settings							Web Service	Rootkit	Spoof Reporting Message
		Modify System Settings								Spoof Command Message	
		Modify Tag								Spoof Reporting Message	
		Rootkit									
		Spoof Reporting Message									

Illustration 20: CrashOverride Modeling with MITRE Matrix (25)

3.2 CAT – Cyber Attack Taxonomy

In this Project, the CAT attack taxonomy (26) is introduced. This taxonomy is born from an open source project under Creative Commons Attribution 4.0 International (27) license, therefore, both documentation and information are released and accessible on the Internet.

This taxonomy is currently in development and was created by Mildrey Carbonell Castro and Francisco Luis de Andres Perez. It defines a series of strategies, tactics, techniques and procedures that allow to have a more complete view of cyberattacks.

Illustration 21: CAT phases, source: S21sec (28)

CAT has 7 phases that allow attack modelling. Such modelling allows, among other things, understand attacks executed by cybercriminals nowadays and provides incident response teams a powerful tool to understand them.

1. **Target Profiling:** Initial phase of the taxonomy where the target chosen by the attackers is analyzed. This phase will take into account the exposure of the target selected by the attackers and the possible entry routes when making a first approach to subsequently execute the attack.

This phase is based on two types of analysis:

- **Macro analysis or PESTLE** (29)**:** Consists of the Political, Economic, Social, Technological, Legal and Environment (PESTLE) Study. It lists current threats that are subjected to, sector to attack or geographical location where are located, among others. It allows to replicate attacker techniques and therefore gaining enough knowledge to replicate such attack.

- **Micro analysis:** Focused exclusively on target exposure analysis. The three main factors of exposure are analyzed: people, processes and technologies. It should always be taken into account that people are often the weak link when choosing a target.

2. **Compromise:** At this stage, attacker(s) attempt to obtain an attack vector through which they will infiltrate or simply exploit a vulnerability to cause actions such as denial of service, remote code execution, etc.

In the above-mentioned malware that affect industrial control systems, social engineering is commonly used: phishing, spear phishing, watering hole, etc.

This phase can also constitute the start and end of an attack, going directly from the compromise phase to the target impact execution phase, as with DoS or DDoS attacks, where system availability is compromised (final goal) but the attacker has no interest in accessing his victim's systems (infiltration is not carried out). Such attacks also occur in industrial control systems, but they imply that the attacker does not use advanced techniques or it can simply be a distraction to execute a more elaborate attack.

3. **Infiltration:** Success in this phase depends directly on the compromise phase. If the initial compromise phase is successful, the attacker can begin to take action to, among other things, obtain a direct communication channel with the target undetected and in that way continuing to perform malicious actions they deem appropriate. Such actions include installing backdoors, using Trojans, etc.

   As in previous ones, this stage can be the end of an attack, damaging the confidentiality, integrity or availability of the asset, such as modifying a website, data from a DB, restarting systems, changing configurations that cause malfunction, etc.

4. **Persistence:** Once compromised the target(s), many pieces of malware use concealment techniques to avoid being detected by protection systems. Monitoring tool use is quite common therefore, attackers usually invest a lot of time in developing this phase.

   Persistent memory or using wipe modules for trail removal are some of the techniques used in this phase. Let us remember that, in the industrial world, pieces of malware active for years are beginning to being detected. In this line, attackers whose targets are industrial environments, use their knowledge of such environments to select assets like engineering stations or PLC devices since shutdown of these equipment is not very common. Many industrial equipment run for years without stop only being shut down to perform maintenance actions.

5. **Internal Reconnaissance:** An important phase if the attacker wants to know the environment surrounding the already compromised victim device. In this stage, an attacker can start detecting all existing network devices, assets on the same network as the victim device, similar devices to the already hacked one to have a higher number of victims, etc.

   Techniques such as network traffic capture or ARP table query are often used in industrial control systems to obtain as much information as possible without raising suspicions. This way, attackers keep collecting information to continue infecting devices without trace.

6. **Lateral movements:** This is the phase in which the attacker, based on the results obtained in the previous phase, infects new targets on the same network as the already hacked device or attempts to infect devices on other networks.

   It is very common in industrial malware that infection begins with corporate environment, obtains information about existing network devices (routers, switches, firewalls, etc.) and tries to reach industrial environment due to lack of segmentation or some direct communication between the corporate network and an uncontrolled industrial network. In many cases, attackers have greater knowledge of the victim network than the attacked company itself.

7. **Target Impact Execution:** The ultimate goal typically pursued by attacks is to make the most impact on their victim. At the same time, it is also common for the impact to generate benefits to attackers or third parties. For example, Stuxnet malware served to stop the development of Iran's nuclear program, BlackEnergy rendered a power substation in Ukraine out of service, etc.
   Factors that often influence this impact are industrial espionage, cyberterrorism, information leakage, loss of trust on the customers the victim may have, etc.

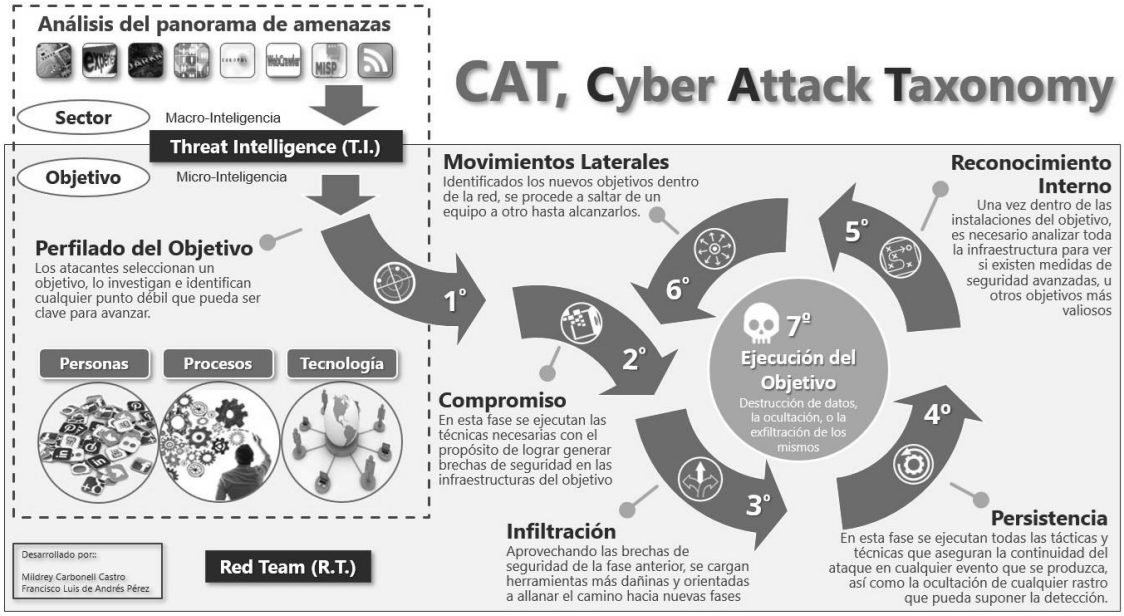


Illustration 22: CAT taxonomy phases

This taxonomy has been developed so that it can be adapted to any environment, whether corporate or industrial. Along this project, a number of adaptations can be observed using CAT with some of the most well-known industrial incidents closely related with electricity sector, specifically in the distribution part.

CAT is based on a DML (Detection Maturity Levels) (30) model. This model was originally used to describe organization's maturity in terms of dealing with and acting on an information of a given threat. Such information may include Indicators of Compromise (IoC), Tactics, Techniques and Procedures (TTPs),

intelligence reports and much more. This model emphasizes the abstraction level of incident response teams and their maturity level combined with technical skills they may have.

Another important point to keep in mind about CAT is that it is enriched with other models such as the one developed by MITRE or Pwnwiki's (31). Thanks to such enrichment, CAT is able to define strategies, tactics, techniques, procedures and tools further deepening at technical level and helping both attack and defense teams more accustomed to using MITRE matrix or Pwnwiki.

Illustration 23: Approach to CAT methodology following DML model, source: Modeling cyberattack scenarios with CAT methodology, Hack&Beers Alicante vol.5

3.3 Cyber Kill Chain vs. CAT

Both are defined as attack taxonomies, but the reality is that, model posed by Lockheed Martin besides being older than CAT taxonomy, has generated great controversy since some deficiencies have been detected. The fact that CAT taxonomy, being a more modern model can be seen as an advantage, since it takes into account details that Cyber Kill Chain does not.

One of the major problems detected in the Cyber Kill Chain modelling is precisely the concept of chain: a lineal approach without loops in which a predetermined structure is followed and presupposes that all attacks will follow the same structure either until the end of phases or it will remain in a previous phase.

On the other hand, and following the problem argumentation related to the Cyber Kill Chain model, weaponization phase does not make much sense when cannot be used to create defensive measures. This phase depends entirely on the attacker as is the one who will develop the malware and will choose both tools and any other details to use. Taking into account the industrial environment adaptation, some of the phases added in the second stage, besides the already one mentioned in the first stage, also do not make sense at defensive level.

Both attack development and tuning phase and validation phase, due being related to the attacker or the evolution of the attack itself for industrial environments, do not have any application at defensive level. In attack development and tuning phase, the attacker creates new capabilities specifically designed for industrial environments. For its part, in the validation phase, custom development for industrial environments is verified by simulating attacks in an environment as close as possible to the real one. Victim's devices deployed in their industrial network are used in this phase.

Another deficiency detected in the original Cyber Kill Chain model is the absence of a phase that takes into account lateral movements. Nowadays virtually all pieces of malware incorporate this phase allowing them to achieve greater propagation and impact within the victim organization. It is true that some variants of the original mode posed by Lockheed Martin incorporate lateral movements, but they are not either official or registered models so they will not be taken into account.

Cyber Kill Chain (CKC)	Cyber Attack Taxonomy (CAT)
Chain concept, linear attacks that follow marked and preset phases.	Possibility to create loops and not follow a linear path to model an attack.
Phases such as *weaponization* do not allow a defensive approach to the modelling offered.	It shows all phases consistently by incorporating the strategic part that provides coherence to all described movements a malware could run.
The official registered model does not take lateral movements into account correctly.	CAT allows, once again thanks to the strategic part, to detect lateral movements and a better visual representation.
It has variants for the industrial sector but they are not industry-specific and are based on a legacy IT thinking.	It allows to adapt new TTPs or incorporate specific frameworks such as the one intended in this project (*caffeine*).

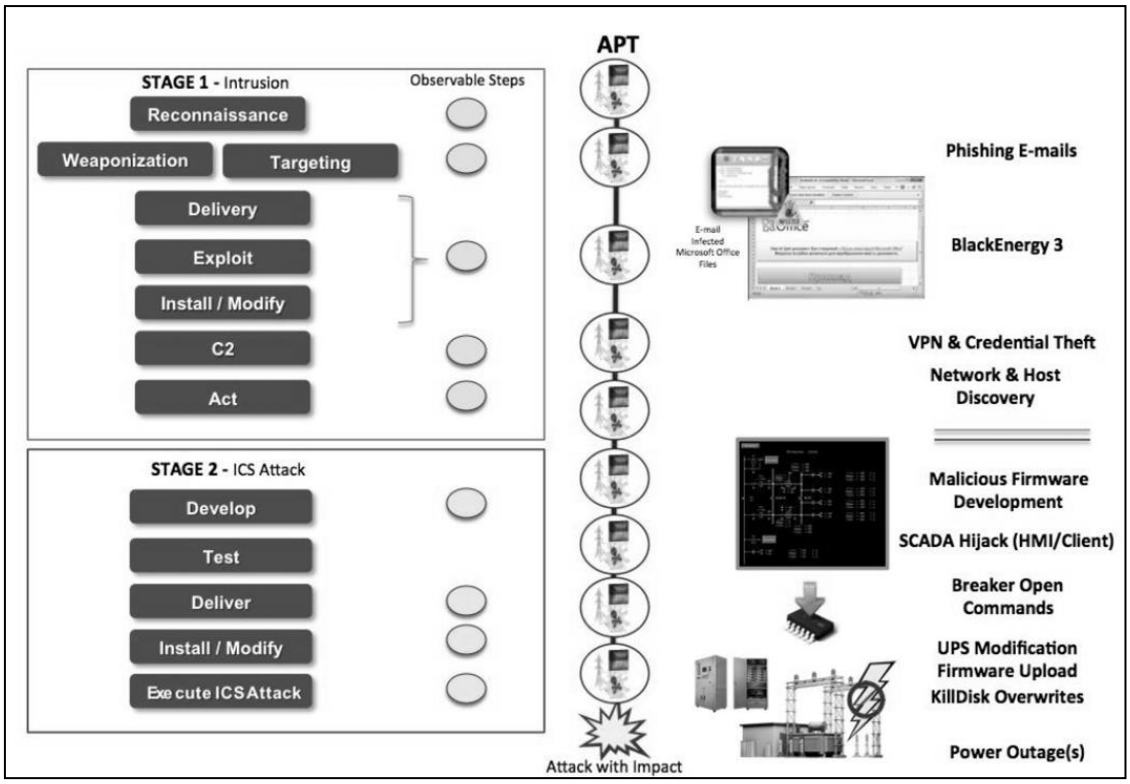


Illustration 24: BlackEnergy mapping with Cyber Kill Chain Modeling for Industrial Control Systems, source: Analysis of the Cyber Attack on the Ukrainian Power Grid (32)

To conclude, another much commented problem related to the modelling posed by Lockheed Martin. Internally originated attacks by possible insiders (33), disgruntled employees with sufficient power and knowledge of the organization's network and resources to execute an attack, cannot be easily represented.

One of the most well-known industrial cases of such attacks internally originated by a disgruntled employee occurred at a water treatment plant in Australia (34). In this case, the insider used a laptop equipped with appropriate control software and a radio modem. The way to access the system was to connect the laptop to the pumping station system trying not to be detected. As a result, liters of residual waters were dumped into rivers and parks, in addition to the discredit to the company in charge of managing the sewerage. The employee was sentenced to 2 years in prison for illegal access to the County sewer control system, which he performed due to being fired from that company

For its part, CAT is a fairly current model, but with a large argumentative base, it does not have great criticism except those raised by its own developers or people who help in its improvement.

CAT aims not only to cover the strategic part as attack taxonomy for strategic phases and methodology, but to have a framework part to unite tactics, techniques and procedures just as MITRE does.

The novelty in this area is the incorporation of the strategy. Defined as the planning and operation development that tactics will later use. The incorporation of strategy is very important since nowadays attackers are highly organized and

hierarchized. Attacks on industrial environments are the proof, since it is necessary a multidisciplinary team, with knowledge in different fields and specialties, to develop the malware used in these environments.

Currently, organized crime is more and more like a company where there are different roles with team leaders, developers, etc. Furthermore, the fact that some attacks are motivated by national interests, money invested to develop a malware can be quite considerable.

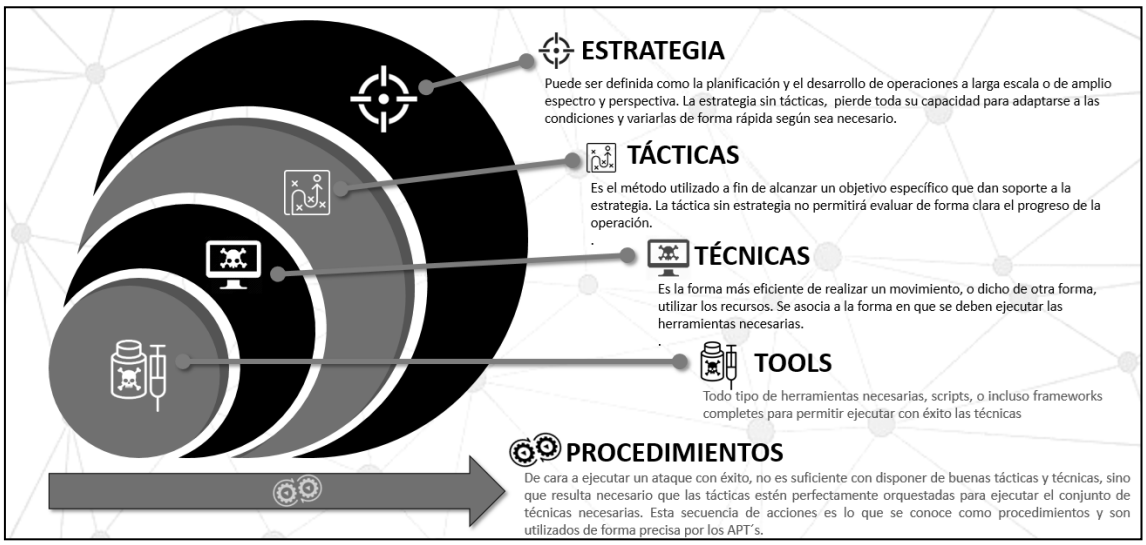


Illustration 25: Strategy, tactics, techniques and CAT procedures, source: Modeling cyberattack scenarios with CAT methodology, Hack&Beers Alicante vol.5

4 Cyberattack Framework for Electricity Sector

The development of this framework, main objective of this project, aims to facilitate the work of teams oriented to the offensive world within cybersecurity in industrial environments, and specifically in the energy sector and electricity subsector (distribution). Being about production environments since availability and safety of the personnel is its primary concern, it is important to consider certain guidelines before performing any offensive task in these environments.

- **Low or zero impact on process availability**. Industrial companies are often very cautious in this regard because, for example a shutdown of an electrical substation that provides power to a large inhabited area would result in a large economic loss and discredit. Therefore, it is advisable to perform offensive tasks in controlled maintenance situations such as discharges.

    - **Discharge:** Situation in which a network installation (line, transformer, bar, etc.) is disconnected from the rest of the electricity system and therefore no electrical power can circulate through it. It is a common practice when part of the electrical installation must remain without voltage and in safe conditions to work in or near it.

  On the other hand, and considering that a loss of availability on a node when performing a load balancing is a critical operation, Red teams, during network tests, should consider such attacks against nodes as a training for operators, always keeping in mind the service availability.

    - **Node balancing:** Practice used in electricity sector to balance power in substations depending on consumer needs. Electricity management in these cases is usually related to environmental issues (extreme cold, high temperatures, etc.) and on demand.

- **Personal Protective Equipment for the offensive team.** Within an electrical substation, certain safety measures are mandatory to prevent work accidents. Therefore, the offensive team must comply with all these measures. Some of such measures are: use of regulatory footwear, helmet, gloves, etc. In meetings prior to conducting offensive tests, the team will be informed by the customer of the safety measures they must comply.

- **Knowing the environment to attack**. The offensive team must be aware of the environment to be attacked, different devices existing within an electrical substation, exchange protocols and regulations affecting such sector. Much of this information can be found in sections **¡Error! No se encuentra el origen de la referencia. ¡Error! No se encuentra el origen de la referencia.**, 2.2 Communications and 2.3 Regulations and Standards.

4.1 Using framework, and what now?

In section 3.2 CAT – Cyber Attack Taxonomy, CAT taxonomy is already introduced for modelling attacks or red team approaches. It brings certain advantages over the one posed by Lockheed Martin and for this reason has been chosen to elaborate this framework. But, what does this taxonomy provide to the framework? The answer is simple, it provides the necessary classification tools with strategies, techniques, tactics and procedures that allow to replicate advanced attacks. At this point 2 advantages can be found, one for the defending teams (blue teams) and another for the attacking teams (red teams). From a defensive point of view, all processed information in the modelling, and ending with the information sharing phase where compromise indicators are developed, snort rules (35), yara rules (36), etc. allow to detect similar threats to those already analyzed. On the other hand, from an offensive point of view, the threats analyzed can be replicated in order to test systems and devices involved in a certain process.

Since there are already different analyses for both IT level attack modellings and scenarios that can be modeled in a case with different taxonomies, main objective of this project, developed in following sections, is to provide a series of guidelines for attackers who wish to perform red team exercises in electrical substations making the environment real and in production. Likewise, an attack modelling will be performed to show all possible CAT applications in industrial environments.

4.2 CAT in industrial environments, *caffeine*

Since CAT methodology already has a framework, but not oriented to industrial environments, this project's contribution is the Caffeine framework (Cyber-Attack Framework for Energy Infrastructures) that is proposed as a framework to incorporate in the github project that CAT owns. Within this framework different strategies, tactics, techniques and procedures can be found, specific to industrial control systems and in particular electricity sector (distribution) shared with CAT framework, MITRE matrix, PwnWiki, etc.

Mostly, specific techniques will be proposed for attack executions in industrial environments. An example of such techniques under the discovery tactic (TA0007) can be seen in detail below:

Tactic	Name - ID	Name	Description
Discovery (TA0007)	**CAFT0001**	**Information through industrial protocols**	Sending packages specifically designed to use industrial protocols in order to obtain certain information about industrial devices over the network, as in the examples below: **Ethernet/IP, obtaining information** – Using industrial protocol Ethernet/IP to obtain information over TCP and UDP port 44818. **Modbus TCP, obtaining information** – Using Industrial protocol modbus TCP to obtain information over TCP port 502. **Factory Interface Network Service (FINS), Discovery and obtaining information** - Use of FINS protocol to obtain PLC information in industrial networks. This protocol works under both TCP and UDP port 9600. **S7, obtaining information** – Use of industrial protocol S7 to obtain information over TCP port 102. **IEC 61850-8-1, mms protocol for obtaining information** - Use of industrial protocol mms to obtain information over TCP port 102. **IEC 60870-5-104 for obtaining information** - Use of industrial protocol

			IEC 60870-5-104 to obtain information over TCP port 2404.

Among others, tools that can be used to execute the above technique are:

Tactic	Technique_ID	Tool	Description
Discovery	**CAFT0001**	enip-info.nse	Script developed in lua for nmap. IT sends a request to TCP port 44818, used by the Ethernet/IP protocol and parses information such as device type, manufacturer ID, product name, serial number, device status, etc. ***Example of Use*** `nmap --script enip-info -sU -p 44818 <host>`
		modbus-discover.nse	Script developed in lua for nmap. It lists slave IDs (sids) and collects device information. ***Example of Use*** `nmap --script modbus-discover.nse --script-args='modbus-discover.aggressive=true' -p 502 <host>`
		omron-info.nse	Script developed in lua for nmap. It sends a FINS package to the device containing a control command for parameter reading. If the command is valid, the device responds with information that will be parsed by the script and displayed on screen. ***Example of Use.*** `nmap --script omron-info -sU -p 9600 <host>`
		s7-info.nse	Script developed in lua for nmap. It lists and obtains information about Siemens S7 PLCs in a network.

			Example of Use `nmap --script s7-info.nse -p 102 <host/s>`
		mms-identify.nse	Script developed in lua for nmap. It verifies that protocol IEC 61850-8-1 is actually used over TCP port 102 and then sends a request to extract information from the device. ***Example of Use*** `nmap -d --script mms-identify.nse --script-args='mms-identify.timeout=500' -p 102 <host>`
		iec-identify.nse	Script developed in lua for nmap. It verifies that protocol IEC 60870-5-104 is actually used over port 2404 and performs a communication test against the device to obtain information about stored object addresses. ***Examples of Use*** `nmap -sV --script=iec-identify <target>`

Obviously, there are alternatives to these tools such as PLCScan (37) or mbtget (38).

In case of wanting to send IEC104 requests, a metasploit module can be used for this purpose (39) allowing to establish communication and send packages to interact with the device or obtain information.

Caffeine framework, being part of the CAT methodology, has both tactics and techniques typical of industrial environments and specifically energy sector, electricity subsector (distribution) as well as tactics and techniques of MITRE, PwnWiki, etc. Tactics and techniques that are their own, have been created to facilitate attack modelling to red teams and therefore, if they match already written ones can be used within the framework using MITRE nomenclature for example, where tactics start with *TAXXX* and techniques follow *TXXXX* nomenclature. On the other hand, tactics and techniques used exclusively in the *caffeine* framework will use *CAFTAXXXX* for tactics and *CAFTXXXX* for techniques.
CAFTAXXXX para tácticas y *CAFTXXXX* para técnicas.

4.3 Cyber-Attack Modelling scenarios with CAT for electrical sector (*caffeine*)

An advanced attack is proposed to modify parameters received in the SCADA control center by spoofing an RTU sending 104 communications. To achieve this, the red team has been able to introduce a device within the substation using social engineering techniques and supplanting the identity of supposed operators of the company which the electrical substation belongs to. The device introduced into the network has 4G capabilities that allow remote control and contains an advanced tool suite related to industrial world and specifically to the electricity sector. Taking advantage of 0-day vulnerabilities in the RTU, red team has been able to make the necessary modifications to supplant the RTU and send parameters with the device introduced into the network.

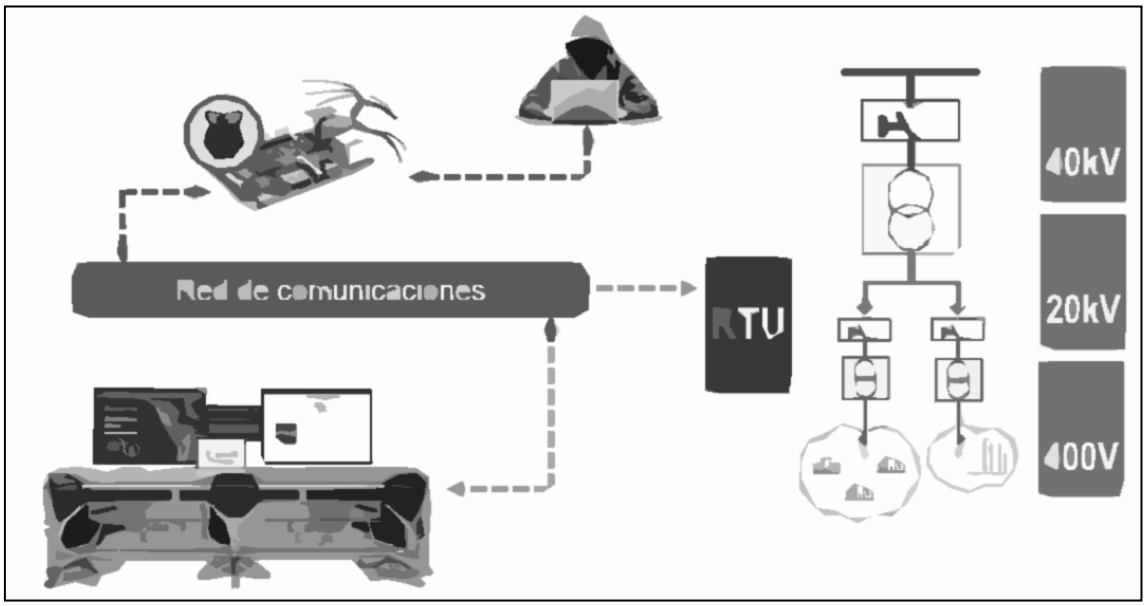


Illustration 26: Hypothetical network situation of the proposed scenario

This scenario would be represented with CAT as follows:

Tactics, Techniques and Tools

CAT phase	Tactics	Techniques	Tools
Target Profiling	TA001: Target Selection	T1245: Determine approach/attack vector T1242: Determine operational element T1241: Determine strategic target	Web search engines that allow to get information on the Internet such as Google, Bing, etc. Searching for information in specialized forums. Tool usage like Theharvester (40) or Shodan (41). More tools: https://github.com/jivoi/awesome-osint

Target Profiling	TA0016 – People Information Gathering	T1266: Acquire OSINT data sets and information T1272: Identify business relationships T1268: Conduct social engineering T1273: Mine social media	Web search engines that allow to get information on the Internet such as Google, Bing, etc. Use of Facebook, Instagram and Pinterest to gather information. Tool usage like Theharvester (40) or Shodan (41). More tools: https://github.com/jivoi/awesome-osint
Target Profiling	TA0017 - Organizational Information Gathering	T1300: Analyze organizational skillsets and deficiencies T1303: Analyze presence of outsourced capabilities	Searching for information in specialized forums. More tools: https://github.com/jivoi/awesome-osint
Target Profiling	TA0015 - Technical Information Gathering	T1247 - Acquire OSINT data sets and information T1249 - Conduct social engineering	Specific searches in forums and obtaining information thanks to dialogue and social engineering techniques.
Compromise	TA0001 – Initial Access	T1200 - Hardware Additions	Use of picklocks for executing lock picking techniques. Operator uniform of the attacked company. Finally, device to be introduced into the network substation (raspberry pi 3).
Infiltration	TA0011 – Command and Control	T1052 - Exfiltration Over Physical Medium	Installing a stick USB 4G on the device introduced into the substation network to maintain communication and exfiltrate information.
Infiltration	TA0011 – Command and Control	T1043 - Commonly Used Port T1105 - Remote File Copy	Command Shell like netstat, ifconfig, pas –aux, top, etc. with sh, ash (common in busybox), bash and other interfaces. Information copy using FTP or another protocol with ftp command or programs like filezilla.
Persistence	CAFTA001 - external power	CAFT003: use of external	To prevent possible device shutdowns, use external batteries powerful enough to endure the

		battery with solar cells	whole time target is being attacked.
Internal Reconnaissance	TA0007 – Discovery.	T1254 - Technical Information Gathering CAFT0001 - Information through industrial protocols T1254 - Conduct active scanning	mms-identify.nse and iec-identify.nse
Lateral Movements	TA0008- Lateral Movement	T1078 - Valid Accounts T1037- Logon Scripts	Use device documentation where default passwords are listed or controlled brute force attacks to avoid raising suspicion. Dictionary to use scadapass (42).
Target Impact Execution	CAFTA0002 - Cheat the control center	CAFT0002: Modification of parameters by industrial protocols	Use of scapy library for sending custom packages, developing specific scripts, using metasploit module that supports IEC104 communications. Simulate RTU communications to deceive SCADA system or send single/double command requests in EC104.

Procedures

A strategic substation of a company based in Spain has been selected, classified as critical infrastructure given the large territory to which it provides electricity. Another reason because is classified as critical is that provides electricity to one of the most important hospitals with a huge number of patients in Spain.

1. Introduce the malicious device, previously configurated, into the substation. Within the device, in this particular case a raspberry pi 3, all kind of libraries and applications required to run the desired tests can be found. When introducing the device, it is necessary to know the victim's network since it is possible to discover a flat network and the device to be inserted does not need to be introduced directly within the substation.

2. Gather more information about the network and devices within it thanks to 4G communication between the device introduced in the victim organization (raspberry pi 3) and the attacker's computer.

3. Once victim device has been detected, access and make the appropriate modifications to be able to supplant it with our introduced device. Such

access can be done thanks to knowledge of the device's vulnerabilities or studying manuals provided by the manufacturer where default credentials are listed. If credentials have been modified, brute force or custom attacks can be performed.

4. Sending erroneous signals and SCADA collapse. Using IEC104 protocol, employed between electrical substations and control networks, the attacker can send specific requests that will result in a loss of network visibility between an RTU and the SCADA located in the control center. In addition, control commands such as single or double command can be transmitted, depending on the size of the information to be sent to interact with the system.

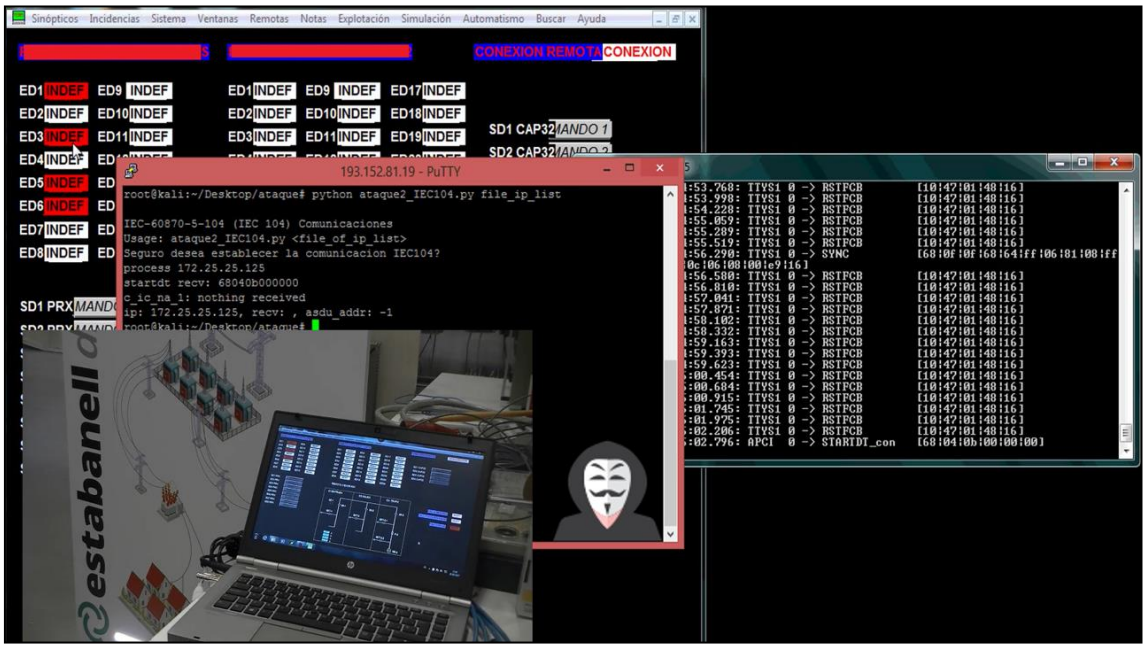


Illustration 27: Cyberattack performed using IEC-104 commands spoofing a RTU in its communication towards SCADA

4.4 From a defensive point of view…

The above scenario will mainly serve offensive teams (red teams) but it does not mean that they cannot be used by defensive teams (blue teams) in order to prevent or already have a response plan against previously modelled scenarios thanks to Compromise Indicators, Yara and Snort rules, etc.

In this case, regulatory compliance affecting the industrial system to which defensive support is provided, electricity sector in our case, must be taken into account, as well as procedures against this type of attacks affecting a particular sector.

Among the positive points that can be drawn from defensive point of view of posing scenarios for offensive teams to attack we will have:

- **Training for incident response teams.** By analyzing different scenarios that an attacker or attacking team can execute, defensive teams can take

it as training exercises. With this training response incident teams or blue teams will be able to improve their real field experience making their service more efficient in the face of real attacks.

- **Improved procedures and response times.** Since it is possible to know both the steps executed by attackers and the impact that the attack will have on the supported industrial systems, incident response teams or blue teams will be able to improve their response times and better procedurize the tasks to be performed depending on the type of attack detected.

For the above mentioned attack scenario, a network-level mitigation can be applied using an IDS such as Snort.

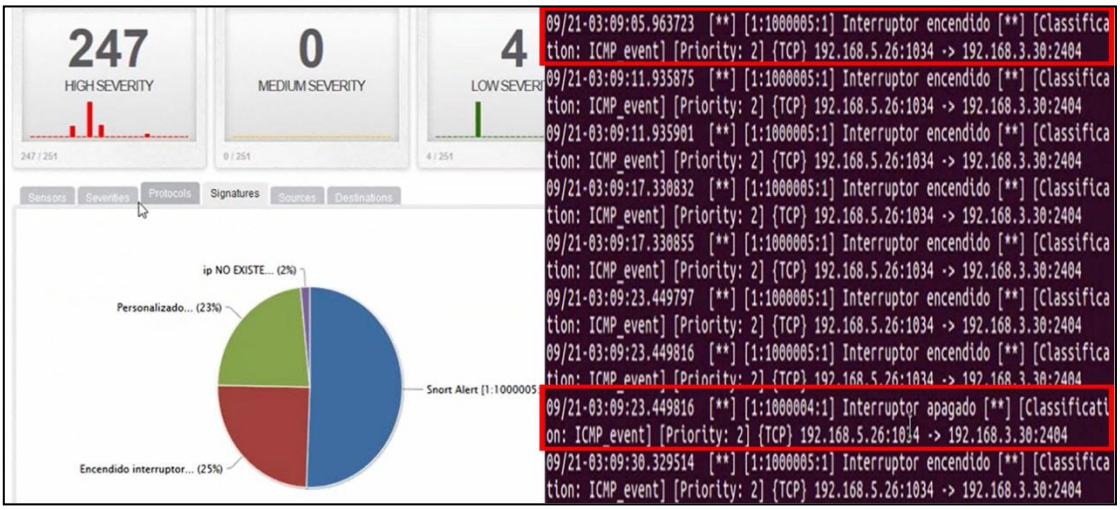


Illustration 28: Example of implementing Snort rules for anomaly detection with IEC104 protocol packet sending. Using Snorby tools to display alerts

4.5 Modelling a cyberattack, GREYENERGY

As a final example to show the capabilities of CAT methodology in industrial environments, one of the latest attacks detected in the energy sector, particularly in the electricity sector, has been modelled. Such attack was GreyEnergy.

In order to see the differences between the two modellings, the attack has been analyzed with both MITRE matrix (43) and CAT attack taxonomy.

4.5.1 MITRE Matrix

ID	Tactic	Technique	Usage (incident information)
T1193 **CAPEC ID:** CAPEC-163	**Initial access**	Spear phishing with attached documents.	Emails with attachments. Attached documents contained macros that executed malicious code when activating. Initial infection with these macros was from GreyEnergy mini, also known as FELIXROOT). More information about FELIXROOT. **SCENARIO 1**
T1051 **CAPEC ID:** CAPEC-563	**Initial access**	Web servers compromised	GreyEnergy's group of attackers used web services of the victim organization. Such services were

			hosted on servers communicating directly with the internal victim network. **SCENARIO 2**
T1085	**Persistence**	Creating a Start Menu Entry for Process Execution with malicious DLL as argument	GreyEnergy mini (dropper) allows download of a malicious DLL (%APPDATA%) and create a .LNK file against the malicious DLL itself, creating an entry in the Windows Start Menu. Downloaded DLL looks "legitimate" for Windows.
T1078 **CAPEC ID:** CAPEC-560	**Privilege escalation**	Valid accounts	Using Mimikatz tool, attackers were able to obtain admin credentials and privileges.
T1116	**Defense Evasion**	Code signing	GreyEnergy was digitally signed with an Advantech certificate.
---	**Defense Evasion**	Hosted in memory	GreyEnergy was implemented in two ways, only in memory or by using DLL persistence as a service. First mode is used when attackers trust that their malware implementation does not require any persistence (for example, high-traffic servers); second one is used when the malware needs to survive any reboot.
---	**Defense Evasion**	System settings modification	---
---	**Defense Evasion**	Parameter modification	---
---	**Defense Evasion**	Inhibitin security tools/systems	GreyEnergy used among other, anti-reversing and forensics techniques to prevent being detected and analyzed. It also possessed a self-erasing feature in case of exceeding a certain number of failed connection attempts to C&C.
T1003 **CAPEC ID:** CAPEC-567	**Credential Access**	Credential dumping	M*imikatz* module: use Mimikatz software to obtain Windows credentials.
	Discovery	Network listing	---
T1087 **CAPEC ID:** CAPEC-575	**Discovery**	Account discovery	*Password* module: Collects stored passwords of various applications.
T1007 **CAPEC ID:** CAPEC-574	**Discovery**	System service discovery	*Info* module: Collects information about the infected system, log events, SHA-256, etc.
---	**Lateral Movement**	Valid accounts	---
---	**Lateral Movement**	Remote Access services	---
---	**Execution**	Scripting	GreyEnergy received commands from the C&C server. Commands such as: Command ID = 3: executed a Shell command. Command ID = 5: downloaded and run a .BAT file from a temporary directory.
---	**Execution**	Module loading	Attackers did not load all modules at once on the compromised device. By using C&C server, they downloaded and ran only the required modules for each task.
T1072	**Execution**	Third-party software	GreyEnergy used legitimate third-party software on Linux servers:

			• 3proxy tiny proxy server • Dante SOCKS server • PuTTY Link (Plink)
T1085	**Execution**	Rundll32	Related to the persistence part and how to host the malware on the affected system.
T1005	**Collection**	Data from local system	Command ID = 1, collected information about the infected device. Information was collected using WMI Query Language (WQL).
T1113	**Collection**	Screen capture	*Sshot* module
T1125	**Collection**	Video capture	*Sshot* module
---	**Collection**	Keylogger	Keylogger module – recording keystrokes.
T1022	**Exfiltration**	Data encrypted	Channels
T1041	**Exfiltration**	Exfiltration over command and control channel	Use of both internal and external proxies for communication with C&C. (TRIUNGULIN)
T1090	**Command and Control**	Connection Proxy	It is very likely that each C&C server had an .onion address in Tor and attackers used it to access, control or transfer data. Note: *OPSEC requirement, which adds an additional layer of anonymity for attackers.*
T1001	**Command and Control**	Data Obfuscation	Most of GreyEnergy's simples used a slightly different encryption algorithm. Specifically, the first four bytes of the encrypted block are used as the decryption key for running T1001 XOR operations.
T1102	**Command and Control**	Web service	Communication with C&C was over HTTPS, but HTTP was also used in some cases. HTTP requests were encapsulated in the same MIME format. However, it should be noted that data was encrypted using AES-256 and RSA-2048.

In its research, ESET did not observe any modules specifically designed for Industrial Control Systems (ICS). However, they have noticed that GreyEnergy attackers have been strategically targeting workstations related to ICS environments running SCADA software. Such stations or servers tend to be critical systems never to be disconnected, except in maintenance cases.

Analysis of FELIXROOT backdoor (mini GreyEnergy) (44):

Domain	ID	Name	Use
Enterprise	T1059	Command-Line Interface	FELIXROOT opens a remote shell to execute commands on the infected system.[1][2]
Enterprise	T1043	Commonly Used Port	FELIXROOT uses Port Numbers 443, 8443, and 8080 for C2 communications.[1][2]
Enterprise	T1022	Data Encrypted	FELIXROOT encrypts collected data with AES and Base64 and then sends it to the C2 server.[1]
Enterprise	T1107	File Deletion	FELIXROOT deletes the .LNK file from the startup directory as well as the dropper components.[1]
Enterprise	T1112	Modify Registry	FELIXROOT deletes the Registry key `HKCU\Software\Classes\Applications\rundll32.exe\shell\open`.[1]
Enterprise	T1027	Obfuscated Files or Information	FELIXROOT encrypts strings in the backdoor using a custom XOR algorithm.[1][2]
Enterprise	T1057	Process Discovery	FELIXROOT collects a list of running processes.[2]
Enterprise	T1012	Query Registry	FELIXROOT queries the Registry for specific keys for potential privilege escalation and proxy information. FELIXROOT has also used WMI to query the Windows Registry.[1][2]
Enterprise	T1060	Registry Run Keys / Startup Folder	FELIXROOT adds a shortcut file to the startup folder for persistence.[2]
Enterprise	T1105	Remote File Copy	FELIXROOT downloads and uploads files to and from the victim's machine.[1][2]
Enterprise	T1085	Rundll32	FELIXROOT uses Rundll32 for executing the dropper program.[1][2]
Enterprise	T1064	Scripting	FELIXROOT executes batch scripts on the victim's machine.[1]
Enterprise	T1063	Security Software Discovery	FELIXROOT checks for installed security software like antivirus and firewall.[2]
Enterprise	T1023	Shortcut Modification	FELIXROOT creates a .LNK file for persistence.[2]
Enterprise	T1071	Standard Application Layer Protocol	FELIXROOT uses HTTP and HTTPS to communicate with the C2 server.[1][2]
Enterprise	T1082	System Information Discovery	FELIXROOT collects the victim's computer name, processor architecture, OS version, volume serial number, and system type.[1][2]
Enterprise	T1016	System Network Configuration Discovery	FELIXROOT collects information about the network including the IP address and DHCP server.[2]
Enterprise	T1033	System Owner/User Discovery	FELIXROOT collects the username from the victim's machine.[1][2]
Enterprise	T1124	System Time Discovery	FELIXROOT gathers the time zone information from the victim's machine.[2]
Enterprise	T1047	Windows Management Instrumentation	FELIXROOT uses WMI to query the Windows Registry.[2]

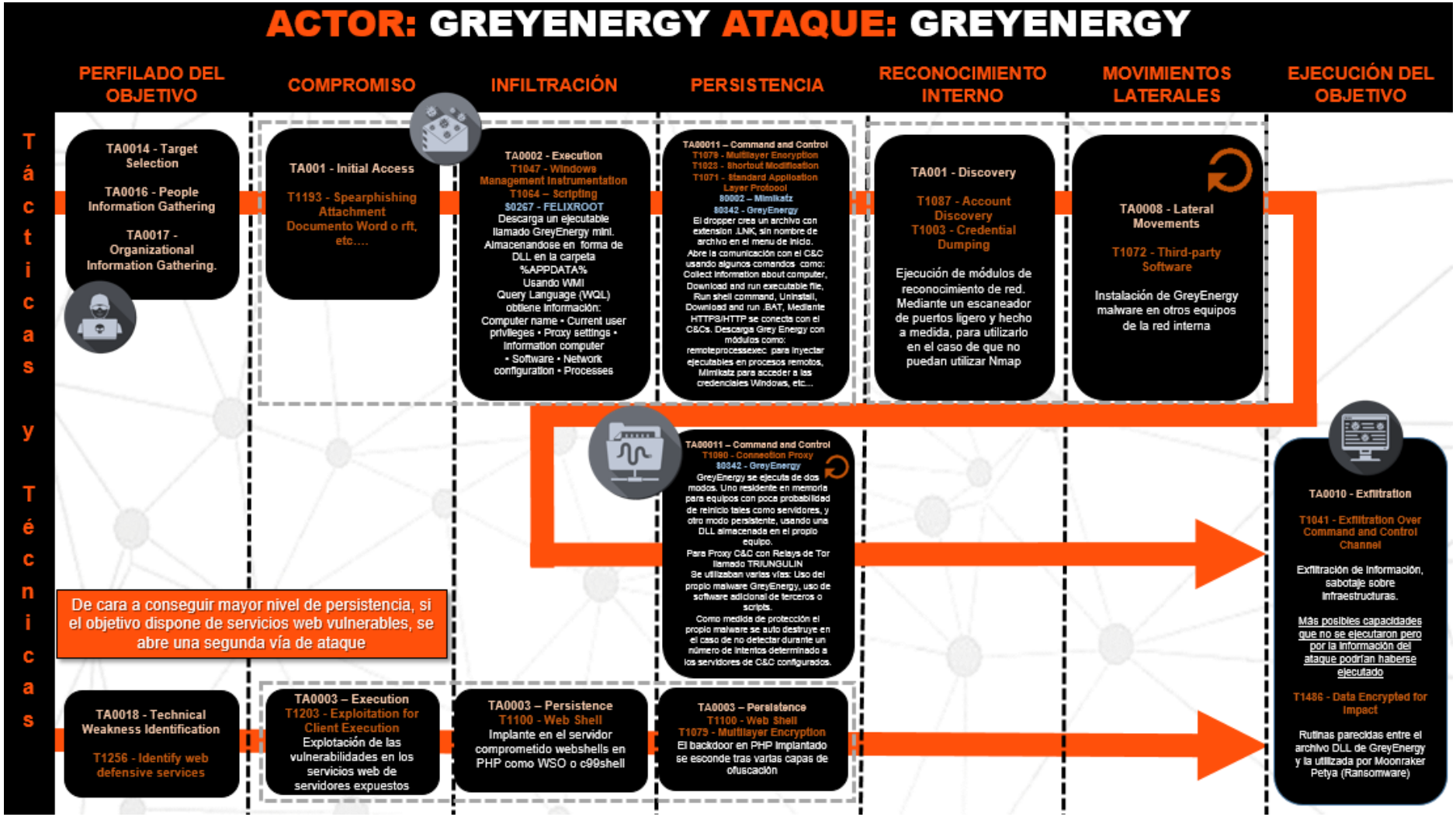
Illustration 29: Techniques used by FELIXROOT backdoor (Mini GreyEnergy), source: MITRE

Analysis of GreyEnergy backdoor (45) by MITRE:

Domain	ID	Name	Use
Enterprise	T1116	Code Signing	GreyEnergy digitally signs the malware with a code-signing certificate.[1]
Enterprise	T1059	Command-Line Interface	GreyEnergy uses cmd.exe to execute itself in-memory.[1]
Enterprise	T1003	Credential Dumping	GreyEnergy has a module for Mimikatz to collect Windows credentials from the victim's machine.[1]
Enterprise	T1107	File Deletion	GreyEnergy can securely delete a file by hooking into the DeleteFileA and DeleteFileW functions in the Windows API.[1]
Enterprise	T1056	Input Capture	GreyEnergy has a module to harvest pressed keystrokes.[1]
Enterprise	T1031	Modify Existing Service	GreyEnergy chooses a service, drops a DLL file, and writes it to that serviceDLL Registry key.[1]
Enterprise	T1112	Modify Registry	GreyEnergy modifies conditions in the Registry and adds keys.[1]
Enterprise	T1188	Multi-hop Proxy	GreyEnergy has used Tor relays for Command and Control servers.[1]
Enterprise	T1027	Obfuscated Files or Information	GreyEnergy encrypts its configuration files with AES-256 and also encrypts its strings.[1]
Enterprise	T1055	Process Injection	GreyEnergy has a module to inject a PE binary into a remote process.[1]
Enterprise	T1105	Remote File Copy	GreyEnergy can download additional modules and payloads.[1]
Enterprise	T1085	Rundll32	GreyEnergy uses PsExec locally in order to execute rundll32.exe at the highest privileges (NTAUTHORITY\SYSTEM).[1]
Enterprise	T1045	Software Packing	GreyEnergy is packed for obfuscation.[1]
Enterprise	T1071	Standard Application Layer Protocol	GreyEnergy uses HTTP and HTTPS for C2 communications.[1]
Enterprise	T1032	Standard Cryptographic Protocol	GreyEnergy encrypts communications using AES256 and RSA-2048.[1]
Enterprise	T1007	System Service Discovery	GreyEnergy enumerates all Windows services.[1]

Illustration 30: Techniques used by GreyEnergy backdoor written in C and compiled in Visual Studio, source: MITRE

4.5.2 CAT Taxonomy



5 Conclusions

A series of lessons learned, critiques and future lines of work related to the developed project are shown below:

5.1 Lessons learned

- The complexity of modelling an attack extensively both technically and at high level so that many people can understand what is really happening.

- Large amounts of information on the Internet but that does not have an order when applying certain technical concepts.

5.2 Critical reflection

- All objectives have been achieved and tactics and techniques raised in this Project are under review by the CAT community for its appearance on the github website.

    - https://github.com/fdeandres/CAT----Intelligence-Led-Cyber-Attack-Taxonomy

- Regarding to planning, it has been correct. Points set out in the Project have been able to be developed and investigated in time.

- Different initial planning changes have been made to the points to be dealt with, to avoid extending the project much further. Bearing that fact in mind, an easy-to-read document with interesting content is intended to be delivered.

5.3 Future lines of work

- **Execution of the evidence posed**. Work is already underway to apply the theorical concepts of this Project.

- **Development of specific tools** that allow to perform certain attacks in industrial environments, specifically in electrical substations.

- **Modelling more industrial cybersecurity incidents** that will arise over time.

- **Incorporation of more tactics, techniques and tools in the *caffeine* framework** that allow to perform better attack modelling and propose new attack scenarios for red teams.

6 Glossary

6.1 Acronyms

DoS: Denial of Service
DDoS: Distributed Denial of Service
HMI: Human Machine Interface
IED: Intelligent Electronic Device
IDS: Intrusion Detection System
INCIBE: Spanish National Cybersecurity Institute
IT: Information Technology
LAN: Local Area Network
NIST: National Institute of Standards and Technology (United States).
OSI: Open System Interconnection
OT: Operation Technology
PLC: Programmable Logic Controller
RTU: Remote Terminal Unit
SCADA: Supervisory Control and Data Acquisition
TTPs: Tactics, techniques and procedures
CSU: Central Substation Unit

6.2 Terms

- **0-day:** 0-day vulnerabilities refer to vulnerabilities that only the attacker has knowledge of. For their part, companies where the attacker has detected such vulnerability are not aware of it, neither other potential attackers. There is no solution to this problem because it will not be known until the vulnerability is exploited and evidences have been found.

- **Blue team:** Cybersecurity incident response team. Defensive team.

- **Red team**: Team made up of ethical hacking professionals whose goal is to simulate real attacks in environments, usually production ones. Offensive team.

7 Bibliography

1. **Nicolas Falliere, Liam O Murchu y Eric Chien.** *Symantec.* [En línea] Febrero de 2019. https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

2. **Pinto, Alessandro Di.** Nozomi Networks. [En línea] Febrero de 2019. [Citado el:] https://www.nozominetworks.com/downloads/US/Nozomi-Networks-GreyEnergy-Dissecting-the-Malware.pdf.

3. ***TIBER-EU FRAMEWORK.*** [En línea] Febrero de 2019. https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf.

4. Pols, Mr. drs. Paul. *Cyber Security Academy (CSA).* [En línea] Febrero de 2019. https://www.csacademy.nl/images/scripties/2018/Paul-Pols---The-Unified-Kill-Chain.pdf.

5. *TIBER-NL GUIDE.* [En línea] Febrero de 2019. https://www.dnb.nl/binaries/TIBER-NL%20Guide%20Second%20Test%20Round%20final_tcm46-365448.pdf.

6. Bank of England. *CBEST Implementation Guide.* [En línea] Febrero de 2019. https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/cbest-implementation-guide.

7. Insider, Tech. *Youtube.* [En línea] Febrero de 2019. https://www.youtube.com/watch?v=pL9q2lOZ1Fw&feature=youtu.be.

8. Wikipedia. [En línea] Febrero de 2019. https://es.wikipedia.org/wiki/Efecto_Joule.

9. *BOE - Boletín Oficial del Estado.* [En línea] Febrero de 2019. https://www.boe.es/buscar/doc.php?id=BOE-A-2007-13024.

10. Wikipedia. [En línea] Marzo de 2019. https://es.wikipedia.org/wiki/DNP3 .

11. INCIBE-CERT. [En línea] Marzo de 2019. https://www.incibe-cert.es/blog/estandar-iec-61850-todos-uno-y-uno-todos.

12. Castillo, Javier F. *CCI, Centro de Ciberseguridad Industrial.* [En línea] Marzo de 2019. https://www.cci-es.org/documents/10694/613683/Establecimientos+zonas+y+conductos.pdf/a479e3db-81f4-43c1-b5d1-f9e5f7754bcf .

13. INCIBE-CERT. [En línea] Marzo de 2019. https://www.incibe-cert.es/blog/zonas-y-conductos-protegiendo-nuestra-red-industrial.

14. Aarón Flecha Menéndez. [En línea] Marzo de 2019. https://www.ccn-cert.cni.es/pdf/documentos-publicos/xi-jornadas-stic-ccn-cert/2632-m22-01-descontrol-industrial/file.html.

15. INCIBE-CERT. [En línea] Marzo de 2019. https://www.incibe-cert.es/blog/crashoverride-el-malware-sci-ataca-nuevo.

16. Aarón Flecha Menéndez. [En línea] Marzo de 2019. https://www.cci-es.org/documents/10694/431723/10.+S21Sec+DEFENDIENDO+MI+ENTORNO+INDUSTRIAL.pdf/cb576393-8cc1-4dbe-bd65-5da3f56ec418;jsessionid=5096EFB8A58A12579C2F9D83E40CB8B8?version=1.0.

17. Cherepanov, Anton. [En línea] Marzo de 2019. https://www.welivesecurity.com/wp-content/uploads/2018/10/ESET_GreyEnergy.pdf **.**

18. Lockheed Martin. [En línea] Mayo de 2019. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

19. Panda Security. [En línea] Marzo de 2019. https://www.pandasecurity.com/spain/mediacenter/src/uploads/2017/11/Adaptive_Defense-Understanding_CyberAttacks-es.pdf.

20. MITRE. [En línea] Marzo de 2019. https://www.mitre.org/ **.**

21. MITRE. [En línea] Marzo de 2019. https://attack.mitre.org/ .

22. MITRE. [En línea] Marzo de 2019. https://attack.mitre.org/matrices/pre/.

23. MITRE. [En línea] Marzo de 2019. https://attack.mitre.org/matrices/mobile/ .

24. Robert M. Lee y Michael J. Assante. *SANS.* [En línea] Abril de 2019. https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297.

25. Alexander, Otis. [En línea] Mayo de 2019. https://www.acsac.org/2017/workshops/icss/Otis-Alexander-ICS,%20Adversarial%20Tactics,%20Techniques.pdf.

26. Mildrey Carbonell Castro, Francisco Luis de Andres Perez y Francisco Jimenez del Castillo. *github.* [En línea] Mayo de 2019. https://github.com/fdeandres/CAT----Intelligence-Led-Cyber-Attack-Taxonomy.
27. Creative Commons. [En línea] Mayo de 2019. https://creativecommons.org/licenses/by/4.0/.
28. S21sec. [En línea] Mayo de 2019. https://www.s21sec.com/en/s21sec-revoluciona-la-simulacion-de-ciberataques/.
29. Wikipedia. [En línea] Mayo de 2019. https://es.wikipedia.org/wiki/An%C3%A1lisis_PESTEL.
30. Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence, Bromander, Vasileios y Mavroeidis, Siri**.** [En línea] Mayo de 2019. https://www.researchgate.net/publication/319701970.
31. Pwnwiki. [En línea] Mayo de 2019. http://pwnwiki.io/#!index.md .
32. Robert M. Lee, Michael J. Assante y Tim Conway. *SANS.* [En línea] Mayo de 2019. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.
33. INCIBE-CERT. [En línea] Mayo de 2019. https://www.incibe-cert.es/blog/insider-las-dos-caras-del-empleado.
34. sommerville-videos. [En línea] Mayo de 2019. https://es.slideshare.net/sommerville-videos/maroochy-water-breach.
35. Snort. *Snort.* [En línea] Mayo de 2019. https://www.snort.org .
36. Yara. *Yara.* [En línea] Mayo de 2019. https://yararules.com/ .
37. PLCScan tool, [En línea] Mayo de 2019. https://code.google.com/archive/p/plcscan/ .
38. l.lefebvre. [En línea] Mayo de 2019. https://github.com/sourceperl/mbtget .
39. John, Michael. [En línea] Mayo de 2019. https://github.com/rapid7/metasploit-framework/blob/master/documentation/modules/auxiliary/client/iec104/iec104.md .
40. Martorella, Christian. [En línea] Mayo de 2019. https://tools.kali.org/information-gathering/theharvester.
41. Matherly, John. *shodan.* [En línea] Mayo de 2019. https://www.shodan.io/ .
42. scadastrangelove. [En línea] Mayo de 2019. https://github.com/scadastrangelove/SCADAPASS .
43. Aarón Flecha Menéndez, Elyoenai Egozcue, Francisco Luis de Andrés, Enrique Dominguez, Miryam Sánchez, Anibal Santiago, Enrique Martín, Silvia Villanueva, Ignacio Paredes, Samuel Linares, José Valiente y Susana Asensio. [En línea] Mayo de 2019. https://www.cci-es.org/buscador/-/journal_content/56/10694/753289?p_p_auth=Y80pD8Tf.
44. *MITRE.* [En línea] Mayo de 2019. https://attack.mitre.org/software/S0267/ .
45. *MITRE.* [En línea] Mayo de 2019. https://attack.mitre.org/software/S0342/ .
46. INCIBE-CERT. [En línea] Mayo de 2019. https://www.incibe-cert.es/blog/insider-las-dos-caras-del-empleado**.**
47. Mildrey Carbonell Castro, De verano a primavera en los servicios de Red Team, https://player.vimeo.com/video/333300937
48. Aarón J. Pozo Sánchez y Francisco Luis de Andrés Pérez, Modelado de escenarios de ataque con metodología CAT, Hack & Beers Alicante -Vol. 5 (26 abril de 2019), https://hackandbeers.es/sessions/modelado-de-escenarios-de-ataque-con-metodologia-cat/

Extra Documentation consulted

Web sites

- https://azeria-labs.com/tactics-techniques-and-procedures-ttps/, February 2019.
- https://dragos.com/wp-content/uploads/CrashOverride-01.pdf, February 2019.
- https://github.com/rabobank-cdc/Blue-ATTACK/wiki, March 2019.
- https://github.com/NextronSystems/APTSimulator, March 2019.
- https://gitlab.com/d0ubl3g/industrial-security-auditing-framework, March 2019.
- https://github.com/snabbco/snabb, March 2019.
- https://github.com/ITI/ICS-Security-Tools, March 2019.
- https://github.com/atimorin/scada-tools, March 2019.
- https://github.com/nshalabi/ATTACK-Tools, March 2019.
- https://github.com/hisanmehmood/Awesome-Red-Teaming, April 2019.
- https://www.endgame.com/blog/technical-blog/introducing-endgame-red-team-automation, April 2019.
- https://securelist.com/greyenergys-overlap-with-zebrocy/89506/, April 2019.
- https://www.novainfosec.com/2016/02/12/the-dml-model/, April 2019.
- https://www.larazon.es/espana/el-estado-islamico-intento-hackear-una-depuradora-y-envenenar-el-agua-de-miles-de-personas-en-inglaterra-CH20148208, March 2019.
- https://github.com/ITI/ICS-Security-Tools, May 2019.

- https://www.sans.org/webcasts/ Attendance to different webcasts over the months during the project was executed:

  - Ken Warren, **Falcon and the MITRE ATT&CK Framework – Better Together**, 17th January 2019

  - Justin Henderson y John Hubbard, **MITRE ATT&CK and Sigma Alerting**, 13th February 2019.

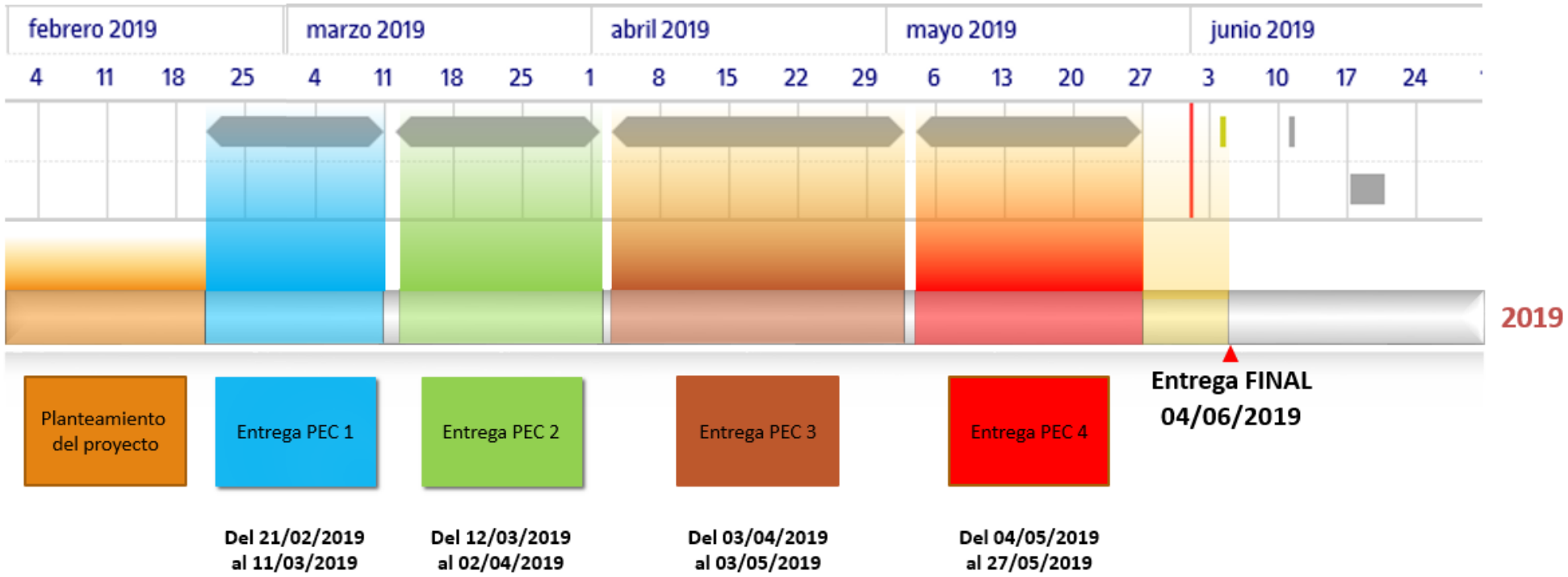
Books

- Clint Bodungen, Bryan Singer, Aaron Shbeeb, Kyle Wilhoit and Stephen Hilt - **Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions**. *McGraw-Hill Education (16th September 2016)*

- Pascal Ackerman - **Industrial Cybersecurity: Efficiently secure critical infrastructure systems**. *Packt Publishing (18th October 2017)*

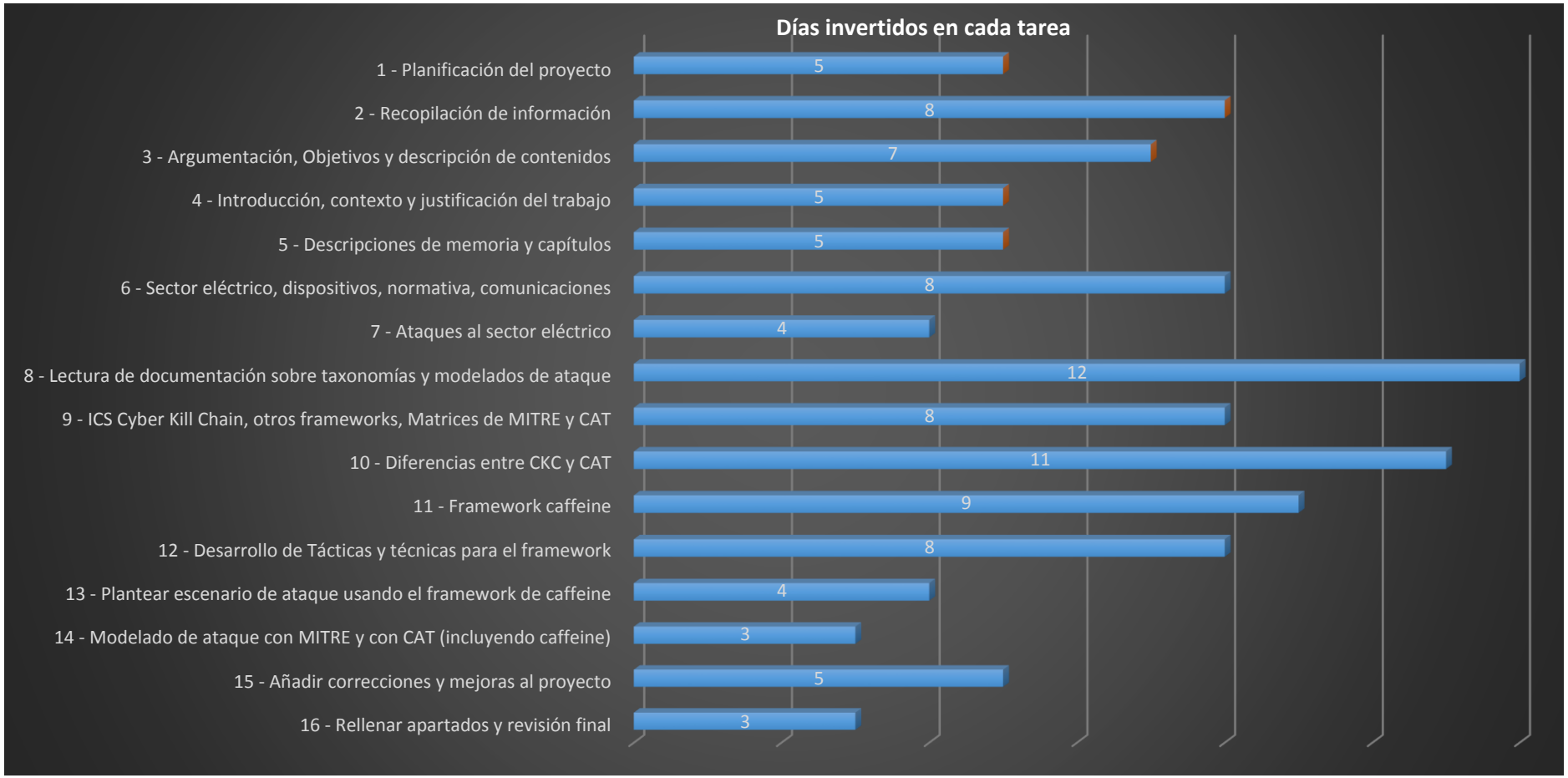
- Eric D. Knapp (Author), Joel Thomas Langill (Collaborator) - **Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems**. *Syngress; Edition: 2 (15th December 2014)*

8 Annex I – Planning Diagrams



Extra information

PEC	Task	Starting date	Ending date	Milestone or activity	Started	Task duration
1	1 – Project planning	21/02/2019	25/02/2019	Beginning	21/02/2019	5
1	2 – Gathering information	26/02/2019	04/03/2019	Activity 2	26/02/2019	8
1	3 – Argumentation, Objectives and content description	05/03/2019	11/03/2019	Activity 3	05/03/2019	7
2	4 - Introduction, context and work justification	12/03/2019	16/03/2019	Activity 4	12/03/2019	5
2	5 – Memory and chapters description	17/03/2019	21/03/2019	Activity 5	17/03/2019	5
2	6 – Electricity sector, devices, regulations, communications	22/03/2019	29/03/2019	Activity 6	22/03/2019	8
2	7 – Attacks on the electricity sector	30/03/2019	02/04/2019	Activity 7	30/03/2019	4
3	8 – Reading documentation on taxonomies and attack modelling	03/04/2019	14/04/2019	Activity 8	03/04/2019	12
3	9 - ICS Cyber Kill Chain, other frameworks, MITRE matrixes and CAT	15/04/2019	22/04/2019	Activity 9	15/04/2019	8
3	10 – Differences between CKC and CAT	23/04/2019	03/05/2019	Activity 10	23/04/2019	11
4	11 - *Caffeine* framework	04/05/2019	12/05/2019	Activity 11	04/05/2019	9
4	12 – Development of tactics and techniques for the framework	13/05/2019	20/05/2019	Activity 12	13/05/2019	8
4	13 – Creating attack scenario using *caffeine* framework	21/05/2019	24/05/2019	Activity 13	21/05/2019	4
4	14 – Attack modelling with MITRE and CAT (including *caffeine*)	25/05/2019	27/05/2019	Activity 14	25/05/2019	3
FINAL	15 – Adding corrections and improvements to the project	28/05/2019	01/06/2019	Activity 15	28/05/2019	5
FINAL	16 – Filling in sections and final review	02/06/2019	04/06/2019	Activity 16	02/06/2019	3


Días invertidos en cada tarea
1 - Planificación del proyecto
5
2 - Recopilación de información
8
3 - Argumentación, Objetivos y descripción de contenidos
7
4 - Introducción, contexto y justificación del trabajo
5
5 - Descripciones de memoria y capítulos
5
6 - Sector eléctrico, dispositivos, normativa, comunicaciones
8
7 - Ataques al sector eléctrico
4
8 - Lectura de documentación sobre taxonomías y modelados de ataque
12
9 - ICS Cyber Kill Chain, otros frameworks, Matrices de MITRE y CAT
8
10 - Diferencias entre CKC y CAT
11
11 - Framework caffeine
9
12 - Desarrollo de Tácticas y técnicas para el framework
8
13 - Plantear escenario de ataque usando el framework de caffeine
4
14 - Modelado de ataque con MITRE y con CAT (incluyendo caffeine)
3
15 - Añadir correcciones y mejoras al proyecto
5
16 - Rellenar apartados y revisión final
3

9 Annex II – Cyberattack on Venezuela, technical review

Venezuela is a tropical country located in northern South America that owns around 18% of world's oil according to outdated data. Although this percentage is currently lower, as there has been a decrease in its oil production due to political influence and international situation. Given its amount of oil and resources it has to export, Venezuela could become a strategic objective for other nations wanting to manipulate its resources or guide its development in a specific direction to profit themselves.

On the afternoon of May 7, 2019, Venezuela suffered a large scale blackout that paralyzed the country. Critical infrastructures were directly affected and it evolved into a general unrest on part of the population that was suffering continuous blackouts being unable to preserve food, light at night, etc. In addition, different problems must be added that led to continous tumults in the streets throughout Venezuela and a destabilized government.

After days of continuous problems, Venezuelan President Nicolas Maduro announced in various public media that these blackouts had been caused by a cyberattack. In his speech, the president pointed out a possible culprit, the United States being such culprit attacking the entire electricity system of Venezuela. Besides, Nicolas Maduro added information about the attack perpetrated by US divided into 3 phases or attacks:

- The first attack would be against the computer central system owned by the Corporación Eléctrica Nacional (Corpoelec) company in the Simón Bolivar Hydroelectric Power Plant (the third largest in the world) located in El Guri dam. This cyberattack would also affect the capital, Caracas. It is important to note that Simon Bolivar hydroelectric power plant provides electricity to 80% of Venezuela and would therefore be classified as critical infrastructure.

- Following this alleged first attack, the president commented on a possible electromagnetic attack with "*mobile devices that interrupt and reverse recovery processes*". It seems that the president wanted to refer to advanced inhibitors that prevented communication transmission correctly.

- Finally, in a last attack burning and explosion of electrical substations via sabotage would be carried out.

As extra information, Maduro revealed that the attack was performed from two American cities, Houston and Chicago and confirmed that they have evidences on how such cyberattack on the electricity grid was performed.

But, could it be determined if these blackouts have actually been caused by a cyberattack?. There is some technical research focused on this line on the Internet amd virtually all of them come to the same conclusion, it cannot be determined if there has been a cyberattack. What can be said about that period

of blackouts is that search engines like Shodan, Zoomeye, Phoofa, etc. received quite an influx of searches, all of them focused on Venezuela and its infrastructure.

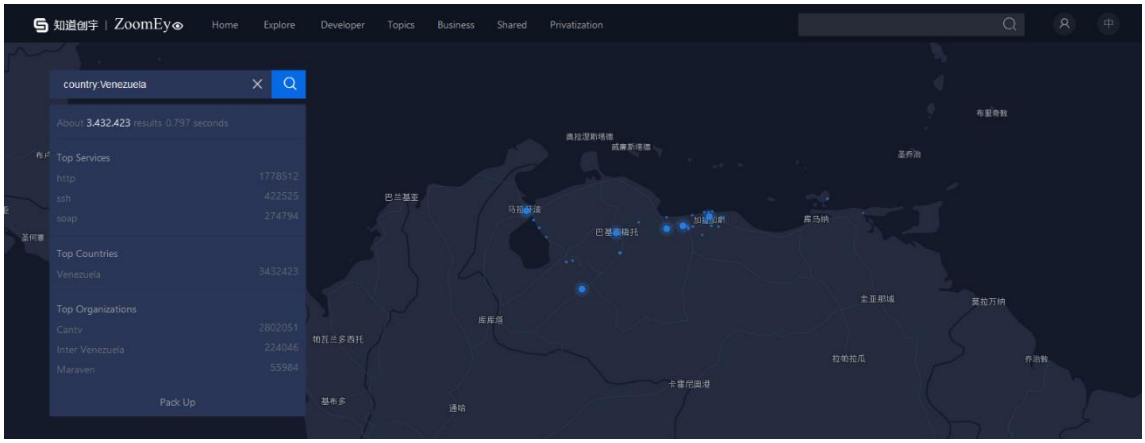


Illustration 31: Searching for Internet connected devices located in Venezuela from ZoomEye

After these attacks, different searches have been carried out to locate devices connected to the Internet using protocols associated with the electricity sector. Considering that most extended protocol in America is DNP3, a search for devices with this active port has been performed with this result:

Illustration 32: Using Shodan to detect possible DNP3 devices in Venezuela

53 devices with TCP port 20000 open. Such port is used by DNP3 protocol by default but it appears that some of these ports do not have a true DNP3 service behind but another service used by other communications.

A more advanced search with ZoomEye has allowed to reduce possible false positives and detect 48 hosts that are initially industrial devices and use DNP3 protocol.

Query submitted:

```
port:"20000"+country:"VE"+service:"dnp"
```

On the other hand, a search for Modbus/TCP protocol using TCP port 502 by default was also made.

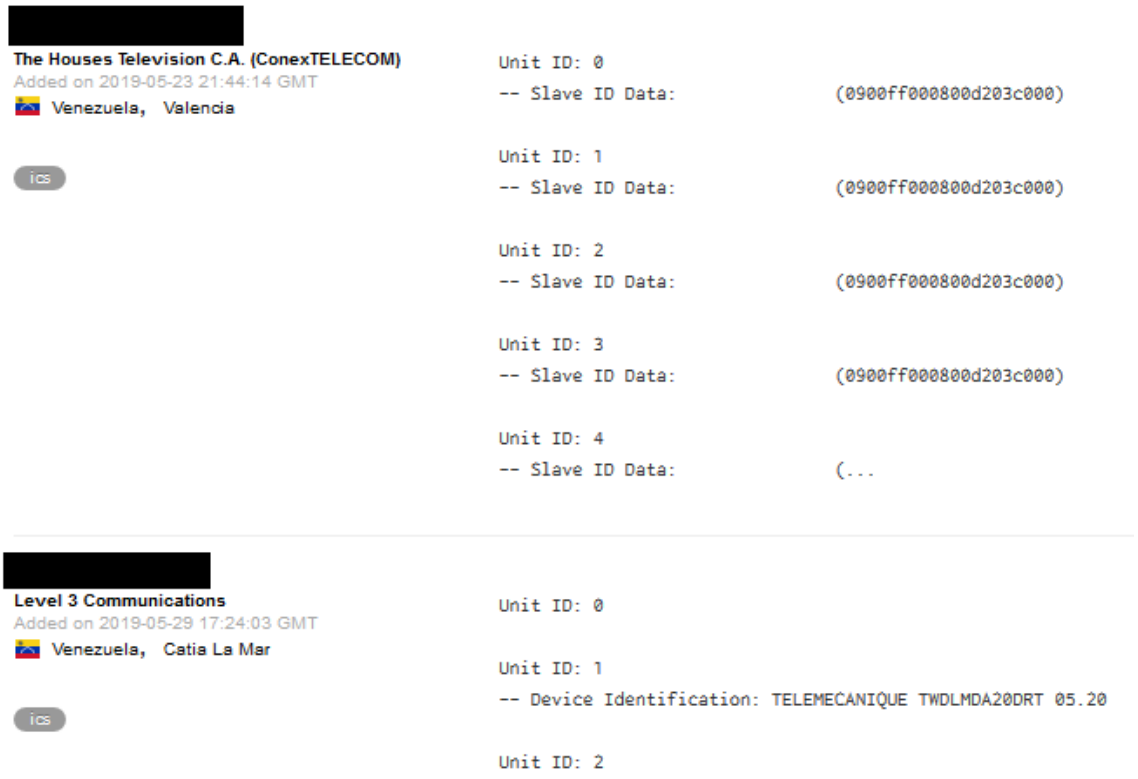


Illustration 33: Searching for Internet connected devices using Modbus/TCP (502/TCP) Protocol with Shodan

In this case, they seem to be real devices given responses can be received by port 502.

In addition to all these searches with protocols related to the electricity sector and industrial control systems in general in the case of Modbus/TCP. Information has been looked for from major manufacturers or companies that collaborated on the hydroelectric plant that allegedly suffered the attack. Such companies are Edelca, Andritz, Alstom and ABB. Some of these companies such as ABB are infustrial manufacturers that provide equipment to infrastructures and have public information about their devices online.

Estructura general del sistema DCS

Interfaz hombre-máquina (HMI)
El sistema ABB de portales de generación de procesos (Process Generation Portal) se utilizará en las estaciones de operador. El sistema de consolas se basa en estándares industriales y en el sistema operativo Windows XP. Tiene una arquitectura abierta que permite utilizar numerosos protocolos de comunicaciones con capacidad para interconectar con programas y bases de datos de terceros.

TEI controlador AC800M

Protocolos y medios de soporte
El controlador utiliza los protocolos de comunicación y medios de soporte siguientes:

línea B, y si ambas líneas A y B se averían, entonces la estructura de anillo cambiará a una estructura de bus.

Comunicación a través de la red E/S
La red E/S conecta todos los dispositivos E/S de la planta con el controlador. Hay 3 tipos de protocolos de comunicación utilizados para la red E/S:

- ModuleBus, para comunicar directamente con los clusters E/S locales por cables de fibra óptica de plástico. ModuleBus soporta la funcionali-

Illustration 34: Example of a device deployed by ABB at Simón Bolivar hydroelectric plant

On the Internet, public videos that show how to manage or program their devices can be found.

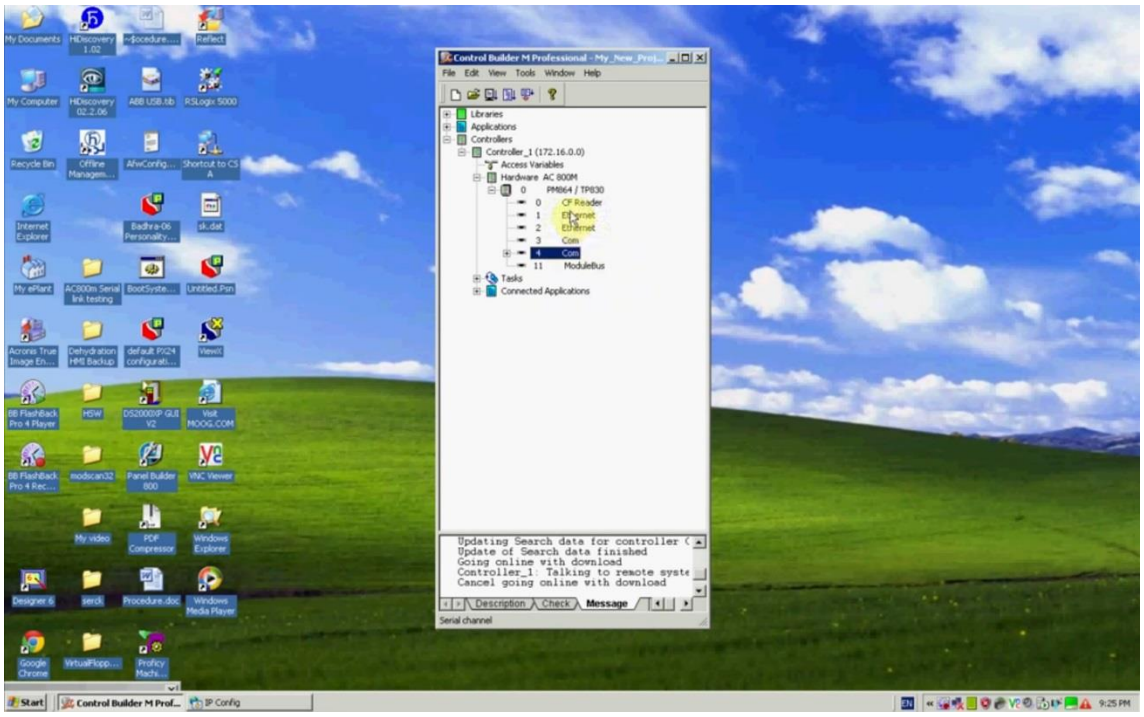


Illustration 35: Video capture showing how to program an ABB DCS AC 800M device, source: YouTube

While it is true that a person with Internet connection can collect such a large amount of information about such an important infrastructure for Venezuela, it can be argued that a cyberattack on the electricity sector could be carried out perfectly with a multidisciplinary team. It is also true that behind these attacks must be a state or a very well organized company with many resources to be able to make a satisfactory attack.

There is no doubt that the alleged cyberattack could have been executed, but until new evidence came to light, it is not possible to confirm that the facts happened in such a way.

On the other hand, it can be confirmed that an attack of these magnitudes on a critical infrastructure of the electricity sector could cause severe problems to a country and even collapsing it as happened in Venezuela. In this way, the choice of electricity sector and specifically the distribution part in this project becomes much more meaningful after seeing these events although they have been not comfirmed at cyber level, problems detected have been more than remarkable.

Reference Information used

- https://docplayer.es/10209350-Central-hidroelectrica-simon-bolivar-guri-marzo-2012.html, June 2019.
- https://es.wikipedia.org/wiki/Central_Hidroel%C3%A9ctrica_Sim%C3%B3n_Bol%C3%ADvar, June 2019.
- http://interelectricas.co/pdf/ABB/03-2006/32-36%203M647_SPA72dpi.pdf, June 2019.
- http://www.abb.com/cawp/seitp202/e3d432695eb75e8ac12572f800445309.aspx, June 2019.
- https://new.abb.com/news/detail/13622/abb-wins-us-28-million-contract-to-boost-venezuelan-electrical-transmission-system, June 2019.
- https://new.abb.com/news/detail/13649/abb-wins-us-41-million-in-orders-for-venezuelan-substation-and-transmission-lines, June 2019.
- https://www.telesurtv.net/news/venezuela-investiga-ciberataque-sistema-electrico-20190312-0032.html, June 2019.
- https://www.securityweek.com/venezuelas-maduro-says-cyber-attack-prevented-power-restoration, June 2019.
- https://www.ivcco.com/application/App%20Note%20-%20ABB%20Guri%20Dam.pdf, June 2019.
- https://www.reuters.com/article/us-venezuela-politics-russians/russian-deployment-in-venezuela-includes-cybersecurity-personnel-us-official-idUSKCN1R72FX, June 2019.
- https://paper.seebug.org/869/, June 2019.
- https://www.360enconcreto.com/blog/detalle/concreto-en-generacion-de-energia-central-hidroelectrica-simon-bolivar, June 2019.
- https://www.youtube.com/watch?v=pB4uIISa0zw, June 2019.
- https://fofa.so/, June 2019.
- https://www.zoomeye.org/, June 2019.
- https://www.shodan.io/, June 2019.