CYPRESS

CYPRESS : Report D1.2 – Describing the relevant cyber-components, threats, and barriers

Task 1.2 – Project Report

Sami Ben Mariem, Vincent Rossetto, Volkan Guler, Adrien Godfraind, Laurent Mathy

Date: 2022-02-14

Contents

Executive Summary

This document is the second deliverable of the "Cyber-Physical Risk of the bulk Electric Energy Supply System" (CYPRESS) project. The work presented in this document has been performed in the frame of the second task (T1.2) of the first work package WP1, titled "*Criteria and benchmarks for cyber-physical risk management*". The objective of CYPRESS WP1 is to generalize and adapt the concepts currently used in the reliability management of electric power and energy systems so that they can correctly cover the cyber-threats from various system-wide control and communication layers.

Within this framework, Task 1.2 (T1.2) seeks at presenting the first steps of the cyber-physical risk assessment task, which will focus on modeling the cyber-part of the power grid following an adapted version of the NIST[1] specifications. Indeed, this task is of particular importance when considering further work packages such as WP3 that should revisit the barriers that should be used to mitigate the risk of the threats mentioned in this document.

First, T1.2 seeks to select relevant cyber-components that enable the operation of the power grid or that can directly/indirectly be used to harm its physical infrastructures. Then, T1.2 aims at providing a methodology for identifying and selecting the relevant threats and vulnerabilities in the cyber-space that could potentially lead to the disruption of the correct behavior of the power grid and its output. Finally, T1.2 provides preliminary proposals on a list of threats resulting from applying the aforementioned methodology as well as some countermeasures that could be used to prevent cyber-attacks resulting from the modeled threats.

The electrical grid is being operated directly/indirectly through a complex and constantly evolving cyber environment. In this context, the increasing number of devices and the speed at which new devices are introduced in the cyber-space leads to a very difficult process in identifying the components that interact in the cyber-part of the cyber-physical power grid. Chapter 2 provides a non-exhaustive list of traditional software and hardware components that constitutes the backbone of the cyber-part. In addition, it describes the various subsystems that these components are part of, the tasks that they perform, and part of their action space, i.e. the sensing and actuating actions that they can perform on the physical part of the system. Furthermore, the Cyber-Space as Services (CSaS) abstraction is defined to address the variability, heterogeneity, and scale of the power grid's cyber-space. This model attempts to abstract the physical cyber-components of the system using the cyber-service (s) they provide to the physical part of the system.

Using this modeling approach, the report subsequently describes a methodology to identify the threats and vulnerabilities that are relevant to cyber-physical power systems and the output of applying the first steps of this methodology to the system (Chapter 3). The methodology presented in this chapter is inspired by an adapted version of the NIST framework. While the original NIST methodology relies on STRIDE, a state-of-the-art strategy for cyber-threats modeling, the approach depicted in this chapter attempts to circumvent the limitations of STRIDE in the context of cyber-physical systems. To do so, threats are modeled as a degradation

[1] Cyber-security framework providing a set of guidelines to mitigates cyber-security risks, published by the US National Institute of Standards and Technology (NIST).

in the quality of some of the CSaS service (s) which is shown to allow the consideration of an exhaustive set of threat scenarios. Finally, Chapter 3 also provide several use cases, defined as threat scenarios, that can be used as a starting point to define the benchmarks of T1.3.

Finally, the report discusses some mitigation strategies that can be integrated into the cyber part of the power grid (Chapter 4). The report presents an overview of the traditional techniques that enables the security, safety, and resilience of the cyber-physical system using state-of-the-art cryptography techniques, and puts them into contrast with more innovative solutions such as Polymorphic systems.

Author Contributions

Table 1 lists all the authors that have contributed to this report. Sami Ben Mariem and Vincent Rossetto are the main authors of this report. They co-wrote most of its content and they also took part in the integration of the other authors' content. Volkan Guler contributed to Chapter 3 by describing the original version of the NIST framework, as well as some first results of applying this methodology. Then, Adrien Godfraind provided valuable inputs regarding the physical part of the system and is the main author of section 2.1.2 and the content related to the tasks and action space of subsystems depicted in Section 2.1.1. Finally, Hakan Ergun and Laurent Mathy contributed to reviewing the entire document.

Author	Affiliation
Sami Ben Mariem	Université de Liège
Vincent Rossetto	Université de Liège
Volkan Guler	Katholieke Universiteit Leuven
Adrien Godfraind	Haulogy
Laurent Mathy	Université de Liège
Hakan Ergun (Work-package Leader)	Katholieke Universiteit Leuven

Table 1: List of authors

List of acronyms

- ACSI: Abstract Communication Service Interface
- AFP: Apple Filing Protocol
- AH: Authentication Header
- AMI: Advanced Metering Infrastructure
- ASIC: Application-specific integrated circuit
- ASSP: Application-Specific Standard Parts
- BIOS: Basic Input/Output System
- CA: Certification Authority
- CAN: Controller Area Network
- CIFS: Common Internet File System
- CPU: Central Processing Unit
- CRC: Cyclic Redundancy Check
- CSaS: Cyber-Space as Services
- DAS: Direct-Attached Storage
- DC: Data Concentrators
- DCS: Decentralized Control System
- DDR: Double Data Rate Synchronous
- DER: Distributed Energy Resource
- DMS: Distribution Management System
- DNP: Distributed Network Protocol
- DoS: Denial of Service
- DPI: Deep Packet Inspection
- DRAM: Dynamic Random Access Memory
- DREAD: Damage, Reproducibility, Exploitability, Affected users, Discoverability
- DSO: Distribution System Operator

- EHV: Extra-High Voltage
- EMS: Energy Management System
- ESP: Encapsulating Security Payload
- EV: Electric Vehicle
- FACTS: Flexible Alternating Current Transmission System
- FPGA: Field-Programmable Gate Array
- F-RAM: Ferroelectric Random Access Memory
- GigE: Gigabit Ethernet
- GOOSE: Generic Object Oriented Substation Events
- GPS: Global Positioning System
- GUI: Graphical User Interface
- HBA: Host-Bus Adapter
- HDD: Hard-Disk Drive
- HDL: Hardware Description Language
- HLS: High-Level Synthesis
- HMI: Human-Machine Interface
- HTTP: Hyper-Text Transfer Protocol
- HVDC: High-Voltage Direct-Current
- IANA: Internet Assigned Numbers Authority
- ICCP: Inter-Control Center Communications Protocol
- ICS: Industrial Control System
- ICT: Information and Communication Technologies
- IDS: Intrusion Detection System
- IEC: International Electrotechnical Commission
- IED: Intelligent Electronic Device
- IEEE: Institute of Electrical and Electronics Engineers
- IKE: Internet Key Exchange
- IoT: Internet of Things
- IP: Internet Protocol
- IPX: Inter-network Packet eXchange
- IT: Information Technology
- LAN: Local Area Network
- MAC: Media Access Control
- MAC: Message Authentication Code
- MDM: Meter Data Management
- MIC: Message Integrity Code
- MMS: Manufacturing Message Specification
- MT: Mega-Transfer
- MV: Medium Voltage

- NAND: Not AND (logic gate)
- NAPT: Network Address and Port Translation
- NAS: Network-Attached Storage
- NAT: Network Address Translation
- NetBEUI: NetBIOS Extended User Interface
- NFS: Network File System
- NIC: Network Interface Controller
- NIDS: Network Intrusion Detection System
- NLTC: No-Load Tap Changer
- NOR: Not OR (logic gate)
- NTP: Network Time Protocol
- OLTC: On-Load Tap Changer
- OS: Operating System
- OSI: Open Systems Interconnection
- PCIe: Peripheral Component Interconnect Express
- PCS: Process Control System
- PID: Proportional Integral Derivative
- PKI: Public Key Infrastructure
- PLC: Programmable Logic Controller
- PMS: Power Management System
- PMU: Phasor Measurement Unit
- PSK: Pre-Shared Key
- PTP: Precision Time Protocol
- QoS: Quality of Service
- RAID: Redundant Array of Inexpensive Disks
- RAM: Random Access Memory
- RDRAM: Rambus Dynamic Random Access Memory
- ROM: Read-Only Memory
- RS: Recommended Standard
- RTU: Remote Terminal Unit
- SA: Security Association
- SAN: Storage Area Network
- SAS: Substation Automation System
- SATA: Serial Advanced Technology Attachment
- SCADA: Supervisory Control And Data Acquisition
- SCSI: Small Computer System Interface
- SDN: Software Defined Networking
- SDRAM: Synchronous Dynamic Random Access Memory
- SMB: Server Message Block

- SRAM: Static Random Access Memory
- SSD: Solid-State Disk
- STRIDE: Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, Elevation of privilege
- SV: Sampled Value
- SVC: Static Var Compensator
- TCP: Transmission Control Protocol
- TLS: Transport Layer Security
- TSO: Transmission System Operator
- UDP: User Datagram Protocol
- VHDL: Very High-Speed integrated circuit Hardware Description Language
- VPN: Virtual Private Network
- WAN: Wide-Area Network

List of Figures

List of Tables

1

Introduction

Electric power is currently the most efficient way to convert potential energy to working energy and transport that working energy to where it is needed using energy transport systems scattered across the globe. Energy transport systems include the infrastructures needed to transport non-electrical resources needed for production such as liquid petroleum, natural gas, or coal, but also, the power grid that enables transporting working energy under the form of electricity over long and short distances with some economies over transporting fuel. Indeed, the power grid allows moving energy from where it occurs naturally, or where it is produced efficiently to where it is consumed.

However, the components at the backbone of the power grid, delivering electricity to businesses and residences, are constantly being modernized to enable a more and more efficient and cost-effective delivery of energy. In this context, the brain of the so-called *smart grids* has become more and more complex, creating big challenges in the operation of the system both from the security, safety, and performance point of view. Indeed, the recent upgrades in the existing infrastructure with the integration of new components *-i.e., system—substation automation, GPS/satellite timing, new local and wide-area metering systems, advanced protection and control units* combined with distributed controllers and SCADA systems result in a very opaque and novel attack surface that exposes the system to a variety of new cyber-threats.

The "Cyber-Physical Risk of the bulk Electric Energy Supply System" (CYPRESS) project attempts to provide a valuable contribution to assessing the risks that threaten the transmission part of the grid as well as novel mitigation strategies to enable the resilient and secure operation of the system. In this context, Task 1.2 attempts to lay-out part of the foundation of the risk assessment methodology when considering the cyber-threat identification in the cyber-physical power grid. As further work packages attempt to provide frameworks for risk assessment and risk mitigation, T1.2 proposes a methodology to model the threats that may harm the cyber and/or the physical infrastructure as well as some preliminary leads on potential countermeasures.

In the context of such a task, the boundaries of the system that needs to be studied go beyond the system of interest. Indeed, threats on neighboring systems, as well as their potential consequences, might not be confined to the only neighboring infrastructure. In addition to that, components of large infrastructures such as power grids are incredibly heterogeneous with a variety of hardware and software components coming from different

vendors, using different technologies and protocols. All in all, coming up with an exhaustive list of threats and assessing their potential consequences is an incredibly difficult task.

Still, T1.2 attempts to partially answer the need for threat identification in a cyber-risk assessment methodology with two main objectives. Firstly, T1.2 aims at giving first sights on the hardware and software jungle that makes up the cyber-part of the cyber-physical power grid. Here, T1.2 seeks to describe the traditional and the power system-specific cyber-components that are or might be used in the real infrastructure. Then, T1.2 attempts to unveil the threats that might harm the whole system through those components in a methodological manner. Finally, T1.2 gives the first lead on potential mitigation strategies and countermeasures that should be studied in further work packages.

The threat identification methodology that was adopted in this work involved the bottom-up construction of useful abstractions. In other words, the cyber-components are first identified with as much exhaustiveness as possible and are then, methodologically agglomerated into higher-level abstractions based on the functionality they provide to the system -*i.e., the service* -. This agglomeration, called *Cyber-Space as Services* (CSaS), enables to have a broad but complete picture of the whole cyber-space and ease the task of identifying the cyber-threats that might be exploited. Complementarily, state-of-the-art industry standard threat identification methodologies such as STRIDE can be used to bring insight into how particular vulnerabilities of the system can be found and exploited. However, STRIDE lacks the ability to cover spontaneous bugs and failures scenarios while CSaS offers additional insights for simulations and risk assessment.

As soon as relevant threats are identified, mitigation techniques for cyber-physical resilience and security can be discussed. Those techniques may either focus on mitigating the impact of successful attacks and failures by keeping them localized or, directly prevent those attacks/failures from happening. In both cases, those techniques may also harm the performance or the good behavior of the system and therefore, should be studied with particular attention.

2

Cyber-Components & Services

Power grids can be seen as a particular type of cyber-physical system in which the computational cyber-part is tightly integrated with the physical components [1].

This chapter aims at identifying and describing the different cyber-components that are involved in the operation of the power grid. Indeed, the analysis of those components, as well as their interaction, is crucial to assess the overall performance and security of the entire system. However, the task of identifying every single type of device operating such a large-scale system is beyond the scope of this project. In this context, this chapter attempts to model the services provided by those devices that form the cyber-space and that enable the operations of advanced metering and control infrastructures.

2.1 Power Grids Control Systems

Power grids are operated using a complex interconnection of multiple systems and devices with many of these individual systems and devices being built upon newer, more intelligent components of generation, transmission, distribution, and metering. In this context, the number of devices and the flow of information that needs to be handled is becoming more and more important, making power grids a particularly difficult type of cyber-physical system to study.

This section aims at describing the tasks involved in the coordinated and synchronized work of all those devices and systems and positioning the cyber-space into these tasks. Then, this section will identify and describe the traditional cyber-components enabling the operation of general cyber-physical systems as well as components that are more related to the cyber-physical power grid.

2.1.1 Cyber-Space Architecture

The cyber-part of power grid systems attempts to coordinate, optimize and secure the interaction between the operators, the generation, the transmission, and the distribution sub-systems. More specifically, cyber-

components sense the state of the system and environment and then provide continuous feedback for controlling the system and actuating on the environment.

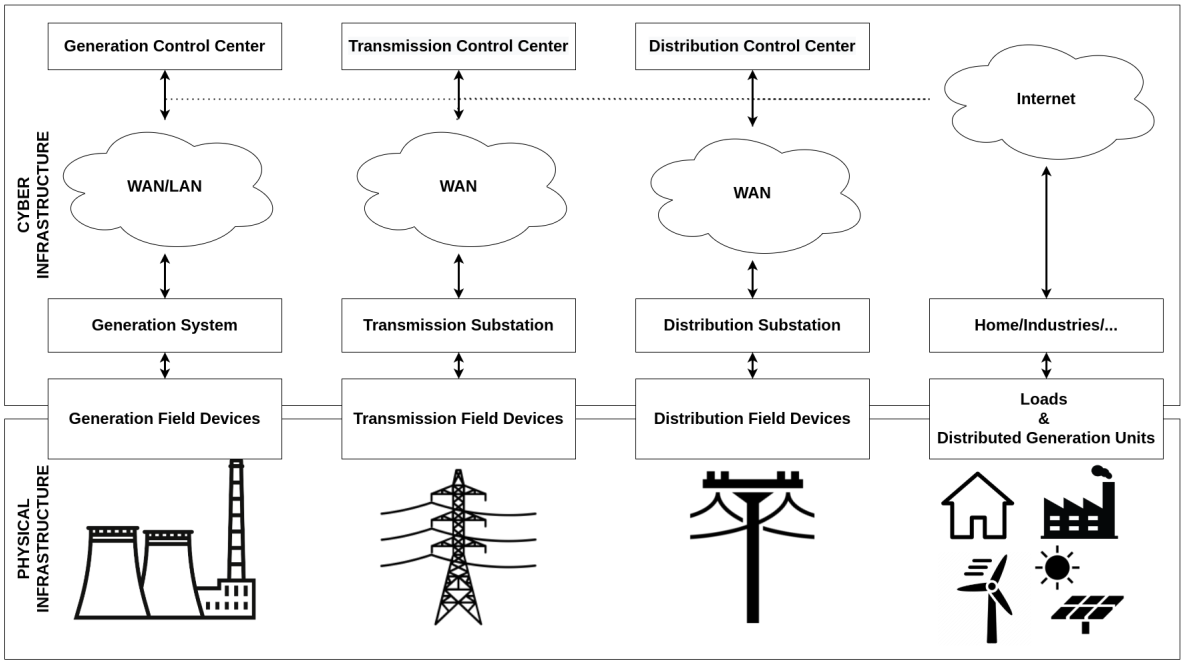

Figure 2.1: Cyber-Physical view of the Power Grid

Figure 2.1 represents a general view of the interaction between the different physical sub-systems as well as the devices that coordinate these interactions. It also attempts to represent the common concepts around information generation, utilization, and automation that are used to operate the power grid.

Generation System

The generation system is the part of the power grid that comprises the power generation units supplying power to the entire power grid. Power generation systems can be divided into two categories: (1) Centralized generation and, (2) Decentralized generation. Historically, the generation sources were provided electrical power through the transmission systems. However, the advent of decentralized generation sources modified this historical structure. Indeed, more and more generation sources are directly connected to the distribution systems.

The generation control system allows ensuring the stability and safety of operations by maintaining a constant equilibrium between power production and load demands. Indeed, a disequilibrium would cause a shift in the frequency of the network which may harm the physical infrastructure. To do so, the system relies on three control loops, namely primary, secondary, and tertiary control [2]. While the first two operate automatically and without the need of human operators under normal conditions, the third typically involves the power grid operator to manually adjust the dispatch of some power plants. On the other hand, the primary frequency control system mainly uses local measurements, controllers, and actuators that are close to power plants/generation units while the secondary frequency control and tertiary frequency control are typically implemented via remote control centers. Finally, the primary and the secondary control systems typically operate in the range of seconds while the tertiary may operate in the time frame of minutes to hours.

Tasks Some of the tasks involved in the operation of the generation systems are [2],[3],[4]:

1. *Frequency regulation:* As mentioned above, it is important to keep the frequency of the grid in a narrow range around its nominal value to guarantee the stability of the system. Firstly, it is necessary for the correct operation of the generators and loads and secondly, it is an indicator of the active power balance between generated and consumed power. Thus, frequency regulation is intended to adjust the grid frequency when it deviates from its nominal value and this regulation can be done by acting on the generation or controllable loads.

2. *Voltage regulation:* The voltage must be kept within acceptable limits: not too high so as not to damage insulators, sensitive equipment, etc., but not too low so as not to disturb/interrupt the operation of certain components. Voltage regulation can be performed locally either at generation level by means of generators or using dedicated reactive power compensation devices. Note that some synchronous machines equipped with a voltage regulator are only used to regulate the voltage at one point of the grid (and do not produce active power), these are called synchronous compensators (or condensers).
3. *Undervoltage protection:* In extreme situations, the voltage of a generator can decrease sharply, so that the auxiliary equipment of the power plant, such as the pump motors, can no longer be supplied correctly. In this case, Undervoltage protection is needed.
4. *Loss of field protection:* It is necessary for the event that a failure of the excitation system would cause the amplitude of the electro-magnetic field in the machine proportional to the excitation current to fall below its minimum limit. In such a case, there would be a loss of synchronism of the machine, which therefore requires protection to avoid damage to the machine by losing this synchronism.
5. *Fulfill its role as a Balancing Service Provider:* A producer may engage as a Balancing Service Provider. In this case, its role is to balance the unplanned fluctuations on the power grid by rapidly increasing or decreasing its production. This production is adapted by the producer according to the requests provided by the TSO.

Action Space The cyber-space can perform several control and monitoring actions on the physical infrastructure of the generation systems [2]–[6]:

1. *Measurement of the rotation speed of the turbine-generator assembly of a generating unit:* In the case of grid frequency control, this measurement is compared with the nominal rotational speed (corresponding to the nominal frequency of 50 or 60 Hz) and the following action may result.
2. *Act on the control valves of a generating unit to increase or decrease the fluid intake to the turbine:* In the case of frequency control, a speed controller will use the difference between the measured and the nominal speed to increase/decrease the fluid (steam, gas, or water) input to the turbine. Therefore, this action amounts to varying the output of the generation unit. Note that not all generators in a grid participate in this control and that to do so, its output must be placed below the maximum capacity of the turbine (so that it is ready to produce more).
3. *Measurement of the voltage at the MV busbar of a generator via a potential transformer:* This measurement may be used for voltage regulation.
4. *Modification of the excitation voltage of a synchronous machine:* To regulate the voltage at the MV busbar of a generator, the measured voltage is compared to the voltage setpoint. If this measured voltage decreases or if the setpoint increases, the excitation voltage[1] of the generator increases, and vice versa. This regulates the voltage and changes the reactive power produced and this is usually done with an *Automatic Voltage Regulator*.
   Note that in some cases (over/under-excitation limiters), the voltage setpoint depends on a current measurement to be regulated instead of voltage measurement. In this case, the machine is controlled in current but the action still consists in modifying the voltage setpoint.
5. *Measurement of the rotor or stator current of a synchronous machine:* The goal may be to keep this current within certain limits and as explained above, this measurement may enable voltage regulation.
6. *Trip a generating unit:* In order to protect a generator in case of under voltage, for instance, protection constantly monitors the system voltage. If the voltage level goes below its acceptable limits, the undervoltage protection may trip the generator. A loss of field protection can also trip a machine to prevent it from being damaged by losing synchronism.
7. *Vary the production output of a generating unit.* For example, a generating unit with a Balancing Service Provider role must respond to its TSO requests by varying its output in order to keep the balance. Note that some of the actions listed above result in varying the production output, but here it is simply a matter of varying this output regardless of the method.
8. *Adjust the reactive power of a Distributed Energy Resource.* In order to regulate the voltage of the distribution grid, the DER grid support functions with reactive power capabilities can be used. Indeed, various control

[1] An exciter is an auxiliary machine supplying a direct current under a direct voltage and must be able to vary these quantities rapidly following a variation in the signal supplied by the voltage regulator.

functions, such as those described in [7], can be included in DER devices to adjust the reactive power and, by extension, the grid voltage. Note that this kind of setting is not yet widespread but will become more important as DERs continue to be deployed.

9. *Measure of non-electrical parameters* There are several other parameters that should be monitored by the operators such as water or steam pressure, boiler or burner temperature, etc. For instance, it is important to monitor the metal tube temperature of a power plant's boiler in order to ensure efficiency, optimized fuel consumption, reliability, and availability of boiler unit [8]. On the other hand, temperature of generating units can be measured by several means *-i.e.,* thermocouples embedded in the slots of the stator windings or by recording the difference between the inlet and outlet of the cooling medium - to protect a generator from overheating. Monitoring other parameters of a boiler such as pressure or humidity should be done for safety and to improve the reliability of the boiler.

Applications The cyber-space allows the automatic & manual operation of the generation systems through several subsystems:

1. Centralized generation: Generation management systems (GMS) which comprise a set of tools management of centralized or geographically distributed generation facilities including SCADA capabilities, forecasting, etc. A GMS usually presents the following primary functions:
   - EMS/SCADA provides real-time control and monitoring of geographically localized generation systems at the TSO level.
   - DCS (Distributed Control Systems) provides monitoring and control of the generation assets at the power plant level.
   - Monitoring, scheduling, and control of the distributed generation assets at the generation company level.
   - Work management: determine and schedule human worker interventions.
   - Energy trading functions for participation in the energy markets.
   - Black start capabilities allow the autonomous restart of a plant without reliance on the transmission grid in the case of its unavailability, e.g during a blackout scenario.
2. In the decentralized case, no central authority decides when generation happens. The advanced metering infrastructure (AMI) and IoTs are used. IoTs can be used to schedule local consumption while the AMI can be used by DSOs to learn about the amount of energy produced and consumed locally. (see more in the loads system section 2.1.1).

Transmission System

The transmission system is the part of the power grid that allows the delivery of electricity from the place where it is generated to the site where it is used. The electricity leaving the generating station enters a first substation that raises the voltage using a *step-up transformer* to improve long-distance transmission. Then, the high-voltage electricity is carried over transmission lines and transmission substations to local distribution substations where a *step-down transformer* reduces the voltage to levels suitable for customer loads. Some customers needing a very large amount of electric power may be connected directly to some of those substations for specific usages. By their nature, transmission systems spread over wide areas, with power lines covering large geographic areas. Therefore, they require wide-area communication technology to support remote real-time monitoring and control of the infrastructure.

The transmission control system mainly deals with the grid topology, reactive power compensation, voltage regulation, and line protection. The system consists of heterogeneous, geographically spread substations that operate on the physical infrastructure using tap-changing or phase-shifting transformers, flexible AC transmission systems (FACTS), and switchgear. While the transmission grid is constantly being monitored and controlled by human operators in a centralized control room, automatic control loops become more and more common to address the increasing need for efficiency and flexibility of the transmission grid. Indeed, the advent of new distributed generation and energy storage units as well as of new metering devices involves both new challenges and potential improvements to the operations of the entire power grid.

Tasks Some of the tasks involved in the operation of the transmission systems are [3], [4], [6], [9]:

1. *Voltage regulation.* The voltage must be kept within acceptable limits: not too high so as not to damage insulators, sensitive equipment, etc., but not too low so as not to disturb/interrupt the operation of certain components. This regulation can be implemented at the transmission level.

2. *Protection of the system and its equipment against faults (short circuits).* It is necessary to protect power grids from faults by disconnecting the faulted parts from the rest of the system. The purpose of a protection system is to maintain the stability of the power grid by isolating only the faulty equipment while leaving as much of the grid as possible in operation, to protect power system equipment from damages and most importantly to ensure safety for humans.

3. *Balancing consumption and production.* A TSO aims to maintain the balance on the transmission grid in real-time by making use of the market flexibility offered by Balancing Service Providers. Those are market participants, such as generators or demand facilities, providing balancing services to their connecting TSO. Their role is to balance unforeseen fluctuations on the power grid by rapidly increasing or reducing their power output.

4. *Re-routing (active) power flow.* In case of grid congestion, it may be needed to re-route power flows via more favorable paths in order to relieve overloads on heavily loaded circuits.

5. *Generation dispatch.* In order to avoid or resolve occurring congestion, the TSO can ask (dispatchable) power plants operators to adjust their active power output: some power plants will have to lower their production while others will have to increase it so that the congestion is avoided while the total active power production is still the same.

Action Space The cyber-space can perform much control and monitoring actions on the physical infrastructure of the transmission systems [2], [3], [10], [11]:

1. *Measurement of the voltage at a busbar.* In the case of voltage regulation, this measurement will allow reacting, for example, with the connection of shunt capacitors or inductors or by acting on the turn ratio of a transformer, as described below.

2. *Adjust the number of turns of a transformer connecting different voltage levels.* The purpose of this action is to adjust the voltage in the vicinity of the transformer. This can be done either on-load (On-Load Tap Changer) or by manual tap-changing (No-Load Tap Changer) once the unit is de-energized and the taps adjustment can be done automatically (most often for OLTC) or remotely by an operator from a control center (more common for NLTC). These tap changers are placed on transformers between EHV transmission and HV distribution systems. Note that some transformers are fully dedicated to voltage regulation.

3. *Opening/closing the circuit breaker of a shunt element to switch it off/on.* For voltage regulation purposes, connecting shunt capacitor banks allows to produce reactive power and to correct a voltage drop at a busbar while connecting shunt inductors allows to consume reactive power and to correct a voltage increase. Their switching is either manually controlled (from a control center by an operator having a voltage remote measurement) or automatically (via a device located in the substation which switches on the shunt element when the voltage exceeds a low/high threshold and remains there for a specified time).

4. *Controlling the power electronics of Static Var Compensators.* For network applications, Static Var Compensators (SVC) can be used to regulate nodal voltage and improve system stability. This action is close to the previous one, an SVC is composed of one or more banks of fixed or switched shunt capacitors or reactors, of which at least one bank is switched by thyristors. The latter are electronically controlled semiconductor switches. SVCs are therefore used to inject reactive power quickly using power electronics. Nowadays, they are preferred to traditional synchronous compensators (STATCOMs and STATCONs) as described in Section 2.1.1.

5. *Measurement of the current of a line via a current transformer* so that the protection systems can use this measurement to act or not.

6. *Measurement of voltage of a line via a voltage transformer* so that the protection systems can use this measurement to act or not.

7. *Measurement of the impedance of a line seen from one end of the line using those current and voltage measurements.* Indeed, some protection systems need the impedance value in order to make decisions.

8. *Opening of circuit breakers located on a line.* For instance, if a short circuit occurs on the network and the protection system monitoring a line detects the appearance of high currents or the decrease in impedance, it can send a signal to open the circuit breakers located at both line ends[2], which puts the line out of service and eliminates the fault.

9. *Return of a line to service.* Transmission system lines are equipped with automatic reactivation devices that return the line to service after a certain delay. Note that there is no reclosing possible for the cables.

10. *Modify the difference in the phase angle of the voltage between the two sides of a transformer (phase-shifting transformer).* Phase-shifting transformers work by adjusting the phase angle of the voltage of two parallel lines so that we can control the current distribution between the two lines. The active power flows can therefore be controlled, which allows, in case of overload of a part of the network, to redirect the power through more favorable paths.

11. *Control the active power flowing through an HVDC line.* It is possible to control the AC-DC converters to decide the active power that should flow (in one direction or the other) from one HVDC converter substation to another. Voltage source converter based HVDC links can also be used for voltage control and improvement of system stability.

12. *Opening and closing circuit breakers within a substation.* In order to avoid congestion, an operator may change the topology of the grid by reconfiguring the connections between buses, lines, and transformers in a substation. This is done by acting on circuit breakers.

Applications The cyber-space allows the automatic & manual operation of the transmission systems through several subsystems:

1. EMS/SCADA system: main system responsible for the control and monitoring of the transmission grid, it provides all the elements and real-time information needed to support operational activities and functions relevant to transmission automation in dispatch centers and control rooms.

2. Substation automation system: elements necessary to the remote or local automatic operation of a substation and its connected assets (e.g. loads, gridlines).

3. Blackout prevention system: prevent instability and collapse in power systems while ensuring the continuity of load growth in the context of reduced operating margins within stability limits.

4. Flexible AC Transmission System (FACTS): a collection of systems based on power electronics. These solutions are applied in power systems to provide a rapid dynamic response, the ability for frequent output variations, and smoothly adjustable output. Use cases of FACTS in the context of transmission systems include fast voltage control, increased transmission capacity over long lines, power flow control in meshed systems, and power oscillation damping.

Distribution System

The distribution system is the part of the power grid that allows the transmission of electricity from distribution sub-stations, that are responsible for transforming the high voltage electric power coming from the transmission lines into a medium voltage range. Then, medium-voltage electricity is carried over distribution lines and distribution substations where transformers again lower the voltage to utilization voltage. At this point, the electric power can be directly used by industries, commercial and residential customers.

The distribution control system is responsible for the control of distribution operations, including manual and automated control of load management, voltage regulation, and line protection. Similar to the transmission system, the distribution grid is often being monitored and controlled by human operators in a centralized control room with more and more decentralized and distributed control and monitoring. Indeed, the distribution control system is the first entity needing to interact with distributed generation units.

Tasks Some of the tasks involved in the operation of the distribution systems are [3]:

1. *Voltage regulation* (cfr. Paragraph on Transmission System)

2. *Protection of the system and its equipment against faults (short circuits).* It is necessary to protect power grids from faults by disconnecting the faulted parts from the rest of the system. The purpose of a protection

[2] Typically, circuit breakers are located at both ends of a transmission line.

system is to maintain the stability of the power grid by isolating only the faulty equipment while leaving as much of the grid as possible in operation.

3. *Re-routing (active) power flow.* In case of grid congestion, it may be needed to re-route power flows via more favorable paths in order to relieve overloads on heavily loaded circuits. It should be noted that this is more difficult to do than in transmission grids due to the (mostly) radial/loop topology.

4. *Load shedding or rolling blackout.* If the demand for electricity exceeds the power supply capability of the grid, in order to stabilize the system against generation outages or voltage drops, load shedding consists of voluntarily stopping the supply of one or more consumers to quickly restore the balance between production and consumption of the grid.

Action Space The cyber-space can perform much control and monitoring actions on the physical infrastructure of the distribution systems [3],[11]:

1. *Measurement of the voltage at a busbar.* In the case of voltage regulation, this measurement will allow reacting, for example, with the connection of shunt capacitors or inductors or by acting on the turn ratio of a transformer, as described below.

2. *Adjust the number of turns of a transformer connecting different voltage levels.* The purpose of this action is to adjust the voltage in the vicinity of the transformer. This can be done either on-load (On-Load Tap Changer) or by manual tap-changing (No-Load Tap Changer) once the unit is de-energized and the taps adjustment can be done automatically (most often for OLTC) or remotely by an operator from a control center (more common for NLTC). These tap changers are placed on transformers feeding MV distribution networks. Note that some transformers are fully dedicated to voltage regulation.

3. *Opening/closing the circuit breaker of a shunt element to switch it off/on.* For voltage regulation purposes, connecting shunt capacitor banks allows to produce reactive power and to correct a voltage drop at a busbar while connecting shunt inductors allows to consume reactive power and to correct a voltage increase. Their switching is either manually controlled (from a control center by an operator having a voltage remote measurement) or automatically (via a device located in the substation which switches on the shunt element when the voltage exceeds a low/high threshold and remains there for a specified time).

4. *Controlling the power electronics of Static Var Compensators.* For network applications, Static Var Compensators (SVC) can be used in order to keep the voltages at certain nodes almost constant and to improve the stability of operation. This action is close to the previous one, an SVC is composed of one or more banks of fixed or switched shunt capacitors or reactors, of which at least one bank is switched by thyristors. The latter are electronically controlled semiconductor switches. SVCs are therefore used to inject reactive power quickly using power electronics. Nowadays, they are preferred to the synchronous compensators described in Section 2.1.1.

5. *Measurement of the current of a line via a current transformer* so that the protection systems can use this measurement to act or not.

6. *Measurement of voltage of a line via a potential transformer* so that the protection systems can use this measurement to act or not.

7. *Measurement of the impedance of a line seen from one end of the line using those current and voltage measurements.* Indeed, some protection systems need the impedance value in order to make decisions.

8. *Opening of circuit breakers located on a line.* If a short circuit occurs on the network and the protections monitoring a line detect the appearance of high currents or the decrease in impedance, they open the circuit breakers located at both ends[3], which puts the line out of service and eliminates the fault.

9. *Modify the difference in the phase angle of the voltage between the two sides of a transformer (phase-shifting transformer).* Phase-shifting transformers work by adjusting the phase angle of the voltage of two parallel lines so that we can control the current distribution between the two lines. The active power flows can therefore be controlled, which allows, in case of overload of a part of the network, to redirect the power through more favorable paths. However, the high cost of phase-shifters makes them rarer in distribution systems than on the transmission side.

[3]Typically, circuit breakers are located at both ends of a distribution line.

Applications The cyber-space allows the automatic & manual operation of the distribution systems through several subsystems:

1. Advanced Distribution Management System: main system responsible for the control and monitoring of the distribution grid, provides all the elements and real-time information needed to support operational activities and functions relevant to distribution automation in dispatch centers and control rooms. Its major functions are real-time monitoring and control (SCADA), work and outage management, grid modeling, and other advanced grid applications.
2. Feeder automation system: provides all the elements and functionalities to automatically operate the components present within the distribution grid itself, e.g. feeder lines, circuit breakers, switches, disconnectors.
3. FACTS devices: same description as in transmission systems. Uses cases of FACTS in the context of distribution systems include: feeder load balancing, new component discovery, and configuration, clock distribution, and synchronization, monitoring and reduction of voltage flicker and harmonic mitigation, management of the connection of generation to the grid.
4. Substation automation system: same role as in transmission systems.

Load system

The load system is the part of the power grid that is related to consumers' demand. Traditionally, the load of a given consumer was entirely under their immediate control. However, the modernization of the power grid and its transformation into a smart grid introduces some automation of the load. Through the introduction of digital meters and increased use of ICT and controllable of electrical loads (such as heating systems, EVs, smart appliances, ...), consumers can get access to different pricing schemes or markets (such as balancing, automatic frequency reserves,, ...).

The load can thus be indirectly controlled via pricing incentives. Consumers can automate this sort of behavior in the context of a smart home by using IoT (Internet of Things) devices. For example, one may program an IoT to only charge an electric vehicle when it is least expensive while still guaranteeing adequate battery levels when necessary.

Prosumers may even go even further by allowing instructions from power grid operators (transmission grid for big consumers, distribution grid for the others) to non-intrusively regulate their consumption with IoT devices, e.g. turn off the air conditioning for short intervals during peak demand time. They may even allow intrusive control against remuneration.

Tasks Some of the tasks involved in the operation of the loads are [12]:

1. *Undervoltage protection.* Undervoltage conditions can have adverse effects on electric motors. Indeed, these are designed to operate under specific rated conditions of current, speed, mechanical torque, temperature, frequency, and voltage, and under-voltage may reduce performance or even make it completely mechanically fail.
2. *Overheating protection.* Loads such as motors need to be protected against overheating.
3. *Demand response.* In order to match the demand for electricity with the available supply, consumers can adjust their demand instead of adjusting the supply. This change in a customer's power consumption is called demand response and is part of demand-side management.

Action Space The cyber-space can perform several control and monitoring actions on the loads [3],[13]:

1. *Monitor the temperature of a machine or a device.* To prevent overheating, sensors can monitor the temperature of industrial machines.
2. *Shutting down-loads.* For example, to protect against under-voltage, loads can be switched off. Another example is when high-use industrial consumers have agreements with electricity utilities to turn off equipment at times of system-wide peak demand.
3. *Controlling the power electronics of Static Var Compensators.* Static Var Compensators can be used for dynamic load compensation. They can be used to balance loads with phase imbalance or to stabilize the voltage across a rapidly fluctuating load, typically by being connected near large industrial loads such as

arc furnaces. As written above, an SVC is composed of one or more banks of fixed or switched shunt capacitors or reactors, of which at least one bank is switched by thyristors. The latter are electronically controlled semiconductor switches. SVCs are therefore used to inject reactive power quickly using power electronics.

4. *Measure (real-time) consumption of a consumer using a smart meter.* A smart meter is a digital meter that electronically records information such as the amount of energy a consumer takes from the grid, the amount of energy he injects, as well as the voltage and current levels or the power factor. It stores this data in its memory and transmits it remotely to the relevant DSO.
   The consumption data can be used to prepare the consumer's bill but also to help system operators understand the needs of the power grid with great granularity (compared to older meters). This facilitates system planning to meet consumers' energy needs by reducing the need for additional infrastructure investment.
5. *Measure (real-time) production of a prosumer using a smart meter.* The production can also be used to prepare the consumer's bill.
6. *Measure (quasi-real-time) voltage, current, and power factor of a consumer's power system.* These measurements can help operators detect system disruptions more rapidly and thus help to react directly with corrective actions to minimize negative impacts such as blackouts.
7. *Turning on a load.* An appliance can be turned on via the cyber layer either automatically if for instance the consumer is equipped with a system that allows programming the turning on of electrical appliances in advance ("Smart Home"), or remotely via an energy management application. For instance, starting up a device might depend on time-based pricing information. Price signals are sent to the consumer's system and the system starts devices when it is the more economically interesting.
8. *Charging/discharging home batteries.* In response to high price signals sent from the electricity utility, a customer may adjust its power demand by switching part of its consumption to alternate sources such as batteries if he has some and charge the battery in low price moments.

Applications The cyber-space allows the monitoring and control of the loads through the AMI:

1. The Advanced Metering Infrastructure (AMI) empowers the monitoring and control (when financially compensated) of consumer loads. Its main use is billing with dynamic prices. It may be used for demand-side management through a connection with generation and demand flexibility systems. Within a smart grid, demand-side management is used as part of monitoring and controlling the actions of the wider grid. The AMI is composed of:
   - The smart meters that perform the monitoring and control on the consumer side
   - Home network gateways that provide communication facilities
   - Meter data concentrators and Head-end Systems which manage data communication with the meters and their integration with a Meter Data Management system (MDM) by coordinating Wide Area Network (WAN) communications
   - The Meter Data Management system (MDM) interfaces the AMI with the energy markets.

2.1.2 Traditional Power System Tasks

This section aims at giving first sights into the traditional tasks that are performed to operate power systems and how the cyber-space integrates into those tasks. Particularly, this section will focus on the protection, automation, and control philosophy of the Belgian transmission system operator, Elia [10]. Additional information on this part has been given in deliverable D1.1 [2] but this section attempts to complete the view of the reader and to make the document standalone.

Protection Task

Protection systems englobe the set of equipment and functions that seeks at detecting a fault and taking actions -*i.e., tripping* on grid components to prevent any further damage or cascading effects.

Protection systems of HV grids are composed of 3 main parts: **(1)** the measurement device (via current and voltage transformers), **(2)** the protection device (protection relays), and **(3)** the actuating device (circuit breaker).

The measurement transformers (or instrument transformers) will, as their name indicates, measure the current and/or the voltage, the protection relays will detect a fault via this/these measurement(s) and send a decision to the circuit breakers that are used to isolate the element from the network and interrupt the short-circuit current. Note that a "protection system" refers to all the elements of the chain, including the instrument transformer(s) that might be connected to the protection relay itself connected to the circuit breaker. In addition to circuit breakers, high-voltage substations are often equipped with devices called disconnectors (or disconnect switches). These electromechanical devices allow to mechanically separate an electric circuit from its supply. Contrary to circuit breakers and switches, they do not have any cutting or closing power, only a separation function.

There are 3 main types of protection: electrical, mechanical, and logical, each providing particular guarantees on reactivity, sensibility, etc.

Electrical Protections For electrical protections, the protection system depends on the environment:

- *Overcurrent Protection* In the context of a single current transformer, the protection system often consists of overcurrent relays. The relay simply measures the current and trips a circuit breaker in the case of a significant increase of current. Here, the increase of current is considered as a fault of the circuit that is being monitored.
- *Distance Protection* In the context of a hybrid configuration with voltage and current transformers, the protection system often makes use of a distance relay. Here, the direction of the fault is determined as the "current transformer-fault" distance is calculated through the impedance. The impedance is simply obtained by measuring the current and voltage and depending on the value of this impedance and the direction, a trip occurs or not. Note that a problem with this type of protection is that tripping is delayed for a fault beyond a certain distance (80% of a line). The solution is a remote protection system that helps the local tripping by exchanging information between the distance protections at each end of the line.
- *Differential Protection* Here, the protection takes advantage of Kirchhoff's law as it monitors for a non-zero vector sum of the currents at a node. If a non-zero value is detected, it means that there is a fault on the network. Note that a "node" can be a line, a transformer, or a rail and the operation depends on this element.

Mechanical Protections When looking at mechanical protections, a very good example is the Buchholz protection, placed on the transformers that seems to be very common. The protection will rely on relative pressure and displacement of oil to detect internal fault and trips when required. As this document is focusing on the cyber-layer, the actions of such mechanical protection do not seem to be of particular relevance.

Logical Protections There are mainly 2 types of logic protections:

- *Backup Protections* are the main protection for the trip refusal of an outgoing feeder connected to the busbars. If the outgoing feeder is faulty, its protection sends a trip to the circuit breaker and the backup. If this signal lasts more than a fixed delay in the backup, it sends a tripping order to all the outgoing feeders connected to the same busbar.
- *Ramelot/LGR Protections* protects the MV busbars. There is a trip when there is no current start on the feeders while there is a transformer start. On the other hand, there is no tripping when the transformer starts and at least one feeder starts.

Automation & Control

Automation aims at performing tasks faster than a dispatcher while also allowing decentralized management of on-site tasks. Similarly to control tasks, automation is either done locally (directly in the substation) or remotely (from the national control center). In Belgium, all Elia substations are equipped with a remote control system, which is realized via Remote Terminal Units (RTU) or Digital Controlling Systems (DCS). A brief description of the major types of automated and control loops used in power systems is given in [2].

2.1.3 Traditional Cyber-Components

Similar to many computerized systems, the cyber-operations of the power grid make extensive use of traditional cyber-components - *i.e.,* components that are not specific to cyber-physical systems. In this context, this

section aims at identifying, describing the general components that can be found in any computerized system. This may include hardware or peripheral devices such as processors, network materials, hard disks, etc but also any kind of piece of software such as database management systems, firewalls, forwarding algorithms, etc.

Programmable hardware With the advent of Field-Programmable Gate arrays (FPGAs), the algorithms contained in hardware *-i.e.,* not those which are executed in software on internal processor cores - are no longer frozen in silicon. Many software algorithms can be translated to be executed directly in hardware without the loss of performance that is characteristic of software applications run on classic instruction-based architecture such as CPUs and GPUs. These hardware circuits can be programmed using Hardware Description Languages (HDL) such as VHDL and Verilog. From a theoretical perspective, HDLs are also Turing complete which makes them able to express any type of computation. Therefore, some of the applications that will be described in further sections may also be run directly on hardware for obvious performance reasons. On the other hand, the complexity of choosing the appropriate type of FPGA and programming makes them often more appropriate for prototyping and/or low quantities production nowadays. However, upcoming technologies aim to address this complexity partly using High-Level Synthesis (HLS) which allows programming FPGAs using regular programming languages such as OpenCL or C++ but they still require extra programming skills as well as having very high compilation times.

Virtualization Application-Specific Standard Parts (ASSPs) and Application-specific Integrated Circuit (ASICs) refers to hardware electronic chips that are designed and implemented for very specific purposes. They are often incredibly expensive, time-consuming, and resource-intensive to develop but offer extremely high performance and very low power consumption. However, the lack of flexibility of those very application-specific pieces of hardware and their huge development cost is not aligned anymore with the newcomer paradigms. Indeed, more and more applications would like to rely on commodity hardware that allows easy maintenance and stock management as well as lower development costs. In this context, more and more devices are being virtualized or run directly as pieces of software on non-specific pieces of hardware with acceptable performance [14], [15].

Communication Systems

Communication is the process through which information is exchanged between entities in a system using one or more communication mediums. The communication medium can vary a lot from a system to another with some using very old mediums such as postal networks and others using very recent computer networks. While all those communication mediums have very specific differences, they are based on some basic principles of operations such as intermediate entities, protocols, and security mechanisms. Indeed, packets on computer networks and envelopes in postal networks have a lot of common characteristics such as wrapping the raw messages in TCP/IP packets for the former and in an envelope for the latter with some additional information. Then, intermediate devices will relay the wrapped raw message from the source to the destination using that additional information. However, those additional information needs to be formatted to comply with some predefined protocols so that the intermediate devices can efficiently exploit them. Finally, sealing wax provided similar functions that cryptographic hashes to detect some kind of tampering by intermediate entities. In this context, this section aims at describing the mechanisms and devices in computer networks that enable most of the communication between cyber-entities within the cyber-physical power grid.

Communication Channels The communication channels refer to the logical or physical view of the medium allowing the transmission of an information signal from one or several senders to one or several receivers. Communication channels can be characterized by several metrics that can evolve depending on network conditions [16]:

- A bandwidth which indicates the amount of information that can be transmitted over a given period of time. It is generally expressed in bits/sec.
- A latency which indicates the amount of time taken by the information signal to transit from its source to its destination. It is generally expressed in seconds or milliseconds.
- A drop rate which indicates the proportion of information that will not reach its destination. It is generally expressed based on the discretized unit of information considered *-e.g.,* packets.
- An error rate which indicates the proportion of information that has been altered during the transmission. It is generally expressed based on the discretized unit of information.

The physical communication medium may take many forms such as radio waves, Wi-Fi, Unshielded Twisted Pair cables, etc while logical channels may comply with different protocols such as Modbus, CAN, Ethernet, DNP3, etc for short-distance communication or TCP/IP complying protocols for long-distance communications.

Communication Protocols Communication protocols comprise a set of rules *-i;e., protocol specifications* that govern the format and interactions between two communicating parties. In the context of cyber-components, these rules need to be explicit and unambiguously formalized to enable reliable and secure communication between independent parties.

When looking at long-distance communication, most of the systems are complying either with the Open Systems Interconnection (OSI) or the legacy TCP/IP model [2]. While both are are providing a logical view of networking mechanisms using a layered system, OSI segments multiple functions that TCP/IP groups into single layers. This difference might seem subtle but OSI highly reduces the complexity of troubleshooting issues and enhance performance.

On the other hand, serial protocols formalize the synchronous or asynchronous communication of cyber components over a serial line. In this context, data are sent one bit at a time in a sequential manner over a serial line. Then, lines can be multiplied to increase the throughput and concurrently send several bits at the same time [17]. Serial communications are still extensively used in power grid systems for short-distance communication between components in substations among others. For instance, legacy RTUs typically communicate with the SCADA (cfr. Section 2.1.5) master controller over a serial communication line using one of the traditional SCADA protocols such as Landis and Gyr 8979, GETAC, Harris m9000, IEC60870-5 or Modbus [18]. However, the advent of Intelligent Electronic Devices (IEDs) in the automation of cyber-physical systems leads more and more substations to turn to high-speed Ethernet buses that make easier the implementation of comprehensive management, maintenance, and control strategies.

Modbus is a legacy protocol that can only be used in a master-slave configuration. The master sends instructions or queries to the slave that must execute and answer them. Only the master is allowed to initiate communication. The initial version of Modbus ran directly over a serial connection between master and slave but nowadays, there is also a version of Modbus that runs over Ethernet [18], [19]. Then, IEC60870-5 is a Modbus-inspired, master-slave protocol that was developed specifically for power systems and in which the master can poll the slave for information and send instructions [18], [19]. While IEC60870-5 is the preferred protocol in Europe for communication between control centers and remote substations, regions such as North America are using the Distributed Network Protocol version 3 (DNP3) which is a protocol based on an early version of IEC60870-5. IEC60870-5 can run both over Ethernet or over TCP. The possibility of running it over TCP is particularly relevant when the master station is located far from the substation and it can only access it via a (private) Wide Area Network (WAN) [18], [19].

Communication Devices Communication devices comprise all the hardware and software components that enable the communication system to relay analog or digital signals from one or several senders to one or several receivers over a communication channel. Regarding computer networks, the following devices can be enumerated:

- *Network Interface Controllers (NIC)* implements the electronic circuitry needed for a device to communicate using a specific physical and data link layer standard such as Ethernet (IEEE 802.3) or Wi-Fi (IEEE 802.11). The NIC is both a physical layer and data link layer device, as it provides physical access to a networking medium and, for IEEE 802 and similar networks, provides a low-level addressing system through the use of MAC addresses that are uniquely assigned to network interfaces.
- *Modems* (contraction for modulator-demodulators) are devices used to convert data from a digital (binary) format into a format that is suitable for transmission over an analog channel. Modems can be included as components of higher-level devices such as wireless access points or routers. In the context of computer networking, all wireless communication involves a modem. However, modems can be used in other contexts, e.g to transmit network packets through the telephone network, or optic fiber. Concretely, a modem performs two tasks: modulation and demodulation. Modulation is the encoding of binary data into a carrier wave, while demodulation is the reverse operation, i.e. retrieving binary data from the carrier wave.
- *Hubs, switches, and bridges* allow devices to communicate as if they were directly connected, i.e. they form a Local Area Network (LAN). Hubs and switches accomplish this by simple forwarding of Ethernet frames. The difference between both is that switches learn behind which interface a given destination is located

and simply forward on that interface, while hubs broadcast the frames they receive on all interfaces. Bridges accomplish the same role of transparently connecting devices but, larger than hub and switches, the term can refer to devices that interconnect networks using two different technologies, e.g. Wi-Fi and Ethernet.

- *Wireless access points* are devices used to allow wireless devices to communicate with devices on a wired network. The access points present both wireless (typically Wi-Fi) and wired (typically Ethernet) communication capabilities so that they can forward appropriately. It is common for routers to include an access point but several additional access points can be placed in a single LAN (e.g. by connecting them to switches) to offer a more physically widespread wireless connectivity.
- *Wireless repeaters* can be used as an alternative to setting up multiple wireless access points. A repeater offers wireless connectivity for devices to join the LAN and relays that information wirelessly to an access point. It is only by indirection through the access point that devices connected to the repeaters can access the wired network.
- *Network links* refer to any communication medium that allows two devices to communicate with one another. The nature of said links can vary immensely. A link is either physical or logical. Examples of physical links between devices are Ethernet cables, optic fiber, or electromagnetic waves. Logical links are (in)direct connections that rely on physical links and (distributed) software and special hardware (e.g routers) to connect remote devices. An HTTP session between a browser and a web server is an example of a logical link. IP tunnels are logical links that can be used to connect networks that are physically remote from one another. Essentially, all networked applications are built upon communication over logical links.
- *Middleboxes* - Middleboxes are networking devices that are placed in a network to inspect, filter, and modify packets in ways that are not necessary for forwarding. These devices can be deployed to provide interesting functionalities for network engineering but they can interfere with application behaviors and break the important end-to-end principle. This principle states that intermediate nodes should not interfere with application data and features. The end-to-end principle reserves such data to the end hosts.

  As middleboxes can deal with application data, there are few limits to the functionalities they can offer. Enumerating all types of middleboxes is not possible as these can transform application data in any way. However RFC3234 establishes a taxonomy of common types of middleboxes. Examples of common middleboxes are [20]:

  - *Firewalls* - (cfr. 2.1.3)
  - *Network Intrusion Detection Systems* (NIDS) - (cfr. 2.1.3)
  - *IP tunnel endpoint* - IP tunnels are used to create virtual network topologies over an IP network. The first endpoint encapsulates the IP packet into another IP packet so that it gets forwarded to the second endpoint that is then responsible for decapsulating and forwarding the inner packet to its correct destination. These can be used to create Virtual Private Networks (VPNs) which can, for example, be used to connect two corporate networks.
  - *Load balancers* - Load balancers are middleboxes used to split messages across different servers in order for a load of processing and replying to these messages to be balanced between the various servers as possible. Packets sent to the load balancer are redirected to one of the servers in the pool based on some splitting criteria. All packets in a given session must be sent towards the same server for stateful protocols to work correctly.
  - *NA(P)T* - Network Address Translation (NAT) is a technique that was designed as a solution for dealing with the exhaustion of available IPv4 addresses. The idea is to translate private IP addresses that are only valid within a given private network by replacing them with public addresses that can be used on the Internet. If there are fewer public addresses than private addresses available, which is usually the case, TCP/UDP ports are also modified in order for the NAT to unambiguously identify hosts to forward the responses to them. That type of NAT is referred to as NAPT (Network Address and Port Translation).
  - *QoS middleboxes* - Quality Of Service (QoS) for networked applications means guarantees in terms of availability, throughput, etc. QoS techniques consist in prioritizing some traffic over less critical traffic. Packet classifiers classify packets based on policy and can either mark them for differentiated services or select them for special treatment. Schedulers can drop or reorder packets based on priority which is assessed through several means including the marking by classifiers.

- *Involuntary redirection* - Some middleboxes are used to involuntary redirect packets of a certain type. For example, hotels and cyber cafes may be interested in redirecting initial HTTP requests to a page requiring payment.
- *Anonymisers* - Middleboxes can be used to hide the IP address of the sender. Although the implementation may be somewhat different, this is similar to NAT boxes.
- *Proxies* - For various reasons, these middleboxes are used as an intermediate between a client and server. The proxy acts both as client and server in order to perform this task. The client connects to the proxy and the proxy connects to the server.
- *Application-level interceptors* - These middleboxes act as pseudo-proxies. They intercept packets and forward them to another destination, ignoring the actual destination IP address. This can be done with (unencrypted) HTTP traffic to redirect the request to a cache. This behavior is to be avoided with dynamic or non-cacheable content.
- *Application-level multicast* - These replicate application content and send it to multiple destinations. This is of interest for multimedia content.
- *Transcoders* - Transcoders perform on-the-fly conversion of application data into another format.

- *Routers* - The purpose of a router is to forward IP packets towards the correct destination. In order to do so, it must perform two tasks: routing and forwarding. Routing consists in determining the best path to forward packets towards the destination. A given router learns these paths through its participation in routing protocols. Forwarding consists in sending the packets on the correct interface so that they reach the next IP hop on the selected path.

Further Works Choosing an adequate level of granularity in the modeling of communication channels is difficult. One may imagine simple stochastic models where a communication channel is seen as a black box accepting some bandwidth and introducing some delays and errors before outputting the result. The problem with such simple models is that they cannot accurately represent the complexity of communication channels that are used. While such models could be adequate for representing a wire or even a single router, they lack the granularity to represent networks of a larger scale -*e.g.* a corporate network, or some wide-area networks such as the Internet. Indeed, such stochastic modeling of channels would result in discontinuities in the metrics due to rerouting events.

Another abstraction that can be used for modeling networks is the TCP/IP networking stack. While it does not necessarily provide all the answers regarding delays, losses, etc. over a specific network, this is an abstraction that is actually used in every modern networked application and allows to abstract away the physical details of the transmission medium. As reducing complex computer networks to simple models is not satisfactory, it is interesting to only assume an underlying TCP/IP networking stack and rely on simulations for answers regarding delays and other parameters.

Data Storage systems

Memory is one of the fundamental components of a system. Indeed, any computerized system will have at some point to reliably and securely store and retrieve pieces of information for an arbitrary amount of time. To do so, those systems rely on different devices and mechanisms to ensure some guarantees on delays, throughput, etc. Indeed, the queries need to be handled with different guarantees depending on whether they are performed in the context of real-time applications or for performance monitoring. In this section, we will discuss the different types of devices and mechanisms that are involved in the long-term or short-term storage of information as well as key metrics that need to be described in this context.

Physical Memory - Taxonomy Different types of physical devices can be used to reliably store information in a computerized system. However, their usage highly depends on the guarantees they provide on some particular types of metrics and the context they need to be used for. Matching memory types to workload characteristics deliver optimum performance and reliability and each type of memory allows to address the trade-offs between certain characteristics in a way that best fits particular applications. Several performance metrics can be distinguished to discriminate between memory types:

- *Volatility* measures whether or not a storage medium is capable of retaining information after having been disconnected from any power source.

- *Areal density* is a measure of the quantity of information that can be stored on a given area of surface or in a given volume of a storage medium. This metric is of particular importance for the design of space-efficient data storage systems such as data centers, laptops, etc. It is bounded by theoretical limits *-i.e., Bekenstein bound* and by practical noise implications. However, numerous emerging technologies attempt to increase storage densities as it typically also helps in improving the transfer speed at which the medium can operate and reduce the cost-per-bit.
- *Cost* is a basic measure of how much money the storage of a unit of information costs. This metric is of particular importance for the design of cost-efficient and scalable data storage systems.
- *Endurance* is a measure that characterizes the ability of a storage medium to properly store and read pieces of information in time considering its usage and operating conditions - *e.g., temperature, voltage, etc.* It is generally expressed as a combination of an average number of write/erase cycles and life expectancy in nominal operating conditions.
- *Data retention* is a measure that characterizes the capability of a storage medium to retain information that has been stored. It is highly dependent on the usage, operating conditions as well as endurance of the storage medium that is being considered.
- *Access time* is a measure of how long it takes to store or retrieve some pieces of information in a storage medium.
- *Energy consumption* is a measure of the quantity of energy that is consumed by the storage medium to perform its routine tasks - *e.g., write/read requests, data retention, etc.*
- *Nominal operating condition* is a description of the operating condition at which the storage medium will be able to provide its optimal performance in terms of data retention, endurance, energy consumption, and access time. It is generally specifying some ranges in temperature and voltage but can also provide more specific details on radiation performance, shock resistance, etc.

Considering those metrics, memory types can be classified according to how they are used by computer systems. Internal Memory is used for direct and fast access and is embedded into the computer systems. Generally, they do not aim at maintaining information for a long period of time. In this context, volatile memories such as those based on semiconductor chips are often used for this purpose. Random Access Memory (RAM) which temporarily stores data while the Central Processing Unit (CPU) is executing other tasks is a very good example of such type of memory. There are two main types of RAM: **(1)** Dynamic RAM (DRAM) in which memory cells are designed in such a way they need to be periodically refreshed every few milliseconds to retain data, and **(2)** Static RAM (SRAM) that can maintain data as long as power is supplied without needing to refresh it periodically. As such, SRAM is faster but also more expensive, making DRAM the most prevalent memory in computer systems. In this context, several technologies are used to enable DRAMs with various data transfer capabilities. Synchronous DRAM (SDRAM) allows data transfer at up to 133MHz while Rambus DRAM (RDRAM) that was very popular in the early 2000s enabled transfer at up to 1GHz. However, the most common technology used in recent computer systems is the Double Data Rate SDRAM (DDR SDRAM) which extends the SDRAM and nearly doubles the bandwidth of a single data rate by enabling to transfer of data on both the rising and the falling edge of the CPU clock signal. There are several generations of DDR SDRAM, each delivering higher transfer rates and faster performance. The latest DDR4 modules, for example, feature fast transfer rates at 2133/2400/2666 and even 3200 MT/s. There are also internal memories that need to maintain unchanged information for very long periods of time while keeping the same guarantees on performance. Such types of memories are called Read-Only Memories (ROMs) and they are mainly used to store programs essentials for basic input/output systems (BIOS), booting, reading and writing to peripheral devices, basic data management, and the software for basic processes for certain utilities.

Then, External Memory refers to storage devices that can retain or store data persistently and can either be embedded in the computer system or totally removable. They generally aim at providing a good ratio between cost-per-bit and aerial density with data transfer speed being much lower than RAM and ROM technologies. Non-volatile memories such as Hard-Disk Drives (HDDs) and Solid-State Drives (SSDs) are good candidates for such usage. HDDs are made of one or more spinning platters on which data is stored. The platters are protected within a sealed casing, along with other components such as the magnetic heads that read the data. On the other hand, SSDs include no moving parts and instead rely on interconnected silicon chips to store data resulting in much higher performance, aerial density, and energy consumption. Currently, most SSDs medium relies on NAND flash technologies as they allow much higher densities compared to NOR flash technologies and lower cost per bit. While it is quite an obsolete technology, magnetic tapes are still being used by some organizations

mostly for backup and archiving purposes. Magnetic tapes are neither fast nor efficient in terms of energy consumption, data retention, endurance, or access time but their relatively low price and some old habits tend to attract some companies. Other types of external memories exist such as Ferroelectric RAM (F-RAM) that allows very high performance for storing rapidly changing data over long periods of time.

Logical Memory - Storage Configurations While typical day-to-day users are not often experiencing scalability issues when storing personal information, modern storage infrastructures face demands for always increasing scale and efficiency. In this context, mechanisms for efficiently combining several physical memories have emerged with an ever-growing complexity in ensuring the quality of service, maintainability, and resource fairness, raising unprecedented performance, scalability, and programmability challenges. Despite the various options, many data centers continue to rely on three traditional configurations: **(1)** Direct-Attached Storage (DAS), Network-Attached Storage (NAS), and the Storage Area Network (SAN).

DAS is the most common type of storage configuration experienced by users of computerized systems. In this configuration, the storage mediums *-i.e.,* HDDs, SSDs, etc - are attached directly to the computer system via a non-networked link. DAS is a fairly basic, low-maintenance, low-cost configuration that is used by many IT infrastructures as larger DAS storage units can accommodate multiple disks in one enclosure. DAS connects to a computer system via an interface such as Serial-Attached SCSI (SAS), Serial Advanced Technology Attachment (SATA), Small Computer System Interface (SCSI), or Peripheral Component Internet Express (PCIe). While DAS can be used in hyper-scale systems such as Apache Hadoop or Apache Kafka to support large, data-intensive workloads, its ability to grow and scale is very limited as computer systems can support only a relatively small number of expansion slots or external ports. In addition to that, the configuration is not meant to support a lot of system users and activities at once nor for long-distance sharing. NAS better fits this kind of usage as it offers dedicated centralized file serving and sharing through a network with increased performance and reliability. Indeed, features like Redundant Array of Independent Disks (RAID) and swappable drives enable higher multi-drive workloads.

NAS is a file-level storage technology, which provides file-based data storing services to multiple devices on a network via a single, scalable, and relatively easy to set-up access point. It includes built-in fault tolerance, management capabilities, and security protections, and it can support features such as replication and data deduplication. A NAS device is an independent node on the local area network (LAN) with its own IP address. It is essentially a server that contains multiple HDDs or SSDs, along with processor and memory resources. The device typically runs a lightweight operating system (OS) that manages data storage and file sharing, although in some cases it might run a full OS such as Windows Server or Linux. Users and applications connect to a NAS device over a TCP/IP network. To facilitate data transport, NAS also employs a file transfer protocol. Some of the more common protocols are Network File System (NFS), Common Internet File System (CIFS), and Server Message Block (SMB). However, a NAS device might also support Inter-network Packet Exchange (IPX), NetBIOS Extended User Interface (NetBEUI), Apple Filing Protocol (AFP), Gigabit Ethernet (GigE), or one of several others. However, NAS devices must compete with other traffic on the devices

For increased scalability and additional management features, one might consider SAN technology using a dedicated, high-speed network that interconnects one or more storage systems. Indeed, SAN enables a logical view of these combined storage systems so that the users see them as if they were a pool of block-level storage resources. SAN also enables multiple application servers for managing data access, storage management software, host bus adapters (HBAs) to connect to the dedicated network, and many other physical components such as high-speed cabling and special switches for routing traffic. SAN storage arrays can be made up of HDDs or SSDs or a combination of both in hybrid configurations. A SAN might also include one or more tape drives or optical drives. The management software consolidates the different storage devices into a unified resource pool, which enables each server to access the devices as though they were directly connected to that server. With the right network topology and internal configuration in place, a SAN can deliver a block-level storage solution that offers high availability and scalability, possibly even high performance. A SAN includes centralized management, failover protection, and disaster recovery, and it can improve storage resource utilization. Then, SAN architectures aim at reducing contention in LANs as it runs on a dedicated network. However, a SAN is a complex environment that can be difficult to deploy and maintain, often requiring professionals with specialized skill sets. As a consequence, many of the SAN configurations results in low transfer speed and a lot of misconfiguration. Indeed, common SAN problems include compatibility issues, hardware failures, and sluggish storage response times.

In addition to those traditional storage configurations, organizations can also take advantage of cloud storage, object storage, or software-defined storage that might be provided by third parties such as Amazon, Microsoft,

etc. However, storing information in external infrastructures might lead to legal issues, especially for sensitive federal information.

Time Synchronization systems

Another key component that needs to be considered when looking at computerized systems is time. Indeed, issues arise when distributed applications need to keep track of time. As they are made up of remote components that all manage their own independent clocks, it is certain that without any synchronization mechanism, the timelines they keep track of will not be identical. Even if they are all synchronized at a given point in time, a clock drift phenomenon will be observed in the long run as they do not work at the exact same rate.

On the other hand, many devices in a power system require a shared logical clock. As such, several solutions are available but communication delays make this problem difficult for geographically widespread systems. In a power systems context, criteria for the accuracy of the shared clock are more stringent than in other distributed applications. In this context, two solutions can be considered for the use in modern or legacy substations where devices such as synchro-phasors require accuracy at the microsecond level.

Global Positioning System (GPS) GPS offers a reliable way for a set of entities to establish a precise shared time without any need for communication among themselves. This is achieved by attaching each entity to a GPS antenna which can receive positions and timestamps from a set of at least four satellites orbiting the Earth. With this information, the antenna can determine its precise position in space and time. [21] The time spent communicating with the antenna is negligible as the propagation delays with a direct connection are extremely small. GPS time is accurate up to the microsecond. However, the deduplication of GPS antennas (even with the possible use of a shared bus for the output signals of GPS antennas) is not always a satisfactory solution. For instance, within a substation, devices are already connected over Ethernet. Avoiding the necessity for a multitude of antennas or additional buses is preferable. Solutions such as the Network Time Protocol (NTP) allow for the establishment of a shared clock over the network. NTP however is only accurate up to the second which is unsatisfactory. [22]

Precision Time Protocol (PTP) - IEC61588 PTP, also referred to as IEC61588, allows for the establishment of a shared clock over the network with an accuracy up to the microsecond, which combines the convenience of NTP with the accuracy required for power systems. Here, the main idea is that a master clock communicates timestamps to the other devices. Then, precise synchronization is achieved as the slaves attempt to correct the timestamps sent over the network by the master clock so that it takes into account the dynamic delays involved by the networked communications.

Security Systems

The components that have been presented in previous sections all integrate, in some ways, some mechanisms and/or some pieces of hardware to enable some security and safety properties in the system. However, some components can also be dedicated to ensuring the secure operation of the cyber-part of the cyber-physical power grid. In contrast with orchestration systems, security systems are not strictly necessary to operate the physical components. However, they participate in ensuring minimum guarantees on some particular metrics [2] in particular situations such as spontaneous failures, attacks, natural disasters, etc. In this section, components -*i.e.* mechanisms, algorithms, applications, etc - that participate in ensuring guarantees such as those mentioned in the so-called CIA triad -*i.e.,* Confidentiality, Integrity, Availability - are presented.

Firewalls Firewalls are devices that are placed at a strategic place of the network, typically at its entry point (interconnection with some other network). Firewalls observe the network packets that go through them and only transmit them towards their receiver if the communication is allowed according to the firewall's rules. Packets that are not allowed are simply discarded [23].

Simple firewalls may just use basic information, such as source address, source TCP/UDP port, destination address, destination TCP/UDP port, to decide whether to forward or to drop a given packet. Such a very simple firewall can already be pretty useful to block traffic caused by the undesired application. Indeed, the Internet Assigned Numbers Authority (IANA) standardized the destination ports that should be used by particular applications. Therefore, the destination ports can typically be used to identify a single application layer protocol and block a lot of undesired traffic with simple rules [23].

On the other hand, smarter firewalls might also act in a stateful fashion by keeping track of end-to-end connections and acting with more complex rules. Here, the advantage is that it is possible to discriminate between inbound/outbound connections -*i.e.,* from the outside/inside to the inside/outside of the network. Modern firewalls can also perform Deep Packet Inspection (DPI) by treating the packet content to check if it corresponds to regular traffic that should be accepted in the network [24]. Research is still ongoing to enable DPI in the context of encrypted traffic.

Intrusion detection systems (IDS) IDS refers to a collection of devices and/or pieces of software designed to detect that a network intrusion has occurred - *i.e.,* malicious activity or policy violation. This is not to be mixed with the behavior of a firewall. While firewalls prevent intrusions, IDSs try to report them when they have already occurred. Typical IDS are made up of one or several sensors as well as a manager. The manager decides whether an alarm needs to be raised to the operator depending on the information coming from the sensors [23].

IDS enables the system to detect a wide range of well-known attacks or unauthorized actions from legitimate users to attackers. Several techniques can be used to perform intrusion detection. Firewalls can be configured with explicit rules that should trigger an alarm while some other IDS devices can run DPI algorithms to check traffic content against a database of attack signatures [23].

Cryptography Cryptographic techniques are often used to ensure the Confidentiality and Integrity properties of the CIA triad. As mentioned in Chapter 4, encryption algorithms are very common to enable confidentiality within a system while hashes allow enabling some kind of integrity check. Whether those algorithms are run on specific pieces of hardware or in software highly depends on the application that is considered and the performance that needs to be ensured. For instance, Internet of Things (IoT) devices are not often equipped with hardware circuits enabling to perform encryption in hardware while more expensive cyber devices are often equipped with circuits enabling fast CRC checks for integrity checks.

Authentication servers Authentication consists in assessing the identity of a system user. Whether the user is remotely or physically connected to the components that need to be accessed is not of particular interest as both require the use of an authentication protocol that typically relies on cryptographic techniques, biometric information, etc. The authentication mechanisms can either be done by a dedicated authentication server whose sole purpose is to provide user authentication to the other system components or could be done through embedded mechanisms. The advantage of centralizing authentication is to avoid configuring user accounts in many different system components.

Interfacing Systems

Modern cyber-infrastructures tend to integrate more and more automated control and monitoring of their components. However, human operators are still in charge of ensuring the overall correct operation of the system. In this context, Human-Machine Interfaces (HMIs) enable the human operators to manage and interact with the cyber-components through computer-based Graphical User Interface (GUI) [18]. HMIs can be found at several levels with some cyber-components that embeds some HMIs capabilities. On the other hand, modern control centers rely on GUI spread across three or four screens per given operator which allows the human operator to monitor several parts of the system simultaneously [18]. Audible alarms can also be used to draw the attention of the nearby operators to some detected anomaly or important information while printers and fax can be very helpful in keeping track of raised alarms and events. Moreover, control centers are often equipped with a mimic diagram that allows them to have a global view of the entire system [18].

Two kinds of HMIs software can be found in industrial facilities: **(1)** supervisory level, and **(2)** machinery level [13]. The supervisory level is designed for a control room environment and used for System Control and Data Acquisition (SCADA), a process control application that collects data from sensors on the shop floor and sends the information to a central computer for processing (cfr. Section 2.1.5). Then, machine-level HMIs attempts to use embedded, machine-level devices within the production facility itself. Selecting HMIs software requires an analysis of product specifications and features. Important considerations include system architectures, standards, and platforms; ease of implementation, administration, and use; performance, scalability, and integration; and total costs and pricing.

2.1.4 Cyber-Space Handling of Field Equipments

The power grid can be seen as a cyber-physical system in which the cyber and physical parts of the system are coupled to provide critical services. In this context, the field equipment representing the devices that allow the direct monitoring and control of the physical infrastructure are handled through cyber-components by the control centers, human operators, or automated control systems. This section aims at describing the cyber-components that lie at the border between the physical and the cyber-space as well as their general interaction with the rest of the system.

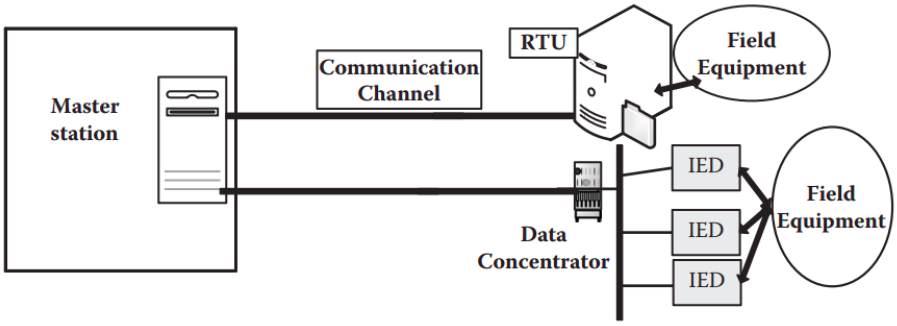

Figure 2.2: Typical orchestration of field devices [18]

Figure 2.2 attempts to represent the main cyber components that are involved in the handling of field equipment as well as the mechanism through which they communicate.

Field Equipment

Field equipment consists of devices through which the operators can directly monitor and control the state of the physical infrastructure. These devices belong to the edge of the physical space and are directly communicating with devices of the cyber-space to forward metering information to the control centers and the automated control systems or to receive control signals from these entities. Often proprietary and analog, they may be controlled differently depending on the context. Most often, they receive instructions from the control center or automated control systems through some network-enabled devices to which they are connected using specific protocols. In other cases, they may be directly controlled by human operators manually or through Human-Machine Interfaces.

Examples Devices belonging to this class of components are various depending on whether the focus is on the generation, transmission, distribution part of the system. In generation systems, the field equipment will be actuators that allow to increase/decrease the fuel supply or sensors measuring the pressure in the steam system, etc. In transmission systems, field devices will be switchgear, transformers, phasor measurements units (PMUs), etc. Those devices may be found at strategic places such as substations which often lie at the intersection of multiple transmission lines. In distribution systems, field devices may also be transformers, switchgear, etc, but new types of devices are becoming more and more common such as smart meters, charging stations, etc, bringing new challenges to the cyber-layer that handles those devices.

Remote Terminal Units

The Remote Terminal Units (RTUs) are devices that are mainly used for wider geographical telemetry and control of the field equipment. Most often, RTUs are not meant to execute control loops and control algorithms but more to interface with remote master stations for directly/indirectly relaying monitoring information and control signals from/to field equipment. They are mostly meant to perform simple data collection tasks with very small amounts of computations and execute the instructions provided by master stations or intelligent electronic devices (IEDs). This involves small translation tasks to ensure that the targeted field equipment receives valid instructions. However, modern RTUs typically support the `IEC 61131-3` programming standard for Programmable Logic Controllers (PLCs) that allows them to execute small process control units such as PID, Alarming, Filtering, Trending, etc.

Examples Devices belonging to this class of components are various depending on the manufacturer, the connectivity, and the capabilities needed. The main manufacturers are ABB, GE Grid Solutions, Honeywell, Schneider Electric, Siemens, etc. On the other hand, RTUs might be interfaced by multiple master stations and intelligent electronic devices (IEDs) with different communication protocols-*i.e.* serial RS232, RS485 or RS422, Ethernet, Modbus, `IEC 60870-5-101/103/104`, DNP3, `IEC 60870-6-ICCP`, etc (cfr. Section 2.1.5).

Intelligent Electronic Devices (IEDs)

The Intelligent Electronic Devices (IEDs), also called Remote Telemetry Units[4], refers to devices that enable more intelligent control and monitoring functions thanks to their higher computing power. Instead of only relaying control signals sent by the control center, they can also perform advanced automatic control functions using control loops and algorithms and can be interfaced with many different other devices. Furthermore, they can also offer many additional services such as waveform capturing, disturbance analyzing, or accurate voltage measurements. While some IEDs might directly operate with the master station through RTUs or direct communication channels, it is more common than they are interfaced using an intermediate device, called a Data concentrators (DCs) [18]. Indeed, they allow addressing the problem of interoperability between IEDs from various manufacturers in `IEC61850` systems as well as the partitioning of the network architecture to minimize networks loads and the impact of network failures [25]. In addition to that, IEDs often need to communicate with each other to perform advanced control and monitoring functions. Therefore, DCs allow faster horizontal communication between that equipment. Regarding their interface with the field equipment, IEDs are usually making use of Merging Units (MUs) which allows the conversion of field equipment outputs to standardized Ethernet-based outputs and that enables the implementation of `IEC 61850`. Merging units perform the processing necessary to produce a precise, time-aligned output data stream of sampled values according to the `IEC 61850-9-2` standard.

Programmable Logic Controllers (PLC) Programmable Logic Controllers (PLC) are industrial-grade computers that are capable of being programmed to perform more or less complex control functions. Initially, PLCs were designed to replace relay logic, but its ever-increasing range of functions means that it is found in many and more complex applications making it a perfect candidate to fit the role of an IED. PLCs are designed for multiple input and output arrangements, extended temperature ranges, immunity to electrical noise, and resistance to vibration and impact. Then, they often provide fast response, easy programming and installation, high-control speed, network compatibility, troubleshooting, and testing convenience as well as high reliability. Programs for the control and operation of manufacturing process equipment and machinery are typically stored in battery-backed or nonvolatile memory. Particularly, PLCs fit applications needing real-time guarantees with bounded response time.

Examples Devices belonging to this class of components are usually performing protection functions. For instance, they can offer automatic capacitor bank switching functionalities to maintain the desired system voltage levels as reactive loads are connected and disconnected to the grid. Protective IED relays will activate the appropriate control function if a meter is above or below the desired threshold. Then, the control function will engage what it needs to correct the problem -*i.e.,* raising voltage levels or tripping circuit breakers- and return the value to the appropriate range. IEDs may be allowed to perform complex signals analysis to allow advanced network alarm monitoring services.

Further Works The relevant tasks that are performed by this class of components need to be identified and modeled. The modeling of such tasks includes the analysis of computation times, failure modes, and prediction accuracies.

Electrical Substations

An electrical substation is a subsidiary station of an electricity generation, transmission, and distribution system where important control and monitoring operations are performed such as voltage transformation, line breaking, etc. Typically, substations gather many cyber components involved in the direct handling of the field devices. In a modern substation, many more tasks are automated. The introduction of IEDs allows for these improvements via the exchange of information inside of the substation in-between IEDs.

[4]The term IED has been introduced partly because of the confusion between Remote Telemetry Units, with the acronym (RTU) and Remote Terminal Units, also with the acronym RTU.

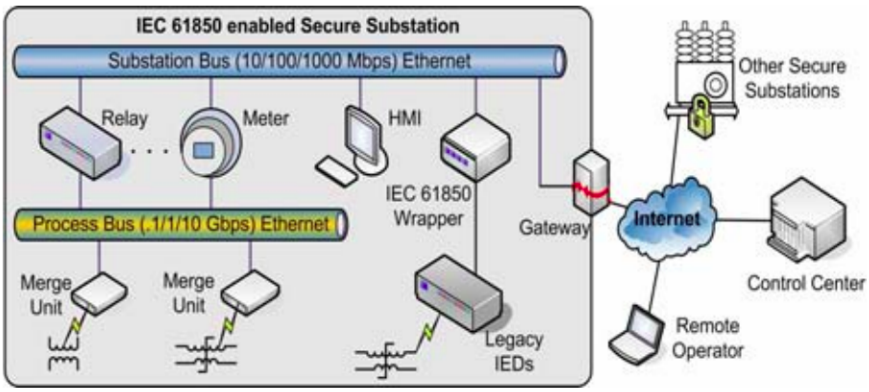

Figure 2.3: Architecture of an IEC61850 substation [26]

The IEC61850 is an international standard defining communication protocols for intelligent electronic devices at electrical substations. In IEC61850, substations are organized around 2 levels of buses that connect IEDs and the substations' gateway. Then, IEDs can use this bus to exchange information among themselves and to communicate with remote control centers [26], [27]. While only one substation bus is used in a substation, there may be many process buses. Indeed, process buses are used to connect the "dumb" devices to the IEDs and there is often, one process bus per bay *-i.e.,* a circuit breaker and its associated equipment such as switches and protection equipment [26]. Both process and substation buses are Ethernet buses. Process buses should have high bandwidth *-e.g., 100 Mbps* - while substation buses can have much lower bandwidth *-e.g., 10 Mbps* - [26].

The IEC61850 standard also defines several protocols that are used in different contexts within the substation. For instance, the Generic Object Oriented Substation Events (GOOSE), and Sampled Values (SV) protocols allow to send messages directly over Ethernet on the buses and that can provide very strict delay guarantees *-e.g., < 4ms*. GOOSE messages are used to exchange various substation events such as alarms and commands, while SV is used for the exchange of sampled measurements. GOOSE and SV messages are strictly limited to communication inside of the substation [27] [26]. Another central protocol specified in the standard is Abstract Communication Service Interface (ACSI) protocol. It can be used in an application-server configuration and is somewhat similar to a more classic master-slave configuration. However, it allows the application (analog to the slave) to initiate the two-way conversation. Then, ACSI defines a standard way to access information about a device with each IED being divided into logical nodes defined by functionalities [27]. IEDs can then act as servers to request data or action from other IEDs. ACSI can also be used for communication between IEDs and the control center using Manufacturing Message Specification (MMS) over TCP [27].

2.1.5 Orchestration System

As depicted in the sections above, cyber-physical systems are composed of a very large panel of heterogeneous cyber-devices each sending/receiving particular information complying with some specific protocols. In this context, the orchestration system is responsible for ensuring a cohesive, and synchronized functioning of all those devices to ensure the supervision of systems with many varying processes. In cyber-physical power systems, the orchestration systems found at transmission and generation and distribution are typically centralized so that they can be operated in control centers offering a global view of the system to human operators. They provide automated configuration, coordination, and management of complex computing networks, systems, and services. In contrast, the load part of the systems is often acting autonomously with small-scale, distributed generation and load [18].

Process Control Systems (PCS) Process control systems, sometimes called industrial control systems (ICS), refers to a wide range of control systems and associated instrumentation, which include the devices, systems, networks, and controls used to operate and/or automate cyber-physical processes. Depending on the industry, each ICS functions differently and is built to electronically manage tasks efficiently. Today the devices and protocols used in an ICS are used in nearly every industrial sector and critical infrastructures such as the manufacturing, transportation, energy, and water treatment industries.

Supervisory Control and Data Acquisition (SCADA)

Centralized orchestration systems are meant to gather and present data such as metering information and alarms to operators in a centralized fashion. Indeed, the information will be retrieved and gathered in one or several control centers so that the operators located at this control center can take actions or other decisions such as retrieving more metering information on processes in the corresponding cyber-physical systems. In this context, the centralized orchestration system is responsible for coordinating the devices in the system so that the decisions are taken by the operators in the control center -*i.e.,* measurements, actuation, etc - are correctly executed with some guarantees on delays, accuracy, etc.

SCADA is a PCS that perfectly fits this role of providing control at the supervisory level to operators in a control center. Indeed, SCADA is a system that is composed of devices such as PLCs or other commercial hardware modules, that are distributed in various locations and that provide centralized monitoring and control for numerous process inputs and outputs. The primary purpose of using SCADA is for long-distance monitoring and control of field sites through a centralized control system. Instead of workers having to travel long distances to perform tasks or gather data, a SCADA system can automate this task. Field devices control local operations such as opening or closing valves and breakers, collecting data from the sensor systems, and monitoring the local environment for alarm conditions.

Decentralized Control Systems (DCS)

Decentralized orchestration systems are meant to control production systems that are found in one location. DCS is another type of PCS that allows the safe and efficient management of multiple local controllers or devices to enable more complex control functions to the system while often providing more guarantees on safety and reliability than SCADA. To do so, DCS uses a centralized supervisory control loop to manage the multiple local controllers or devices. However, implementing a PCS environment is often made from a hybrid configuration of DCS and SCADA wherein attributes from both systems are incorporated.

2.2 Cyber-space as Services: a top-down approach

The cyber-space constitutes a major part of the power grid architecture as it ensures the secure relay of control and metering information between several entities in the system. In addition to that, it also takes part in the decision-making process as it can issue control and metering commands spontaneously and impact the operator's decisions. The advent of cyberspace capabilities enabled smarter and more efficient control of the operational environment. However, this comes at the cost of an exponentially increasing complexity in the sequence of events happening both in the cyber-space and the physical space. This section aims at mitigating the complexity of the chain of events happening in the cyber-space by presenting an abstraction of the services provided by the cyber-layer to the physical infrastructure. In the spirit of the famous *divide and conquer* approach, this abstraction may allow us to identify threats and vulnerabilities on some parts of the system without having to consider every single layer of the software and hardware stack of other parts of the cyber-space.

2.2.1 Modelling Principle

Considering the very large, heterogeneous, and dynamic cyber-space operating the power grid, the attack surface that needs to be considered is constantly evolving and becoming more and more complex with a huge number of devices and processes interacting with each other very fast dynamics. However, the system-wide consequences of several attack scenarios are very similar and many different threats can be handled using more generic countermeasures. For instance, a terrorist attack and a network flooding attack on a data center will both result in the denial of access to the services provided by this data center. On the other hand, redundancies allow mitigating the impact of such scenarios. In this context, the approach presented in this section attempts to provide an exhaustive model of the services provided by the cyber-layer to the physical infrastructure as well as examples of the individual components -*i.e.,* devices, software stacks, etc.- that enable those services. The approach, inspired by the OSI approach in computer networking, is referred to as Cyber-space as Services (CSaS) as its fundamental principle consists in defining a higher level class of services based on the functionalities they provide to the system.

Example From a physical and cyber-security point of view, wireless communications are very different from communications over a wire. Indeed, threats to both media are not identical. For instance, wireless communications can be disrupted via electromagnetic interferences while wires can get cut. However, from a purely

functional standpoint, the scenarios are very similar as they both result in the unavailability of the communication medium. In the context of a risk assessment approach on a very large and complex system, abstracting these details away is not only useful but necessary as it helps build models of reasonable complexity.

Hierarchy of services

As illustrated in Figure 2.4, the services provided by the cyber-space can be organized in three layers: **(1)** the application services that represent the components that are directly used by the operators, the IEDs, etc and that allows them to interact with the physical infrastructure without having to take care of low-level cyber-mechanisms, **(2)** the operational services that represent the layer at which monitoring and control commands are being sent/received by the components in the system and, **(3)** the utility services that enable the other services through the low-level functionalities they provide to the cyber-part of the system.

The rationale for this subdivision may appear natural as it allows to distinguish between the end-functionalities through which the operators directly manage the state of the physical infrastructure, from the functionalities that may not be directly available/useful to the user but that are crucial to the overall cyber-physical system.

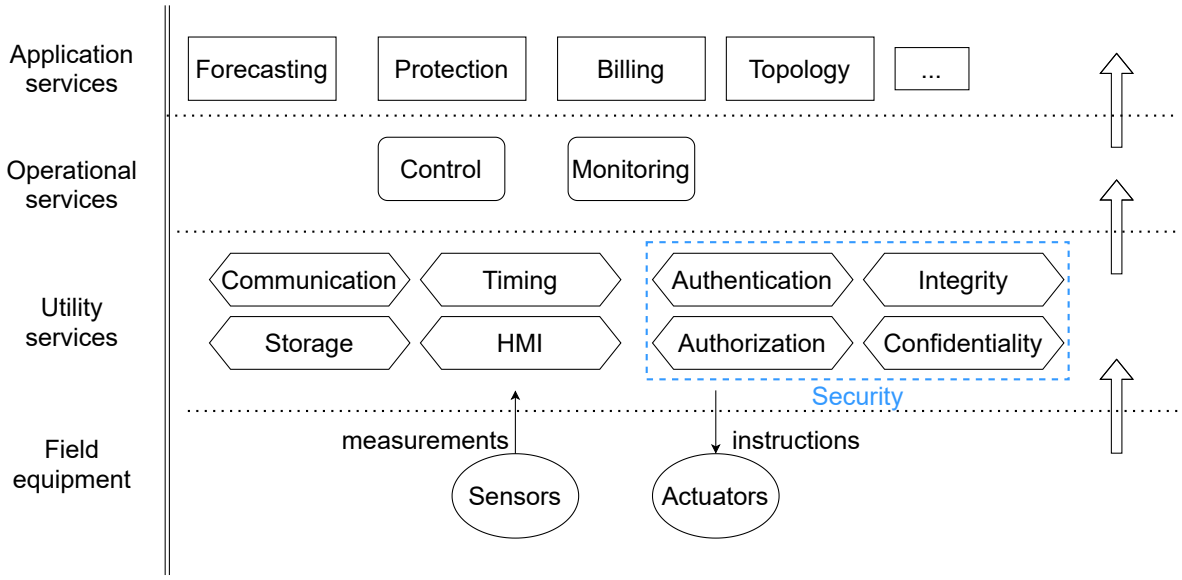

Figure 2.4: Cyber-space as services model

Example An example of application services that are widely used for managing power grid are Energy Management Systems (EMS). EMS comprises a system of computer-aided tools that allows the intelligent monitoring, control, and optimization of electric utility grids. In this context, EMS tools perform complex automation, management, and forecasting tasks such as economic dispatch of generation units, reserve management, and load forecasting in transmission systems.

To perform those tasks, EMSs often rely on SCADA systems to send their monitoring and control commands to the field equipment efficiently and securely. Similarly, SCADA systems also rely on some lower-level services to enable their functionalities to the overall cyber-physical system. The SCADA often uses `DNP3` or `IEC 61850` communication protocols for the interaction between control centers, RTUs, IEDs, etc which in turn, make use of lower-level communication protocols such as TCP/IP, UDP, etc. In parallel, the EMS also often makes use of historical data for performing its forecasting tasks. However, those data sets need to be securely and efficiently stored and timestamped using some cyber components and mechanisms.

2.2.2 Application Services

The Application layer represents the highest level class of services that the cyber-part can provide to the overall system. The application services comprise the end applications that the operators will use to remotely/physically manage the state of the power grid but also the applications that the IEDs/PLCs will run to perform their tasks inside sub-stations. This is the part where the intelligence of the cyber-physical power grid resides. It al-

lows the system to autonomously react to changes in its physical infrastructure but also provide raw/processed data to the different actors and advice based on forecasting and simulations to the operators.

Those services extensively rely on the use of lower-level services such as operational services that enable to query information directly from field devices or send control commands to those devices through SCADA. However, the applications might also use external sources of information to enable more specific functionalities.

Examples The services provided by this layer are mostly enabled by software components that interact or not with each other to perform their tasks. Application services can be the Substation Automation Systems (SAS) providing the software components that enable the operators to manage substation remotely/physically. They also comprise Distribution Management Systems (DMS) that are software applications enabling the handling of peaks demands, the continuous electrical topology processing of the distribution system, fault isolation, and restoration tasks, etc. More importantly, Power Management Systems (PMS) software tools also belong to this class of services. PMS run applications enable the system to determine the appropriate system response to a variety of changes and disturbances by using electrical and physical parameters, loading and generation levels, network topology, and control logic.

Further Works The software components belonging to this class of components need to be identified and modeled to be able to perform any simulations. Indeed, those components will partly define how the systems will react to a change in the physical state of the grid. Their response to modification in the state of the grid needs to be further studied.

2.2.3 Operational Services

The operational services represent the mid-level class of services provided by the cyber layer to the overall system. They comprise the systems made of software and hardware elements that allow the real-time remote/physical operation of the field equipment with guarantees on the safety and security of operations. At this layer, the report of the status of different systems in the substations is enabled as well as the control of operations in substations such as tripping of circuit breakers and tap adjustment for voltage regulation. All in all, the operational layer of services provides two fundamental mechanisms to the system which are monitoring and control of the power grid's state.

Examples The operational services are mainly provided by SCADA components. The SCADA uses lower-level services to relay the control commands and the monitoring data from the masters that decide for the systems to the field equipment that apply those decisions.

2.2.4 Utility Services

The utility services are the lowest class of services provided by the cyber-layer to the system. They represent the building blocks of the cyber-space that will directly/indirectly enable any of the functionalities in the higher class of services. The components belonging to utility services may either be hardware or software elements and maybe enable several functionalities at a time. For instance, communication media enable the communication service in the system but are also involved in the storage service in the context of distributed storage systems.

All in all, the utility services can be broken down into an exhaustive list of sub-services that together enables all the higher layer functionalities in the system:

- *Communication Services*: The components belonging to this class of utility services allow entities in the system to transmit/receive instructions and information through time. This service often relies on a stack of networking protocols to operate (cfr. Section 2.1.3).
- *Storage Services* The components belonging to this class of utility services allow entities in the system to store information on events that have been detected in the system. This service often relies on distributed systems theory to enable efficient and correct management of data (cfr. Section 2.1.3).
- *Timing Services* The components belonging to this class of utility services allows the system to track the time of occurrence of events happening in the system and maintain a coherent and consistent view on the timetable of those events (cfr. Section 2.1.3).

- *Security Services* The components belonging to this class of utility services allow enforcing guarantees on relevant security properties that must be satisfied by the instructions and information in the system. They involved cryptographic techniques, access control mechanisms, etc. Security services may be further decomposed into 3 main sub-services: **(1)** Integrity Services that enable to track any modification of a piece of information (*e.g., instructions, code, data, etc*), **(2)** Authentication Services that enable to identify the source of any information, **(3)** Authorization Services that restrict access to information to authorized entities and, **(4)** Confidentiality Services that enable to ensure the non-disclosure of information/instruction.
- *HMI Service* The components belonging to this class of utility services allow the interaction between physical operators and the cyber ecosystem (cfr. Section 2.1.3).

Further Works The devices and software components that belong to this class of services should be explicitly modeled using the appropriate level of abstraction. For instance, modeling all the links of the communication networks in substations might be relevant while it may not scale to the overall system.

3

Cyber-Risks & Threats & Vulnerabilities

The very heterogeneous and complex nature of modern cyber-physical infrastructures implies a wide variety of new threats and vulnerabilities that can compromise the integrity of the overall system. These threats can target different aspects ranging from purely cyber-related vulnerabilities to the safety of the system as a whole. More specifically, assessing threats in cyber-physical power systems such as the smart grid requires a new strategic view of and planning for the whole lifecycle of the system.

This chapter aims at presenting several threat modeling methodologies as well as quantifying their performance in the context of cyber-physical power systems. Then, the chapter will describe some tools that can be used to rigorously describe threats scenarios that could result in a state preventing the cyber-physical power grid from functioning properly. Finally, some preliminary work on vulnerabilities modeling methodologies will be presented.

3.1 Threat Modelling Methodology

Threat modeling is a risk-based approach that aims at designing secure systems. Particularly, it involves a process by which potential threats, such as structural vulnerabilities or the absence of appropriate safeguards, can be identified, enumerated, and mitigation strategies can be prioritized. In this section, a protocol to unveil the threat surface of the cyber-physical power grid, as well as an associated set of contingency scenarios, will be presented. The approach is a combination of state-of-the-art considerations as well as novel techniques to enable the description of an exhaustive set of cyber-physical threats that may harm the power grid.

First, the traditional approach making use of a state-of-the-art and well-established cyber-threat categorization called STRIDE will be depicted. STRIDE mainly provides a taxonomy to describe an exhaustive set of cyber-attack families and looks into how these families can be refined into specific attacks on the assets of the system. Most often, STRIDE is used in conjunction with a model of the target system including a full breakdown of

processes, data stores, data flows, and trust boundaries.

Then, the flaws of such categorization will be explained, and a novel cyber-physical threat categorization methodology will be described to circumvent these shortcomings.

3.1.1 Key Concepts & Terminology

A variety of terms are used in threat modeling including threat, threat scenarios, threat vectors, attacks, vulnerabilities, etc. Unfortunately, the literature often refers to these terms with varying definitions according to the assumptions on the contexts and purposes for which they will be used. This section aims at defining the key terms that will be used throughout this chapter[1]. Let us define,

- Cyber-Threats represent any circumstance or event with the potential to impact organizational operations, organizational assets, individuals, other organizations, or the nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
- Threat Events are events or situations that have the potential for causing undesirable consequences or impact.
- Threat Scenarios are a set of discrete threat events, associated with means and a specific threat source or multiple threat sources, partially ordered in time.
- Means refer to an agent, tool, device, measure, plan, or policy for accomplishing or furthering a purpose.
- Threat Source/Threat Agent/Vectors refer to the intent and methods targeted at the intentional exploitation of a vulnerability or a situation as well as methods that may accidentally trigger a vulnerability.
- Vulnerabilities refer to weaknesses in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
- Cyber-Attack refer to any deliberate efforts to disrupt, disable, destroy, or maliciously control a computing environment/infrastructure; or steal, alter, or destroy data stored on the IT infrastructure.

3.1.2 General Considerations

After having determined components of modern electricity infrastructure, determining threats facing these components and their communication interfaces is the second step of any conceptual threat modeling methodology. Also, the determination of possible threat actors who might achieve these threats will make it easier to conceptualize threat vectors. This information also adds value for determining motivation and willingness behind any possible attack. In this section, possible threats facing major components of electricity infrastructure will be discussed first using threat categorization methodology called STRIDE, then using the novel methodology presented in Chapter 2 called CSaS. The former methodology declines a general, predefined, and fixed family of attacks that needs to be applied to the assets of the system while the latter is only concerned with how those assets enable high-level functionalities to the system.

The National Institute of Standards and Technology (NIST) defines the risk management process as a sequential procedure involving the identification, the assessment, and the response to risk [28]. In this context, NIST provides a framework that provides a common language for understanding, managing, and expressing cybersecurity risk to internal and external stakeholders. It can be used to help identifying and prioritizing actions for reducing cybersecurity risk, and it is a tool for aligning policy, business, and technological approaches for managing that risk. It can be used to manage cybersecurity risk across entire organizations or it can be focused on the delivery of critical services within an organization.

Inspired by this framework, the MITRE organization attempted to provide many pragmatic considerations on which the risk management methodology that will be presented in this section is based [29].

Finally, [30] gave us insight into the motivation and skill of threat actors that would need to be considered in the context of the cyber-physical power grid.

Table 3.1 provides a general overview of the complete 4-step process for risk assessment, inspired by a standard such as NIST 7168 [31], RAND CT490 [30] and MITRE [29], that will be described in further sections. Step 1 aims at identifying the actors that may pose a threat to the system while Step 2 consists in identifying their means and motivations. Then, Step 3 attempts to provide a categorization of the threats that could harm the

[1] Adapted from `https://csrc.nist.gov/glossary/`

Step	Description
1	Determine the Threat Actors.
2	Determine Motivation and Skills of the Threat Actors.
3	Categorize Threats
4	Asses the risk caused by these threats

Table 3.1: Threat Modelling Methodology Steps

system assets. Finally, Step 4 evaluates the risk caused by any of these attacks. While the first three steps will be explored below, Step 4 may not be explored fully at this stage as the system is too vast and heterogeneous for each asset to be known precisely enough to perform these tasks rigorously. Assessing the risk associated with a threat is beyond the scope of Task 1.2 and should be explored in further work packages.

3.1.3 Step 1: Determining Threat Actors

A threat actor is a person or any organization carrying a motivation or willingness to perform a malicious activity targeting any entity. The National Institute of Standards and Technologies (NIST) has prepared a guideline covering all aspects of cybersecurity on the protection of electricity infrastructure components. According to NIST7628, Guidelines for Smart Grid Cybersecurity [31], there are eight categories of threat actors that might target any electricity infrastructure which is explained below.

- Nation States: State-run, well organized, and financed. Use foreign service agents to gather classified or critical information from countries viewed as hostile or as having an economic, military, or political advantage.
- Hackers: A group of individuals (e.g. hackers, phreakers, crackers, trashers, and pirates) who attack networks and systems seeking to exploit the vulnerabilities in operating systems or other flaws.
- Terrorists/Cyberterrorists: Individuals or groups operating domestically or internationally who represent various terrorist or extremist groups that use violence or the threat of violence to incite fear to coerce or intimidate governments or societies into succumbing to their demands.
- Organized Crime: Coordinated criminal activities including gambling, racketeering, narcotics trafficking, and many others. An organized and well-financed criminal organization.
- Other Criminal Elements: Another facet of the criminal community, which is normally not well organized or financed. Normally consists of a few individuals, or of one individual acting alone.
- Industrial Competitors: Foreign and domestic corporations operating in a competitive market and often engaged in the illegal gathering of information from competitors or foreign governments in the form of corporate espionage.
- Disgruntled Employees: Angry, dissatisfied individuals with the potential to inflict harm on the smart grid network or related systems. The impact on the system is highly dependent on the access of the individual as well as the current state of its employment status.
- Careless or Poorly Trained Employees: Those users who, either through lack of training, lack of concern, or lack of attentiveness pose a threat to smart grid systems. This is another example of an insider threat or adversary.

3.1.4 Step 2: Determine Motivation and Skills of Threat Actors

After having determined threat actors, it is convenient to determine the extent of the damage they are willing to achieve. To answer this question, it is essential to understand their motivation. Motivation is what triggers threat actors to perform any malicious act. After having considered eight threat actors described in the previous subsection, there are four main motivation sources by which they are fed [32]. Those motivation sources are described below [30]:

- Ideological - Gain support for and deter opposition to a cause (i.e., carry out dictates of an ideology)
- Satisfaction - Giving damage for the purpose of being known (i.e., becoming celebrity)
- Geopolitical (or Ideological Violence) - Advance interests of the nation-states

- Profit - Financial gain

The motivation behind is usually in proportion with the skills the threat actor has. If any threat actor targets a nationwide electricity infrastructure, it comes with a set of technical resources or high experience of performing malicious cyber-attacks to the target. Thus, likely techniques of threat actors can be described in form of techniques which are described in MITRE ATT&CK Framework. Although there are thousands of techniques [29], ten general techniques which might be used by threat actors targeting electricity infrastructure are listed in Figure 3.1 given below.

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Operating Mode	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Engineering Workstation Compromise	Execution through API	Project File Infection		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
Exploit Public-Facing Application	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Exploitation of Remote Services	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
External Remote Services	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Internet Accessible Device	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Remote Services	Scripting						Program Upload		Device Restart/Shutdown		Loss of Safety
Replication Through Removable Media	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Rogue Master							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Spearphishing Attachment									Rootkit		Manipulation of View
Supply Chain Compromise									Service Stop		Theft of Operational Information
Wireless Compromise									System Firmware		

Figure 3.1: Techniques used for ICS threats © 2020 The MITRE Corporation.

3.1.5 Step 3: Categorize Threats

Threats are the effects of threat actors accomplishing their motivation and techniques. Any threat can be targeted to some components or all the electricity infrastructure which depends on the target of the threat actor. Anyhow, the motivation of the actor determines what cybersecurity property he/she does targets. If any actor targets confidentiality of data in the smart meter of any consumer, the actor might target the use of electricity consumption in any house. This can indicate that such an actor might follow the movements of anyone living in this house, which breaks the privacy-preserving rules of society. Thus, categorizing threats based on major cybersecurity properties will make it easier to conduct a cybersecurity program which afterward, makes it easier to manage risks.

STRIDE - Spoofing, Tampering, Repudiating, Information Disclosure and Denial of Services

STRIDE is an acronym that stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. STRIDE is a threat categorization methodology developed by Microsoft that helps to identify computer security threats. STRIDE differentiates possible threats under 6 categories, which cover six major essential cybersecurity properties. According to STRIDE, those six cybersecurity properties must be guaranteed for the system to be secured. Table 3.2 illustrate how those properties match with the threat categories that compose the STRIDE acronym.

Each threat category described in Table 3.2 can be refined into several particular threats as illustrated in Table 3.3. Then, those threats can be further refined to distinguish possible attacks that might be performed on the cyber components mentioned in Chapter 2.

Cybersecurity property	Threat concept
Authenticity	Spoofing
Integrity	Tampering
Non-repudiation	Repudiation
Confidentiality	Information disclosure
Availability	Denial of service
Authorization	Elevation of privilege

Table 3.2: STRIDE threats and matching cybersecurity properties

Spoofing [23]	Tampering [33]	Repudiation [33]	Information disclosure [23]	Denial of service [23]	Elevation of privilege [23]
ARP poisoning	Tampering with a file	Repudiating an action	Active reconnaissance	Buffer overflow attacks	Process injection
MAC spoofing	Tampering with memory	Attacking the logs	Source code disclosure	ICMP flood	User enumeration
IP spoofing	Tampering with a network		Inappropriate handling of sensitive data	SYN flood	Kernel exploitation
DNS cache poisoning			File name and file path disclosure	Smurf attack	Fuzzing
GPS spoofing					Directory traversal

Table 3.3: Threats based on threat concepts of STRIDE methodology

Deriving threat scenarios from such a categorization is only possible if we have determined and identified the entire set of assets that compose the system as well as their interfaces. Chapter 2 attempts to perform such a task. However, it does not claim to be exhaustive as the system is very large, very complex, and very dynamic with new devices being continuously introduced. Then, the process of finding how a threat can be materialized into an attack is quite tedious. As such, the threat mentioned by STRIDE only specifies the cyber-property that will be compromised and does not give a single clue on the asset that is being targeted. In addition to that, the methodology is very oriented toward adversarial attacks and hardly encompasses spontaneous failures and bugs. Finally, STRIDE does not help in any way for reducing a system complexity by considering aggregate groups of devices. For these reasons, the STRIDE methodology does not seem to fit the application of categorizing cyber-physical threats in the context of such a large system. Such a methodology is well suited for the determination of common attacks and risk assessment about the magnitude of their potential aftermath on a given cyber-system. It however lacks flexibility in the sense that only threats considered by the predefined families will be identified.

Cyber-Space as Services (CSaS)

Chapter 2 introduced a model of the cyber-space as a collection of services. The interest of such an abstraction is that it groups devices and software that perform the same function into the same category -*i.e.,* a service - and allows to identify of threat scenarios at various service abstraction. Such a modeling approach elegantly addresses the shortcomings mentioned in the previous section as it allows to encompass many meaningful use cases without requiring advanced knowledge about a specific cyber-physical system. While methodologies such as STRIDE the required knowledge of each specific device and piece of software in the system while the CSaS approach allows for the definition of threat scenarios in a much more general fashion. As a consequence, the CSaS framework allows to define and model a near-exhaustive variety of threat scenarios that at least encompass all the scenarios covered by the STRIDE methodology.

Quality of Services (QoS) In the CSaS framework, threats are modeled as disruption of the quality of one or several services. In order for this definition to fully make sense, Quality of Service (QoS) needs to be properly defined. In this context, several metrics can be defined to quantitatively assess the performance of a service.

We define the quality of a given service by using 3 QoS metrics that can be used to quantify the quality of any given service.

- Latency: It quantifies the amount of time taken between the request for a service and the delivery of that service to the system.
- Accuracy: It quantifies the *difference* between the expected and the achieved service.
- Availability: It quantifies the proportion of time that a service is available for being delivered to the system.

QoS guarantees In order to work as intended, a service must keep each of its QoS metrics above a certain acceptable threshold. These thresholds depend heavily on the service that is considered and the given metric, but the approach is quite for every service. Let us show a few examples of the modeling capabilities of this approach by applying the three QoS metrics to derive threats that are equivalent to the degradation of a given QoS metric:

- Example 1 - Time synchronization
  - Latency - An increase in latency would mean that accurate timestamps can still be established but the process takes longer. Latency above a certain (small) threshold would make the system unusable for its intended purpose (e.g. accurate time-stamping).
  - Accuracy - A decrease in the accuracy would mean that the timestamps have a different value from the one they should have at that given time. Too high inaccuracy makes the service unreliable.
  - Availability - An inadequate level of availability means that sometimes, establishing timestamps is impossible.

  Two things are highlighted by this example. Firstly, this is very generic. A lot of scenarios can hide behind a decrease or increase of the QoS metrics. Secondly, the importance of the granularity of services becomes obvious. If a service is not specific enough, then it may be difficult to see what a change in the QoS metrics represents and to evaluate what the acceptable thresholds may be.
- Example 2 - Communication
  - Latency - An increase in latency that information can still be transmitted but reaches its destination after a long delay. Depending on the context, this may be acceptable or not, e.g. some remotely controlled actuator must perform an action in a very short delay to prevent damaging equipment.
  - Accuracy - A decrease in the accuracy would mean that the information is somewhat corrupted during transmission and is different from what was sent. As any inaccuracy can make the information unusable, this typically means that it must be discarded or resent, depending on the requirements.
  - Availability - Unavailability of the communication layers means that some proportion of the time, it is impossible to send information through the channel. The availability acceptable threshold is typically very close to 1 as any disruption of the service causes latency to the higher-level services that rely on it, i.e control and monitoring.
- Example 3 - Control (Application Service)
  - Latency - An increase in latency that the actuation is performed after a given delay, the acceptable delay depends heavily on the controlled device.
  - Accuracy - A decrease in the accuracy would mean that the control instructions are for some reason inaccurate. The acceptable accuracy threshold should be very close to 1 as invalid instructions may damage equipment or cause a blackout.
  - Availability - Unavailability of the control service means that for a proportion of time, the system cannot be controlled. This proportion should be close to 0 as the system requires active (human or automatic) control to work as intended without damage.

Coverage of STRIDE As mentioned in previous sections, STRIDE defines families of threats that can be refined into more specific attacks on particular cyber-assets. In the CSaS framework, threats come in the form of an inadequate level of service quality. If the STRIDE families of attacks can be expressed in terms of inadequate levels of QoS metrics, then it means that the CSaS is shown to encompass the same use cases as STRIDE. The mapping between the two is shown in Table 3.4.

STRIDE family	CSaS equivalent(s)
Spoofing	- Inaccuracy of the communication service - Inaccuracy of the integrity service
Tampering	- Inaccuracy of the storage service - Inaccuracy of the integrity service
Repudiation	- Unavailability of the storage service - Inaccuracy of the integrity service
Information disclosure	- Unavailability of the confidentiality service
Denial of service	- Unavailability of the communication service - Latency of the communication service - Unavailability of application services (e.g. monitoring and control) - Latency of application services
Elevation of privilege	- Inaccuracy of the authentication service

Table 3.4: Mapping between STRIDE families and QoS metrics

Intermediate Results

As a result of applying the first steps of the methodology, a series of threats were identified and provided in Table 3.5, and Table 3.6. They aim at expressing the most common threats considered in cyber-physical systems in the context of the CSaS framework. In these tables, each threat is associated with a potential degradation of the QoS metric(s).

Threat	Service	Latency	Accuracy	Availability
Channel interference	Communication		X	
Configuration errors	Any service	X	X	X
(Un)intentional data corruption	Integrity		X	
(Un)intentional data leakage	Confidentiality		X	
Erroneous use of systems	System-dependent	X	X	X
Erroneous use of administration interfaces	Control	X	X	X
Unintentional data alteration	Integrity		X	
Intentional physical attacks	Any service	X		X
Failures & Malfunctions	Any service	X	X	X
Natural disasters	Any service	X		X
Distributed denial of service	Any service (Comm. in particular)	X		X
DNS spoofing / poisoning	Authentication		X	
DNS registrar hijacking	Authentication		X	
Generation and use of rogue certificates	Authentication		X	
Identity theft	Authentication		X	
Malicious code injection	Storage & Integrity		X	
Malformed data injection	Storage & Integrity		X	

Table 3.5: Decrease of service QoS associated with each threat (1 / 2)

Threat	Service	Latency	Accuracy	Availability
Virus/Worms/Trojans/Malware	Any application Any operational service	X	X	X
Phishing	Authentication		X	
Privilege escalation	Authorization		X	
Password attacks	Confidentiality		X	
Unauthorized software installation	Authorization		X	
Use of restricted software	Authorization		X	
Privilege escalation	Authorization		X	
Distributed denial of service	Any service (comm in particular)	X		X
Information manipulation	Comm. , Storage & Integrity		X	
Information theft/gathering	Confidentiality		X	
Session hijacking	Authentication		X	
MITM Masquerade	Authentication		X	
Wireless network interception	Confidentiality		X	
Replay of messages	Authorization & authentication		X	
BGP Autonomous System hijacking	Comm., authorization		X	X
BGP Address space hijacking	Comm., authorization		X	X
BGP Route leaks	Confidentiality		X	
Smart meter connection hijacking	Authentication		X	
War driving/flying	Confidentiality		X	

Table 3.6: Decrease of service QoS associated with each threat (2 / 2)

Threat scenarios generation

As the CSaS model represents threats as the potential disruptions in the Quality of Services (QoS), threat scenarios must originate from the degradation of one or several QoS metrics. However, this is not specific enough to illustrate clearly how this scenario will affect the overall system and what will be the exact physical consequences of this given scenario. In order to establish a clear link between the degradation of QoS metrics of one or several services and how the power grid may be affected, a methodology based on the construction of attack trees is proposed.

Attack trees Attack trees are a representation of the chain of events in a given attack scenario. The root of the tree is the outcome of the overall attack scenario, i.e. the aim of the attacker. The children of a given node in the tree are conditions to make the parent event true. These conditions can be sufficient, i.e the parent is an OR node, which means one of them must happen for the parent to happen. Alternatively, they can be individually necessary and sufficient when all combined, i.e the parent is an AND node, which means that they must all happen so that the parent happens. Thus, the events of the bottom layers chronologically happen before the ones of the upper layers as they are necessary for their accomplishment [34]. An example attack tree is presented in Figure 3.2.

This concept is very relevant in the context of the CSaS threat model as it allows to work at different levels of abstraction to define the complete chain of events that may follow from a given attack or failure. Attack trees as they are covered in the literature do not encompass failures but they can be easily extended by considering some or all events in a given scenario to be spontaneous failures.

Granularity of the abstraction level Defining different abstraction levels can be meaningful. The services defined in Chapter 2 have three layers of abstraction: application services, operational services, and utility services. Each level relies on the level below it to accomplish its operations. Utility services are the lowest level of services as they abstract actual hardware and software components of the systems.

High-level abstractions allow focusing on different criteria when defining scenarios. For example, working at the application level offers insights into the behavior of the system in terms of end-user experience but does not permit determining the inner workings that led to this given experience. On the contrary, working at the utility level allows to study how specific components or parts of the system can fail or be attacked but it provides little information about the system-wide consequences of the given threat scenario.

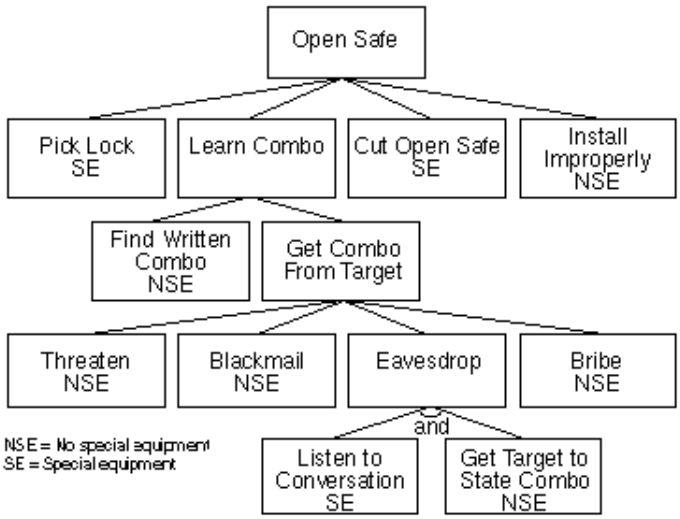

Figure 3.2: Example of an attack tree [34]

Working at several layers of abstraction can be necessary in order to describe a specific threat scenario. Figure 3.3 how a given scenario can be studied at different abstraction levels. This figure highlights how the higher levels can be satisfied until more details are required. Any event in this scenario can be expressed in terms of the degradation of QoS metrics.

Interestingly enough, the diagram presented in Figure 3.3 is essentially an attack tree for the entire attack on the forecasting application. However, while this full-picture view of the scenario is interesting, it lacks a direct connection to the CSaS framework. Indeed, while each attack in this scenario can be associated with the degradation of a QoS metric, a clear methodology for going from one to the other lacks.

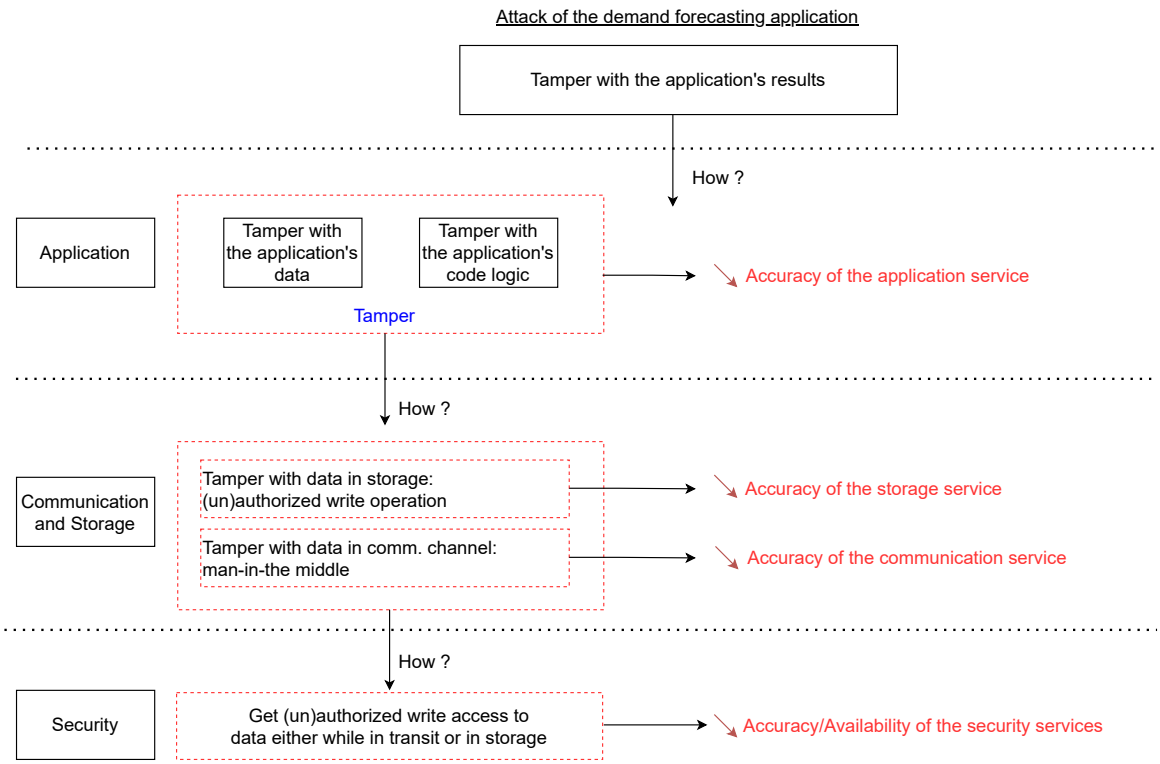

Figure 3.3: Different abstraction levels in an attack on the demand forecasting application

Atomic attacks The remainder of this section will focus on the modeling of atomic attacks. Atomic attacks are attacks that cannot be subdivided into smaller attacks. By definition, each complex (i.e non-atomic) attack can be subdivided into a set of smaller attacks. Thus each attack scenario can be reduced to a set of atomic attacks.

Top-down vs bottom-up Before going further into the modeling of atomic attacks, it is necessary to describe an important principle in how these models can be used for risk assessment and simulations. The modeling approach focuses on linking the degradation of QoS metrics with atomic attacks. There are two ways this can be relevant.

- **Top-down approach**: Go from a given threat to the degradation of a QoS metric. The existing known threat scenarios can be described in terms of the degradation of QoS metrics. This can, for example, help to build simplified simulations.
- **Bottom-up approach**: Go from the degradation of QoS metrics to unknown threat scenarios. QoS metrics of a given service can be modified in order to discover the potential consequences of their joint degradation. Unknown threat scenarios can thus be discovered.

Attack trees for atomic attacks Let us present a specific methodology connecting QoS metrics to atomic attacks. Essentially, the idea is to build an attack tree of a specific structure.

- **Mean**: Initial capabilities of the attacker, what makes the attack possible.
- **Vector**: How the attacker can get the necessary access to successfully perform the attack. This is always equivalent to lowering the QoS of security services.
- **Threat**: The nature of the attack. This corresponds to the degradation of some service(s) other than security services.
- **Consequences**: Outcome of the attack, how the system is affected, and additional means of the attacker gained through the attack.

Figure 3.4 illustrates how data could be modified at the communication level in the scenario presented in Figure 3.2 by an attack tree constructed using the methodology presented above.

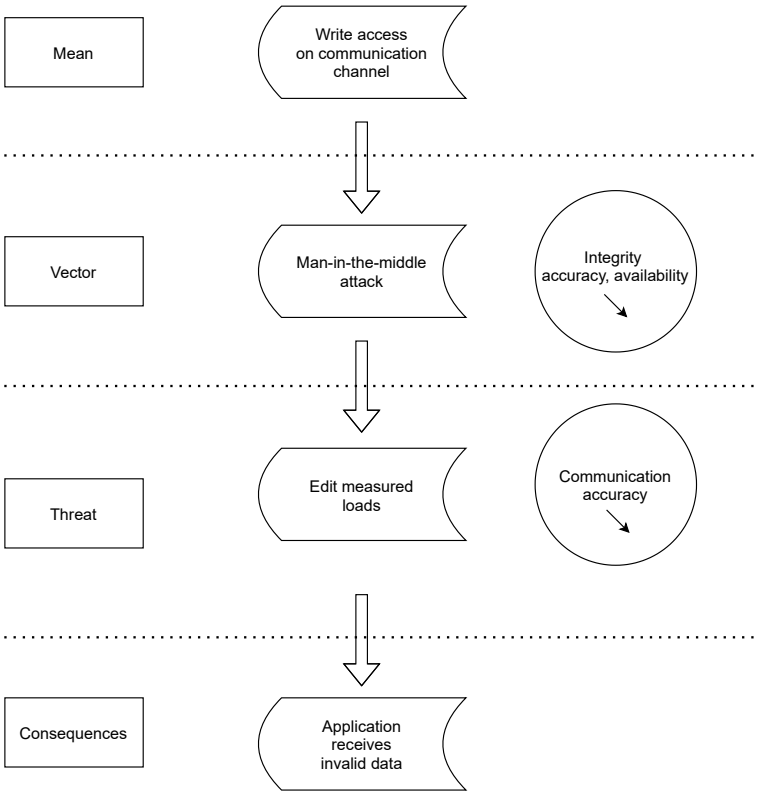

Figure 3.4: Attack tree for the modification of data through the communication channel

These simple attack trees can be used to connect QoS metrics to attack scenarios. The top-down approach consists here in describing a known attack with this technique to find the associated QoS metrics degradation. The bottom-up approach consists in discovering attacks by exploring the possible QoS metrics degradation and finding their possible cause (i.e. the mean) and associated consequences.

While this methodology particularly fits adverse attacks, it could also describe a failure scenario.

- Mean = conditions making the failure possible.
- Vector = unsatisfied security property that allows the failure to have consequences.
- Threat = what the failure does to the system.
- Consequences = how system behavior will be affected.

Using this tool, any attack or failure scenario can thus be expressed in terms of the degradation of QoS metrics.

3.1.6 Step 4: Assess the risk caused by a Threat

A set of well-determined threats matching each component of cyberspace determines the outline of the cybersecurity program the electricity organization will run. However, since the resources of any company are not unlimited, those threats must be sorted based on their impact and probability of occurrence. If a threat is most likely to occur and its impact is high, such a threat must be detected and prevented to protect cyberspace from that threat's impact. This is called a risk assessment activity where several methodologies still exist such as DREAD [35] which also takes part in the NIST framework to perform a risk assessment. As it is very early to determine which risk assessment methodology should be chosen, general concepts and general approaches of any risk assessment model will be explained in this section.

Risk assessment mainly involves determining the likelihood as well as the potential outcomes of the exploit of threat, may it be accidental, or induced. Both in the case of induced and accidental exploit, a vulnerability in the infrastructure is always at the source of the threat scenario. Then, the induced exploit involves threat actors that have motivation, skills, and mechanisms. Preliminary risks definitions are:

- Quantitative risk definition Quantitative risk definition refers to the numerical description of any risk. In this case, the impact and probability are determined in numbers in which are chosen from scales. For example, a risk impact can be 3 where this number well matches a definition made in a scalic description table. There are several tools and techniques of quantitative risk analysis which are Three Point Estimate, Decision Tree Analysis, Expected Monetary Value, Monte Carlo Analysis, etc. [36]
- Qualitative risk definition Some risks are not meant to be determined in numerical values. For instance, the risk of losing reputation after a data breach might not be well determined numerically. Thus, a qualitative approach consists of the non-numerical description of any risk. [36] Possible tools and techniques of qualitative risk analysis are Risk Urgency Assessment, SWOT Analysis, ICOR Analysis, etc.
- Semi-quantitative risk definition Semi-quantitative risk definition refers to a numerical description of risk categorization that assigns probability and impact of potential threat to be exploited based on existing data and available consequence estimates. This method is usually used for types of risks for which it is desired to apply generic quantitative risk analysis parameters such as time and cost are not applicable, or instinctive categorization is needed. For example, any threshold can be determined by company experts to determine the category of any risk. These categories can be described as "High", "moderate", "low" or 1 to 5 [36], [37].

Any evaluation of the risk that may be involved when considering a threat needs to comply with one or several of these risk definition methods. Then, the ease of exploitation and existence of known vulnerabilities should be identified. Section 3.2 attempts to provide preliminary work on identifying a set of broad vulnerabilities in power systems. However, a proper risk assessment would require much more in-depth knowledge about the system than is known at this stage. Additional and more specific vulnerabilities could be found via penetration testing.

3.2 Vulnerabilities

Vulnerabilities refer to inherent deficiencies of any system that, once discovered, can be exploited by threat agents to realize threat scenarios. Threat agents might be attackers using various techniques depending on

their means and motivation but might also refer to an unfocused employee that introduces buggy pieces of code into the system. Vulnerabilities located on valuable assets should be periodically discovered and well managed through different techniques such as penetration testing, vulnerability assessment, etc. Their identification is necessary to fully exploit the framework depicted in Section 3.1. Then, those vulnerabilities can be matched with threats.

In this section, several vulnerabilities that might exist in modern electricity infrastructure will be discussed. Identifying specific vulnerabilities depends on the specific device or piece of software. In practice, vulnerabilities are found via penetration testing. Determining the specific vulnerabilities of each component is beyond the scope of this task. Broad categories of vulnerabilities found in the electrical infrastructure are provided as a reference for further works. According to the research done by Leszczyna [38], ten general vulnerability categories are relevant to electricity infrastructure:

- Insecure communication protocols Existing modern electricity infrastructure standard protocols are based on real-time communication. Adding security measures to these protocols increases data transfer time, which in the end, causes delay. These widely used protocols such as Modbus, GOOSE, and SV, DNP3, or other protocols described by IEC61850 do not target cybersecurity properties such as confidentiality, integrity, availability, or others that were previously defined in STRIDE methodology. Thus, such protocols can be targeted to extract or infiltrate confidential data that they carry.
- Broad use of commodity software and devices Modern electricity infrastructure is made of widely available commodity solutions such as MS Windows or Linux operating systems. Also, they utilize common applications such as Apache, HTTP Server, MS SQL, or other MS solutions. This situation makes electricity systems susceptible to being targeted by the same attack vectors of major organizations. Adding to the lack of updates and patching, the infrastructure is becoming more vulnerable.
- Increased utilization of IP-based network connections, vast connectivity Although IP-based standard network connection brings easiness and cost reduction, it brings all vulnerabilities of such networks. Assuming that the electricity infrastructure is interconnected by IP and/or TCP/IP-based communication within isolated intranets, once this is connected anyhow to the internet, such a system can be reachable if targeted. Adding the use of wireless communication, the system is becoming more and more vulnerable, knowing that wireless communication without additional security measures (e.g encryption) is not secure enough.
- Limited or ineffective network segmentation Network segmentation limits the ability of attackers to penetrate the system and reduces the impact of any possible attack. Although the use of firewalls and other cybersecurity devices has increased, their misuse or misconfiguration can lead attackers to penetrate electricity infrastructure easily.
- Limited applicability of standard cybersecurity solutions Because of the lack of electricity infrastructure-specific cybersecurity devices, it is easier for threat actors to penetrate the systems. Some protocols used in the data transfer of electricity infrastructure cannot be detected with commodity cybersecurity devices such as Firewalls, Intrusion detection and prevention systems, and anti-malware systems, which in result causes breaches, which can even go undetected.
- Increased availability of technical specifications of IACS The ease of finding technical information about devices used in the industry in the Internet era gives attackers deeply detailed information on such devices. Although such sharing is aimed to help domain-specific knowledge spread, it is used by threat actors to perform malicious activities. This gives attackers increased quality of reconnaissance activities.
- Use of non-standard smart meters As electricity infrastructure consists of an extremely large number of devices that are produced by various manufacturers, the production of standardized devices is limited. Devices such as smart meters are typically vendor-specific. Additionally, these are produced in many different countries, which decreases, even more, the standardization level, as the needs of these countries depend on their specificities. Having unstandardized smart meters causes some attackers to be able to exploit some of those devices through device-specific vulnerabilities. This situation can allow an attacker to perform a basic man-in-the-middle attack, leading attackers to track activities of the consumer in the house where the smart meter is connected. Among other concerns, this is problematic from consumer privacy.

It is impossible to provide an exhaustive list of vulnerabilities as their discovery depends on techniques such as penetration techniques. Exhaustiveness in this context would imply that it is possible to identify, with limited

time and resources, every failure scenario that a given piece of software may present. This is probably impossible as this would imply solving the halting problem which is impossible in the general case [39]. However, one should still apply common techniques to try and find vulnerabilities. More importantly, the vulnerabilities which are already known, obvious, or easily found should be a priority when designing security barriers. In particular, the vulnerabilities that were cited above should be explicitly addressed both for risk assessment and countermeasures design.

4

Cyber-Resilience & Barriers

4.1 Cybersecurity principles

4.1.1 Cybersecurity properties

As the potential attackers' resources are essentially unbounded, likely, breaches happen regardless of countermeasures put in place. However, it would be foolish to disregard a large amount of knowledge regarding good cybersecurity practices. These may not prevent sophisticated attacks from an enemy nation-state but can at least keep critical infrastructure safe from less threatening actors.

A successful approach to cybersecurity is attained by defining important properties that must be satisfied for some data and the systems it resides on. The classical set of such properties is often referred to by the acronym CIA: Confidentiality, Integrity, Availability. These 3 concepts are the cornerstone of secure computer systems [23].

Let us define these cybersecurity properties.

- Confidentiality: The data is only accessed by those who are allowed to see it. No unauthorized disclosure of information may happen [23].
- Integrity: The data is only modified in context when it is allowed and in the way that it is supposed to be. No unauthorized modification may happen [23].
- Availability: Authorized actors must be able to access and modify data promptly when they are allowed to do so [23].

It should be noted that while the same terms are used by the CSaS framework, they do not share the same meaning. Integrity as presented here encompasses authentication and authorization. Furthermore, these are considered as properties that should be satisfied at all times, not as services or metrics.

Confidentiality

The problem of confidentiality arises mostly when the information is transferred via an unprotected medium, the most relevant example being transmission over TCP or UDP on a network such as the Internet. When information is not in transit, this problem is reduced to an access control problem. Only a certain set of authorized users may read and/or alter the data [23].

Access control is not a technically difficult problem. A locked door and a camera are sufficient to ensure bad actors stay away from critical systems. If remote access to the system is possible, there exist proper authentication techniques to ensure that access is indeed warranted. These will be discussed when the necessary concepts have been introduced. Nothing IT-based will prevent espionage techniques such as gaining legitimate access by getting hired in the company. For this reason, mitigation techniques have to be considered.

As the most critical operation from a confidentiality standpoint is data transfer, let us focus on how data can be kept safe while it makes its way to its new location. The main tool to prevent eavesdropping on an untrusted shared medium is encryption [23].

Encryption consists of the transformation of information with the use of a secret, the encryption key so that it can only be read by transforming it with another secret, the decryption key. The encryption and decryption keys can be identical, in which case the encryption is said to be symmetric. Asymmetric encryption is an encryption scheme where these keys differ [23].

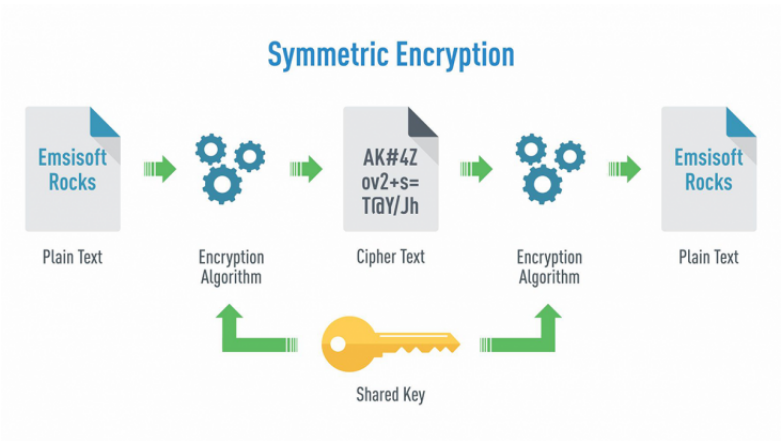

Figure 4.1: Communication with symmetric encryption
Source by `https://upload.wikimedia.org/wikipedia/commons/b/ba/Symmetric_encryption.png`

Symmetric encryption is based on the shared knowledge of the secret key. Through the use of an encryption algorithm, the ciphertext is created from a combination of the plain-text message and the secret key [23], [40]. The message can then be sent through the untrusted medium and be decrypted by the recipient that can apply the decryption algorithm to the ciphertext and the shared key to get back the original message. An eavesdropper could not get access to the message during transit since they would not know the secret key to decrypt the ciphertext [23], [40] This is illustrated in Figure 4.1.

Asymmetric encryption is often referred to as public-key encryption. The reason for this alternative name stems from the way asymmetric key cryptography schemes are designed. Each participant in the communication generates a pair of keys: a public key and a private key. The public keys are made public prior to the transfer of the message of interest [23], [40]

The sender of a given message creates ciphertext by encrypting its plaintext message with the public key of the recipient through a public key encryption algorithm [23], [40]. The only way to decrypt this message should be by feeding the private key of the recipient and the ciphertext to the decryption algorithm. No one but the recipient should be able to read the message since their private key is only known to them [23], [40]. This process is illustrated in Figure 4.2.

This scheme presents the advantage of requiring no shared secret between communicating parties. However, there is a serious difficulty in the problem of reliable public key distribution. Without a way to certify that a key belongs to the legitimate recipient, a sender may encrypt the message with the key of the attacker that would then just need to intercept the message and decrypt. This may even go unnoticed as the attacker may act as

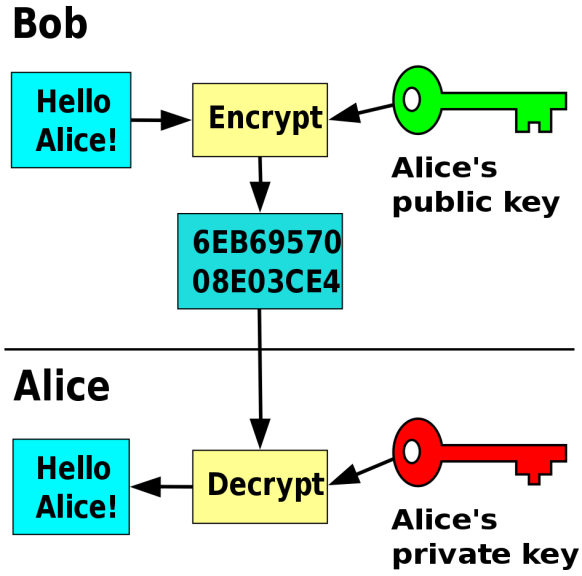

Figure 4.2: Communication with public key encryption
Source by
`https://en.wikipedia.org/wiki/\Public-key_cryptography#/media/File:Public_key_encryption.svg`

a man in the middle, re-encrypting the message with the correct public key and sending it to the legitimate recipient [23], [40].

This problem is usually solved by introducing the Public Key Infrastructure (PKI) allowing the certification of public keys by Certification Authorities (CA). CAs issue certificates validating the public key of the recipient. The CA signs the certificate with its private key so that all can check the signature by applying the public key of the CA to the certificate [23], [40]. This is a technique for guaranteeing integrity, which will be further discussed.

For scalability reasons, CAs are organized as a hierarchy in which each CA's certificate must be signed by a CA above it. CAs at the root of the hierarchy issue self-signed certificates which is acceptable since their public keys are well-known and encoded in every client [23], [40]. In practice, symmetric encryption is more efficient than asymmetric encryption as larger keys and more complex computations are required to achieve the same level of confidentiality with asymmetric methods than with symmetric ones [40].

Common practice thus dictates that, for performance reasons, the use of public-key cryptography is limited to the exchange of symmetric keys. This combines the convenience of no fixed shared secret with the efficiency of symmetric cryptography. Furthermore, changing the symmetric key frequently (e.g once per connection setup, or at periodic intervals) reduces the possibility for attacks and minimizes the impact where one symmetric key is to be breached [23], [40].

Integrity

Asymmetric encryption for integrity The use of asymmetric encryption to ensure integrity was already mentioned when describing the PKI. Signing the message with the private key is a completely valid way to ensure integrity. However, the use of this technique requires trust and the availability of a PKI. This is not really practical depending on the context to even have certificates for each communicating entity. Furthermore, as asymmetric encryption does not scale well, it is not reasonable to use it as such.

Hash functions Hash functions are a special kind of function designed to be used as one-way functions. A hash function should have the following properties [23], [40].

- One-way: Given $h = H(x)$, H being the hash function and x its input, it should be difficult or impossible to find x from h.
- Collision resistant: Given $h = H(x)$, it should be difficult or impossible to find $x' \neq x$ such that $H(x')$ = h from h.

In practice, such functions are of great interest because they can be computed faster and can produce of fixed-length digest of any message. Given a pair (message, digest), it is easy to check if the digest corresponds to the message.

Digests for integrity purposes However, these message digests are not enough to ensure the integrity of a message sent over the network. An attacker intercepting a pair $(m, H(m))$ could simply replace the message and recompute the digest, sending $(m', H(m'))$ [23], [40]. However, this can be fixed easily through a shared secret S. Let us denote concatenation by the symbol ||. Sending $(m, H(S \mid\mid m))$ ensures that only both communicating parties can recompute the digest from the message [23], [40].

With symmetric encryption This is not necessary to incorporate a concatenated shared secret in the hash function if the pair $(m, H(m))$ is encrypted with a secret key as an attacker would not be able to encrypt its own (message, digest) pair [23], [40].

Asymmetric encryption signature Alternatively, as done within the PKI, it is possible to use asymmetric cryptography to ensure integrity. The message digest would be signed (encrypted) with the private key of the sender. The sender thus sends a pair $(m, K^{-}(H(m)))$ where $K^{-}(.)$ is encryption via the sender private's key. Everyone can check the message's integrity by decrypting the digest with the sender's public key but only the sender can generate such valid pairs [23], [40].

Message Authentication Code (MAC) A digest generated using a hash function and used to ensure integrity is commonly referred to as Message Authentication Code (MAC). However, this convention is somewhat misleading as it does not authenticate the sender. Indeed, an attacker could still intercept a message and resend it as is, impersonating the initial sender [40].

The alternative acronym MIC (Message Integrity Code) can be used to remove this ambiguity but this naming convention is more rarely seen in the literature [40].

Availability

Revealing or tampering with important data, i.e. attacking the confidentiality and integrity of that data can lead to disasters when important systems rely on its accuracy. However, preventing operators from accessing the data or making remote devices unavailable may lead to even greater issues. Availability is thus as much if not more important than the other 2 main cybersecurity properties.

Availability depends greatly on the reliability of software. The near-absence of bugs and security flaws is important. A good development methodology should aim to reach that goal. However, from the security specialist's standpoint, this is not realistic to think those will be enough to ensure availability. A natural catastrophe or physical attack is enough to destroy a device. Furthermore, software vulnerabilities are prevalent [23].

Physical protections: Ensure that the equipment is secure enough. It must be able to withstand a range of natural contingencies (e.g. have a backup generator for power outages) and have some physical security from bad actors (e.g be behind a locked door) [23].

Computational redundancies: Ensure that a given resource becoming unavailable does not put the entire operation of the service in jeopardy. There are many examples of this strategy [23]:

- RAID (Redundant Array of Inexpensive Disks): Data is stored in a virtual disk made up of an array of physical disks. The data of the virtual disk is partly replicated over several disks of the array so that the failure of a single disk does not prevent the operation.
- Replicating a web service on different servers so that the service is still reachable if one of the servers goes offline.
- Having a redundant network topology so that different paths to devices remain if a given link goes down.

4.1.2 Authentication techniques

Local authentication

Besides physically isolating devices from malicious actors, which is still an important security measure, control equipment itself should authenticate its user. The traditional way to authenticate the user of a local system is via passwords. The user types their account name and password. The latter will be checked against the stored version of the password. Typically, passwords themselves are never stored but rather salted hashes of them. A salt is arbitrary data associated with the user [23].

Given a password p, a salted hash would be of the form $H(p \mid\mid s)$. The system can easily check the validity of the password by recomputing the salted hash without needing to ever store the password. This presents the advantage that a leak of the password database would not easily result in the publication of a user's password that may be used somewhere else [23].

Remote authentication

Local authentication is achieved through proving knowledge of secret information that is only known to the users, i.e. their passwords. However, this technique cannot be applied as such to remote authentication as the password could be intercepted. Even encrypted, an attacker could still send the encrypted password without understanding it [23], [40]. Thus, a successful design for remote authentication must not only rely on proof of secret knowledge but also a proof of understanding of that knowledge. Only has the sender been properly authenticated by the receiver [40].

Warning Mutual authentication is a more complicated problem than unilateral authentication. Indeed, without care, running two unilateral authentications in parallel does not prevent impersonation by replay attack, i.e. resending intercepted packets [40]. Nevertheless, the principles are identical, and through proper protocol design, this can be avoided. For the sake of simplicity and brevity, all techniques will only be illustrated in a unilateral authentication context.

With symmetric encryption In an asymmetric encryption context, authentication can be attained by showing the ability to encrypt with the private key and by proving liveness, i.e. the message is not a replay of an intercepted message.

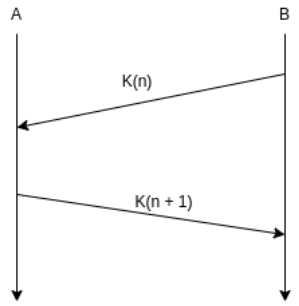

Figure 4.3: Simple unilateral authentication in symmetric cryptography context

Such a mechanism is illustrated in Figure 4.3. B sends a challenge to A, a random number called n. A shows an understanding of the message, knowledge of the key, and liveness by incrementing the message and sending it back to B. An alternative scheme would have been for B to send the challenge unencrypted and for A to encrypt it and send it back, showing liveness and knowledge of the key.

Without encryption Similar reasoning can be applied without the need for any encryption through the use of hash functions.

This is illustrated in Figure 4.4. B sends a random number n and sends it to A. A shows knowledge of a shared secret S and liveness by concatenating S and n and sending the hashed result to B. The one-way property of $H(.)$ guarantees that the shared secret cannot be recovered (easily) from the message.

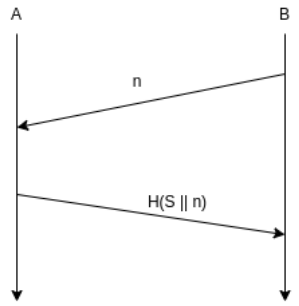

Figure 4.4: Simple unilateral authentication without encryption

With asymmetric encryption In an asymmetric encryption context, authentication through the certificate is guaranteed by the PKI. A certificate binds the identity of a person or service to a public key. The use of the PKI removes the need for a shared secret [23], [40].

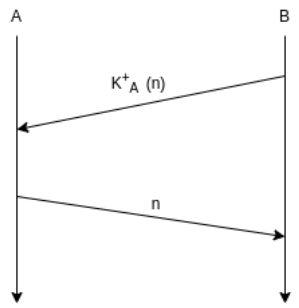

Figure 4.5: Simple unilateral authentication with asymmetric encryption

Figure 4.5 shows how asymmetric encryption can be used for authentication. B encrypts a random number with A's public. A sends the unencrypted number back to B to show liveness and knowledge of the private key.

4.2 Common implementations of cybersecurity properties

The security properties discussed in the previous section are commonly used together for communication over the network. As guaranteeing they are all simultaneously satisfied is a difficult problem and demands a careful protocol design, standard protocols have been designed and are widespread.

A couple of these protocols are introduced below as they give a good idea about how operators can secure data communication in practice.

4.2.1 TLS

Transport Layer Security (TLS) is a protocol that is widely used for communication over the Internet. Its most common use is to secure HTTP traffic. HTTP over TLS is known as HTTPS [23].

TLS can be seen as an additional layer above TCP in the TCP/IP network stack. While it is technically at the application layer, it is typically used as a service rather than implemented by the application's programmer [40]. Implementations of TLS are readily available in libraries for programmers to use.

TLS establishes an end-to-end authenticated, encrypted connection with guaranteed integrity. In most cases, only the server is authenticated as it is inconvenient to purchase a certificate for each web client. This still prevents a potential attacker from acting as a man-in-the-middle since it is impossible to impersonate the server. It is however possible to require both communicating parties to have certificates if necessary [40], [41].

The usual TLS connection establishment consists of the negotiation of a symmetric session key through the use of asymmetric cryptography. The encryption algorithm, key format and size, and all relevant parameters are negotiated [40].

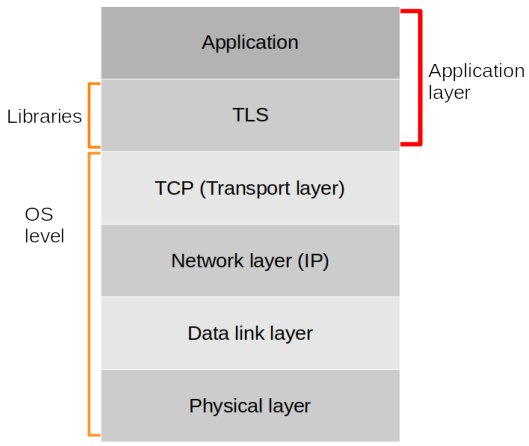

Figure 4.6: Network stack with TLS encryption

Variants of this protocol that make no use of asymmetric cryptography but rely rather on symmetric Pre-Shared Key (PSK) exist and are referred to as TLS-PSK [42].

An important detail to understand is that independently from whether TLS-PSK is used, or one or two certificates are provided, the available encryption technique is only used for the negotiation of a symmetric session key which will be used to encrypt the messages [40], [41].

Using one cryptographic key per session is a recommended practice. The negotiation of that key can simply consist of the client sending a random number to the server which both derive a secret key from [40], [41].

This approach is completely valid but an attacker may still record all traffic in hope that the servers' private key (classical TLS) or the secret key (TLS-PSK) is revealed, in which case, decrypting everything would be possible by deriving the session keys [40], [41].

This can now be avoided through more advanced techniques based on the Diffie-Hellman key exchange, which allows both parties to generate a shared key without sending it over the network. This property is called forward secrecy and it is now standard practice for servers to support it, e.g for web traffic [43].

4.2.2 IPSec

Motivation - TLS flaws

The approach used in TLS of implementing security guarantees over TCP is completely valid but it presents a few disadvantages. Firstly, it obviously only works for applications that run over TCP. This approach will be of no help for applications running over UDP. Secondly, since TLS encryption is technically an application running over TCP, none of the TCP and IP headers are encrypted. Thus, although application data is encrypted, ports and IP addresses are visible. This means that an attacker can easily know which hosts are communicating and may even identify the type of traffic just by recognizing a standard port number [40]. Finally, an active attacker could perform a Denial Of Service (DOS) attack, i.e. end the connection between communicating parties by injecting a single packet into the data stream [40].

Since integrity is implemented as an application running over TCP, there is no backchannel to inform TCP that a packet was injected into the legitimate traffic and should just be rejected [40]. Thus, if an attacker forges a packet masquerading as the next packet in the sequence, it will be accepted by TCP and pushed up to the application, i.e. TLS. The integrity check performed by TLS will fail, but TCP will reject the legitimate packet and its retransmissions as it believes the packet to already have been delivered [40].

Reason for these flaws The reason why TLS presents these shortcomings is the assumption within its design that security guarantees can be implemented on top of, and independently from reliable data transfer. There is no possibility to remove them without getting rid of this design assumption [40].

IPSec: a different approach

The design of IPSec is fundamentally different in the sense that it considers that reliable data transfer is something that should be implemented over a channel that already offers security guarantees such as confidentiality and integrity. IPSec support is built into the operating system of the communicating hosts as it inserts itself into the TCP/IP network stack (see Figure 4.7).

IKE IPSec assumes that symmetric keys for encryption and signatures are available to guarantee confidentiality and integrity. The establishment of such keys is done via the Internet Key Exchange (IKE) protocol [40].

IKE establishes Security Associations (SA) and the related keys. SAs are all the information necessary to communicate via secure unidirectional "connection" (these do not guarantee reliable delivery). IPSec mandates that different keys are used for different operations, so each communicating host will get an encryption key and a signing key that they use for the messages sent to the other. IKE is thus used to establish 4 symmetric session keys [40], [41].

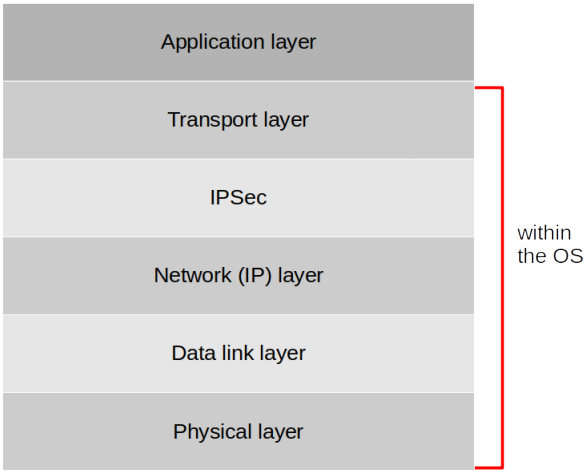

Figure 4.7: Network stack with IPSec

Similar to TLS, the key can be derived from a Pre-Shared Key (PSK), or established via asymmetric encryption techniques. Diffie-Hellman is always used, which guarantees forward secrecy of the IPSec sessions [40], [41].

IPSec modes IPSec offers two modes of operations: transport mode or tunnel mode. Transport mode is an end-to-end connection between two IPSec-capable hosts while tunnel mode is used to establish a tunnel between two devices (typically routers) to encapsulate IP traffic transiting in-between these routers. The usual use of this mode is to establish a secure Virtual Private Network (VPN) [40], [41].

AH and ESP IPSec offers two different ways to provide integrity and/or confidentiality. AH (Authentication Header) provides only integrity but it guarantees the integrity of the IP header (contrary to ESP which does not) [40], [41]. ESP (Encapsulating Security Payload) can be used to guarantee both integrity and confidentiality. It is possible to combine AH and ESP if, for some reason, the integrity of the IP header is truly required (which is rarely the case). It should be noted that important fields of the IP header such as addresses are stored into Security Association databases by the communicating hosts, so the fact that ESP does not guarantee their integrity would not help an attacker modify them [40], [41]. AH and ESP can both be used either in tunnel or transport mode [40].

Conclusion

In the context of the CYPRESS project, the details of protocols such as TLS and IPSec are of little matter. However, these were presented because they illustrate very well that ensuring the basic security of network communication is not a difficult thing. While developing such protocols may require advanced knowledge and techniques, there are already standard protocols readily available for efficiently securing communications over the network.

Applying these techniques should be done by default whenever possible There is rarely any reason for confidentiality and integrity to be easily compromised while transiting through the network. In the case where low delays are required, which can sometimes be the case in power system communications, symmetric encryption (and hashing) can be implemented very efficiently in dedicated or programmable hardware (e.g. FPGA) [44].

4.2.3 Mitigation of breaches

Good security practices may protect systems from actors of low to moderate means, but considering attackers as powerful as nation-states or even disgruntled employees, securing end-to-end communication is not enough. Insider threats mean that even operators themselves may compromise the system. Their actions may thus very well be authorized, and wreak havoc freely.

Since the infrastructures are critical, it is not acceptable to say that such threats cannot be dealt with. While it is impossible to prevent an authorized malicious action by design, it should still be possible to detect and mitigate the impact of successful breaches.

Detection of anomalies

The abnormal behavior of a given device is best detected according to its communication profile. Indeed, if an attack has succeeded and a device is effectively compromised, then the device may very well continue to perform its functions, slightly altering its behavior. If the device's incorrect behavior has physical consequences, those will either be immediately detected or may go unnoticed until a manual inspection is performed. However, if said device communicates over the network, the content of its messages, their frequency, and the recipients may become very different from what they used to look like.

Defining what normality looks like and being able to quantify how different observations are from that "normality envelope" thus offers a way to detect anomalies and raise an alarm when significant discrepancies are measured.

Communication graphs A communication graph represents who communicates with whom. This is a directed graph as communication profiles vary depending on the direction of the messages. Nodes represent a process on a given device. The usual way to identify them is through the tuple (IP address, port number), i.e a socket. Arcs represent whether two processes communicate or not over a given period of time. Arcs may be annotated with the expected amount of data exchanged over the period.

High deviation from the expected data exchange indicates that something atypical for the given time period is going on and an alarm should likely be raised. In particular, communication between two sockets that do not usually communicate (over the time period or at all) is particularly interesting to detect as it is exactly the kind of behavior that would be observed if an attacker used that device has an entry point to access and infect others.

Traffic envelopes It may be of interest to look at other parameters than the amount of data that is being sent between hosts or processes. SCADA traffic is susceptible to present a lot of patterns that may be detected depending on the actual supply and demand mechanics of the electrical market.

Defining a general traffic envelope, frequency of data bursts, time location of bursts, amount of data exchanged, etc. can help define a very precise communication profile. This can be done at several levels: traffic between two processes, two hosts, on a given data bus, etc. If the traffic is regular enough to define such envelopes, they may be a very precise tool for anomaly detection.

Polymorphic systems

An idea to reduce the aftermath of successful attacks would be to design systems so that compromising a given (cyber) component offers little ability to compromise others. The concept of polymorphic systems, that we wish to introduce, can be stated as such: "A given system appears differently depending on the current context and the observer."

Let us enumerate a few examples to clarify what this means and how such a system may be beneficial in the context of power systems.

- Polymorphic filesystem A polymorphic filesystem is a filesystem that appears differently to (potentially) each process that requires access to the arborescence. For example, applications could have a limited

view of the filesystem depending on how they were installed. One could also imagine incorporating some redundancy, e.g. several copies of a file, versioning, into the filesystem so that malicious actions from a given process (e.g crypto lockers) cannot affect the others.

- Polymorphic networks Software-Defined Networking (SDN) decouples routing (control plane) and forwarding (data plane) of packets in a given network [16]. In an SDN network, the physical topology does not define who can communicate with whom, the programmable controller does.

  In a classical network, any physical port from any host machine allows communication with any open software port (socket) of any host of the network. In a polymorphic network, this would not necessarily be the case. One could imagine to only allow communication that usually happens (no anomaly detected) but prevents atypical communication or communication between machines that should not be exchanging information.

  In simple terms, SDN allows defining of a flexible, programmable, virtual network topology over an existing physical topology. This flexibility allows establishing virtual connections between machines that should communicate while leaving machines that should not unable to do so even while they are physically connected.

- Polymorphic firewall A firewall could exist in the form of a physical gateway device but also replicated in the form of rules inside of programmable SDN switches. In this way, if the main device gets taken down, (filtered) communication would not be prevented, as it would be rerouted through the programmable switches that would apply the same rules as the firewall prior to forwarding packets.

5

Conclusion, Further Work & Challenges

Task 1.2 consisted of the preliminary work necessary to bootstrap the tasks of further work packages. Its aim consisted in identifying the various hardware and software components that make up the power grid and how they may fail or be compromised. It identified a list of relevant cyber-physical threats, categorized them, and provided useful abstractions. In addition, first thoughts on countermeasures were provided. This is the basis for further tasks of risk assessment, simulations, and for the study and design of countermeasures against the undesirable scenarios that these threats may cause. According to the needs of the tasks to be performed in the following work packages, the concepts explored in this document will need some refining and specialization but they offer nevertheless an essential common basis.

The second chapter of this document introduced the important subsystems to consider, a list of tasks they accomplish, and the sensing and actuating actions they can perform on the physical part of the system. This consists in an essential basis for the building of the co-simulation platform as those represent the action space of the cyber part on the physical part, i.e. the set of interactions between both parts of the system. A list of relevant cyber-components to characterize was also provided as a direct input to task 1.3. In addition, the Cyber-Space as Services (CSaS) framework, which regroups components into meaningful sets of services by functionality was introduced. This model is relevant for the conception of the simulations of the cyber part of the system as it provides functional abstractions that can be used to abstract away low-level details which are difficult to simulate but not relevant to the outcome of the simulation.

Chapter 3 introduced a methodology for threat modeling and evaluation. As part of this methodology, a way for categorizing threats is necessary. A way to provide such categorization is the STRIDE methodology, which is commonly used in the context of cybersecurity. STRIDE was studied and was found to lack some important characteristics. In order to apply STRIDE to a given system, all of its assets must be identified and fully specified. Further work based on STRIDE could be performed on very specific system configurations and could be used to identify specific vulnerabilities, e.g. through the use of penetration testing. This may offer very pertinent information for risk assessment, although this approach will yield far from exhaustive results.

Alternatively, another approach for threat categorization based on the CSaS model was introduced. The quality of a given service can be quantified through Quality of Service (QoS) metrics, which empower the modeling

of threats as a disruptor in the quality of one or several services. This approach offers a very relevant basis for building the co-simulation platform. Indeed, in order for these simulations to be as close to exhaustive as possible in the threat scenarios they consider, there is a need for abstracting some details away. Essentially, the CSaS model and its QoS metrics offer a way to regroup threat scenarios that will bear the same consequences on the overall system into a single case to simulate.

A large but non-exhaustive set of threats have been identified in chapter 3. Explicitly considering each of them in the context of CYPRESS may be difficult. However, since all of these threats are likely and of direct interest for the security of the system, it would be risky to exclude some of them to select a more manageable subset for risk assessment. However, in the context of the CSaS abstraction, many of these threats impact the same QoS metrics. Thus, a representative subset of threats can be selected by only keeping an arbitrary threat per combination of affected QoS metrics.

Chapter 4 discussed generic cybersecurity principles and how they can easily be implemented. Further work dedicated to proposing barriers and countermeasures should always rely on these basic techniques as a basis. Most power systems protocols were not designed for security as their use was supposed to be restricted to private networks. They should thus be used on top of a basic end-to-end secure communication channel, e.g. TLS, such as was discussed in the first section of Chapter 4. Additionally, as discussed in the second section of Chapter 4, the proper use of cybersecurity measures may not be sufficient to guarantee that no component can be compromised. Mitigation techniques based on anomaly detection and polymorphic systems should thus be explored to ensure that any breach or failure remains localized and under control.

Bibliography

[1] M. Garcı a-Valls, A. Dubey, and V. Botti, "Introducing the new paradigm of social dispersed computing: Applications, technologies and challenges," *Journal of Systems Architecture*, vol. 91, pp. 83–102, 2018.

[2] E. Karangelos, K. Thoelen, F. Faghihi, *et al.*, "CYPRESS: Report D1.1 describing the selected performance metrics," p. 94,

[3] T. Van Cutsem, *Notes du cours elec0014, introduction to electric power and energy systems*, Sep. 2019.

[4] "Balancing Service Provider (BSP)," EUROPEAN UNION EMISSIONS TRADING SCHEME – LEGAL POINT OF VIEW. (2021), [Online]. Available: `https://www.emissions-euets.com/balancing-service-provider-bsp`.

[5] "Undervoltage Protection (ANSI 27)," Schneider Electric. (2020), [Online]. Available: `https://product-help.schneider-electric.com/ED/MTZ/Micrologic_X_User_Guide/EDMS/DOCA0102EN/DOCA0102xx/ProtectionFunctions/ProtectionFunctions-15.htm`.

[6] "Keeping the balance," Elia. (2021), [Online]. Available: `https://www.elia.be/en/electricity-market-and-system/system-services/keeping-the-balance`.

[7] A. Summers, J. Johnson, R. Darbali-Zamora, C. Hansen, J. Anandan, and C. Showalter, "A comparison of DER voltage regulation technologies using real-time simulations," *Energies*, vol. 13, no. 14, p. 3562, 2020.

[8] *Boiler tubes temperature monitoring system*, Masibus Automation and Instrumentation Pvt. Ltd, 2019. [Online]. Available: `https://www.masibus.com/solutions-by-application/scada/boiler-tubes-temperature-monitoring-system/`.

[9] *Redispatch*, 50 Hertz - Elia Group. [Online]. Available: `https://www.50hertz.com/en/Grid/Systemcontrol/Redispatch`.

[10] P. Goossens and C. Moors, *A short introduction to protection and automation philosophy*, [Lecture slides during Université de Liège's lesson "Electric power systems analysis"], Elia, 2020. [Online]. Available: `https://thierryvancutsem.github.io/home/elec0029/PAC%20-%20ULg%20-%20v6.pdf`.

[11] J. De Kock and C. Strauss, *Practical power distribution for industry*. Elsevier, 2004.

[12] M. Proctor, "Application of undervoltage protection to critical motors," in *2018 71st Annual Conference for Protective Relay Engineers (CPRE)*, IEEE, 2018, pp. 1–6.

[13] P. Zhang, *Industrial control technology: a handbook for engineers and researchers*. William Andrew, 2008.

[14] N. Egi, A. Greenhalgh, M. Handley, M. Hoerdt, F. Huici, and L. Mathy, "Towards high performance virtual routers on commodity hardware," in *Proceedings of the 2008 ACM CoNEXT Conference*, 2008, pp. 1–12.

[15] M. Yang, F. Dong, D. Shen, Y. Zhai, and C. Chen, "A cpu load-awared virtual router placement strategy in cloud network," in *2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, IEEE, 2021, pp. 690–695.

[16] J. F. Kurose and K. W. Ross, *Computer Networking: A Top-Down Approach*, 7th. USA: Pearson, 2017, ISBN: 0136079679, 9780136079675.

[17] L. E. Frenzel, "Chapter one-introduction to serial i/o communications," *Handbook of Serial Communications Interfaces*, pp. 1–3, 2016.

[18] M. S. Thomas and J. D. McDonald, *Power system SCADA and smart grids*. CRC Press, 2015.

[19] K. C. Budka, J. G. Deshpande, and M. Thottan, *Communication Networks for Smart Grids*, en, ser. Computer Communications and Networks. London: Springer London, 2014, ISBN: 978-1-4471-6301-5 978-1-4471-6302-2. DOI: 10.1007/978-1-4471-6302-2. [Online]. Available: http://link.springer.com/10.1007/978-1-4471-6302-2 (visited on 07/07/2021).

[20] S. W. Brim and B. E. Carpenter, *Middleboxes: Taxonomy and Issues*, RFC 3234, Feb. 2002. DOI: 10.17487/RFC3234. [Online]. Available: https://rfc-editor.org/rfc/rfc3234.txt.

[21] R. B. Thompson, "Global Positioning System: The Mathematics of GPS Receivers," *Mathematics Magazine*, vol. 71, no. 4, pp. 260–269, 1998, ISSN: 0025570X, 19300980. [Online]. Available: http://www.jstor.org/stable/2690697.

[22] *NTP: The Network Time Protocol: documentation*. The Network Time Foundation. [Online]. Available: http://www.ntp.org/ntpfaq/NTP-s-algo.htm.

[23] M. Goodrich and R. Tamassia, *Introduction to Computer Security*, 2nd. Pearson, 2018, ISBN: 0133575470.

[24] J. Andress, "Chapter 10 - network security," in *The Basics of Information Security (Second Edition)*, Second Edition, Boston: Syngress, 2014, pp. 151–169, ISBN: 978-0-12-800744-0. DOI: https://doi.org/10.1016/B978-0-12-800744-0.00010-5. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780128007440000105.

[25] "Experion's Data Concentrator," en, p. 4, [Online]. Available: https://www.honeywellprocess.com/library/marketing/notes/experion-data-concentrator.pdf.

[26] Y. Liang and R. Campbell, "Understanding and Simulating the IEC 61850 Standard," May 2008.

[27] D. Baigent, M. Adamiak, and R. Mackiewicz, "IEC 61850 communication networks and systems in substations: An overview for users," *Protection & control*, vol. 8, pp. 61–68, 2009.

[28] M. P. Barrett, "Framework for improving critical infrastructure cybersecurity," *National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep*, 2018.

[29] D. J. Bodeau, C. D. McCollum, and D. B. Fox, "Cyber threat modeling: Survey, assessment, and representative framework," MITRE CORP MCLEAN VA MCLEAN, Tech. Rep., 2018.

[30] L. Ablon, *Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data*. Santa Monica, CA: RAND Corporation, 2018. DOI: 10.7249/CT490.

[31] *NIST 7168 - Guidelines for Smart Grid Cybersecurity*. National Institute of Standards and technologies, Sep. 2014. [Online]. Available: https://csrc.nist.gov/publications/detail/nistir/7628/rev-1/final.

[32] *Cyber threat and cyber threat actors*. Canadian Centre for Cyber Security, Jun. 2021. [Online]. Available: https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors.

[33] *STRIDE reference sheet*. Open Web Application Security Project. [Online]. Available: https://owasp.org/www-pdf-archive/STRIDE_Reference_Sheets.pdf.

[34] B. Schneier, "Attack trees," *Dr Dobb's Journal*, vol. 24, no. 12, 1999. [Online]. Available: https://www.schneier.com/academic/archives/1999/12/attack_trees.html.

[35] M. Howard and D. LeBlanc, *Writing secure code*. Pearson Education, 2003.

[36] J.-P. Chavas, "Risk analysis in theory and practice," in Boston: Academic Press, 2004, ISBN: 978-0-12-170621-0. DOI: https://doi.org/10.1016/B978-012170621-0.50000-6.

[37] *Best practices for dam safety: Semi-quantitative risk analysis*. United States Bureau of Reclamation. [Online]. Available: https://www.usbr.gov/ssle/damsafety/risk/BestPractices/Chapters/A4-Semi-QuantitativeRiskAnalysis.pdf.

[38] R. Leszczyna, *Cybersecurity in the Electricity Sector: Managing Critical Infrastructure*. Springer, 2019, ISBN: 9783030195397. [Online]. Available: https://books.google.be/books?id=F-BJzAEACAAJ.

[39] A. M. Turing, "On computable numbers, with an application to the Entscheidungsproblem," *Proceedings of the London Mathematical Society*, vol. 2, no. 42, pp. 230–265, 1936. [Online]. Available: https://www.cs.virginia.edu/~robins/Turing_Paper_1936.pdf.

[40] C. W. Kaufman, R. Perlman, and M. Speciner, *Network Security: Private Communication in a Public World*. Englewood Cliffs, New Jersey: Prentice-Hall, Mar. 1995, ISBN: 0-13-061466-1.

[41] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th. Pearson, 2017, ISBN: 978-0134444284.

[42] P. Eronen and H. Tschofenig, "Pre-shared key ciphersuites for transport layer security (tls)," IETF, RFC 4279, Dec. 2005. [Online]. Available: `https://datatracker.ietf.org/doc/html/rfc4279`.

[43] L.-S. Huang, S. Adhikarla, D. Boneh, and C. Jackson, "An experimental study of tls forward secrecy deployments," *IEEE Internet Computing*, vol. 18, no. 6, pp. 43–51, 2014. DOI: `10.1109/MIC.2014.86`.

[44] K. P. Singh and S. Dod, "An Efficient Hardware design and Implementation of Advanced Encryption Standard (AES) Algorithm," *International Journal of Recent Advances in Engineering & Technology*, vol. 4, no. 2, pp. 5–9, Feb. 2016. DOI: `10.5281/zenodo.48483`. [Online]. Available: `https://doi.org/10.5281/zenodo.48483`.

This project is supported by the Belgian Energy Transition Funds

CYPRESS