Vaasan yliopisto
UNIVERSITY OF VAASA

Österbottens förbund
Pohjanmaan liitto

Regional Council
of Ostrobothnia

Technical Report TR 5.1

Cabled and Wireless Communication Security in Electricity Generation and Distribution Systems

Vaasa Energy Business Innovation Center
VEBIC

Smart Energy Systems Research Platform
SESP

Bahaa Eltahawy

Disclaimer

This document is for general use only, and by no means replaces the existing technical reports and/or standards from the main authority organizations. As well, the work has been done as vendor-neutral, and any references to specific manufacturers are just for exemplification matters only. Finally, this work is under continuous development, and changes might occur between this version and the published version.

Table of contents

Abbreviations

3G	3rd Generation Project
4G	4th Generation Long Term Evolution LTE
5G	5th Generation Project
AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
ACS	Access Control System
AD	Active Directory
AES	Advanced Encryption System
APN	Access Point Name
AV	Anti-Virus
C	Chef
CAN	Campus Area Network
CAT	Category
CB	Critical Business Application
CCMP	Counter Mode – Cipher Block Chaining – Message Authentication Code-Protocol
CCTV	Closed Circuit Television
CEA	Cybersecurity Enhancement Act
CI	Computer Installation
CIA	Confidentiality, Integrity, and Availability
COBIT	Control Objectives for Information and Related Technologies
CSA	Canadian Standard Association
CSF	Cybersecurity Framework
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DLP	Data Loss Prevention
DMZ	Dematerialized Zone
DNS	Domain Name Server
DoS	Denial of Service
EAP	Extensible Authentication Protocol
EMS	Energy Management System
EO	Executive Officer
ESS	The Electronic Security Systems
EU	European Union
FI	Federated Identity
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
FTPS	File Transfer Protocol – Secure

FW	Firewall
GP	Group Policy
HPE	Hewlett Packard Enterprise
HSPD	Homeland Security Presidential Directive
HT	High Throughput
HTTP	Hyper Text Transfer Protocol
HTTPS	Secure Hyper Text Transfer Protocol
IACS	Industrial Automation and Control Systems
IBM	International Business Machines
ICMP	Internet Control Message Protocol
ICT	Information and Communication Technologies
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
InfoSec	Information Security
IP	Internet Protocol
IPDRR	Identify, Protect, Detect, Respond, and Recover
IPS	Intrusion Prevention System
IS	Information Security
IS	Information Systems
IS	Intercommunications System
ISACA	International Systems Audit and Control Association
ISF	Information Security Forum
ISM	Industrial, Scientific, and Medical
ISO	Independent System Operator
ISO	International Organization for Standardization
IT	Information Technology
IV	Initialization Vector
L	Layer
L	Level
LAN	Local Area Network
MAC	Media Access Control
MAN	Metropolitan Area Network
MCS	Modulation and Coding Scheme
MFA	Multi-Factor Authentication
MIMO	Multiple In, Multiple Out
MitM	Man in the Middle
MU	Multi User
N/A	Not Applicable

NAC	Network Access Control
NAT	Network Access Translation
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
NW	Network
Ops	Operations
OSA	Open System Authentication
OSI	Open System Interconnection
PBAC	Port-Based Access Control
PIN	Personal Identity Number
PKI	Public Key Infrastructure
PSK	Pre-shared Key
QAM	Quadrature Amplitude Modulation
RC	Ron’s Code
RF	Radio Frequency
RFID	Radio Frequency Identification
RSA	Rivest, Shamir, and Adelman, as their names
RSN	Robust Security Network
RTO	Regional Transport Office
S	Secure
SANS	The SysAdmin, Audit, Network, and Security Institute
SCADA	Supervisory Control and Data Acquisition
SCC	Security Control Center
SD	Security Development
SES	Smart Energy Systems
SESP	Smart Energy Systems Research Platform
SFTP	Secure File Transfer Protocol
SG	Smart Grid
SGI	Short Guard Interval
SM	Security Management
SME	Small Medium Enterprise
SMS	Short Message Service
SoGP	Standard of Good Practice
SOHO	Small Office Home Office
SS	Scanning Systems
SS	Surveillance Systems
SSL	Secure Socket Layer
SSO	Single Sign On
SYN	Synchronize

TCP	Transport Control Protocol
TKIP	Temporal Key Integrity Protocol
TR	Technical Report
UDP	User Datagram Protocol
UE	User Environment
URL	Uniform Resource Locator
VEBIC	Vaasa Energy Business Innovation Center
VHT	Very High Throughput
VPN	Virtual Private Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
Wi-Fi	A marketing term associated to IEEE 802.11 technology
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WP	Work Package
WPA	Wi-Fi Protected Access
WPAN	Wireless Personal Area

Executive Summary

The energy sector is proceeding with the replacement of the traditional power grids by the more advanced smart grid systems. This transition is beneficial in many ways, for instance maintaining resources, integrating renewables, enabling and integrating other services, and finally cost control and cost reduction. This fits well with the economic and energy sector's plans of Finland as well as the European Union. However, the introduced smartness does not come with no paid costs; in fact, it costs much of the increased systems' complexities, and on top the exposure to the whole can of cybersecurity threats. With the cyberspace rapidly growing, should devices be isolated! With the demand to connect, integrate, and control billions of devices simultaneously, and with the use of the same communication protocols, risks are more common to happen than ever before, and any minor actions could drastically affect the whole system's functionality. For these reasons, cybersecurity arises.

Cybersecurity targets these complex systems, to make sure they are up running and well-functioning, while being free of risks and threats. Cybersecurity gives the measures and the recommendations to address the existing functionality and protection issues, follows the common practices and the advanced technologies, and provides for a secure digital environment. It is not only conceptual; cybersecurity is all about the successful blend between Information Security IS, technologies, people, and the risk management processes.

Many acts and authorities target cybersecurity, as the American Congress, National Institute of Standards and Technology NIST, Internet Engineering Task Force IETF, International Electrotechnical Commission IEC, International Organization for Standardization ISO, and others. These acts and organizations have the same target in concept; however, they provide for more perspective solutions, and for different practical implementations according to certain criteria. Different models are introduced within the given standards; however, they all share the same fundamental security foundation practices. This report as well follows the same theme.

In this report, the topic of cybersecurity is addressed, with the view from the smart energy systems considered. The main goal of this work is to introduce a comprehensive guideline that gathers all the required security concepts and practices in one place, thus to help professionals in the energy sector to securely implement a networked environment. Here, we introduced the concepts under interest, used the previous knowledge to provide for a collective practical solution, and we targeted robustness. The report focuses mainly on three aspects, the security as a process in general, cabled communication security, and finally wireless security. The report beings with the security fundamentals, and concludes by giving the recommended practices on how to apply these concepts. Additionally, an indices section is included, where the abstracts of the main standards from the main bodies and their recommended practices are presented.

Case Description

Smart Energy Systems SES and Smart Grids SGs are the future of energy. They enable integration of different energy sources with the renewable ones, and they incorporate the ICT technologies to create an adequate level of smartness to achieve high level of optimization and performance. In Smart Energy Systems Research Platform SESP, these systems are simulated by creating SES and SG models, then applying the real case scenarios that the network might go through, in aim for improved results, and a final product that is more feasible and applicable. The project is run as nine Work Packages WPs, in which each WP concerns a specific area of interest, to provide altogether for a complete solution from all perspectives. Many topics are covered here, and while energy distribution, programming, data storage, business outcomes, and sustainability are studied in other WPs, Information Security InfoSec is the main focus of WP5. In this report and the proceeding ones entitled TR5.x, different InfoSec cases are studied, reported, and recommendations are given.

Objective

The objective of this work is to form a general guideline for wired and wireless implementation, and to guide the cooperating energy-sector companies under Vaasa Energy and Business Innovation Center VEBIC to a secure communication. This guideline forms the state of art for the current cybersecurity situation, and continues by giving recommendations that would address the found threats. The given recommendations are based on the conducted risk and security assessment and the IS technologies, and they go coherent with the standards, as well as the main regulatory authority organizations.

Scope

The scope of this report concerns the technical, operational, and management surfaces, that form the base for the wired and wireless communication. Cooperating organizations might implement the measures they find matching with their interest and the level of protection they seek.

Here we generally consider the wired and wireless communication’s protocols and means that could be utilized by the industry. This includes but not limited to IEEE 802.3 Local Area Network LAN Ethernet, IEEE 802.11 Wireless Local Area Network WLAN Wi-Fi technologies, Wireless Metropolitan Area Network WMAN, and Wide Area Networks WAN, with all the mobile communication and remote connections technologies included.

Audience

This report concerns those who work in the energy sector, SGs, and the development of SESs. The targeted personnel are:

- Developers, implementers, and who assess LAN and WLANs.
- Administrators, designers, and network analysts.
- Information and network security personnel.
- Auditors, officers, consultants, and the higher Chef "C" level bodies.

Document Structure

The report starts with general introductions to SGs and SESs, and the way that they are built, then it continues towards its goal by explaining security and the measures required achieving it. It continues after with a complete section concerning physical security, and then the distinction between cybersecurity and InfoSec is explained. The section after targets threat analysis, describing vulnerabilities, threats, and attacks. Later security architecture models within an enterprise are proposed, followed by the wired and wireless network practices. Finally, appendices of the standards are given.

1 Introduction to Energy Systems

1.1 Smart Energy Systems

SESP project concerns SESs and the means to develop them in the most efficient way. In contrast to the traditional energy solutions that depend on fossil sources to provide the required energy on demand bases, SES deals with renewable resources as wind, hydroelectricity, and solar power. However, since these renewable resources are limited and not suitable for all places, purposes, and times, the designed system need to be flexible enough to replace the fossil-dependent system without trading off service and performance levels. Figure 1 is an example of a typical SES network. As seen, the system is of high complexity; yet it goes with the themes and goals of the EU, to integrate more renewable energy resources, until fully replacing fossil systems.

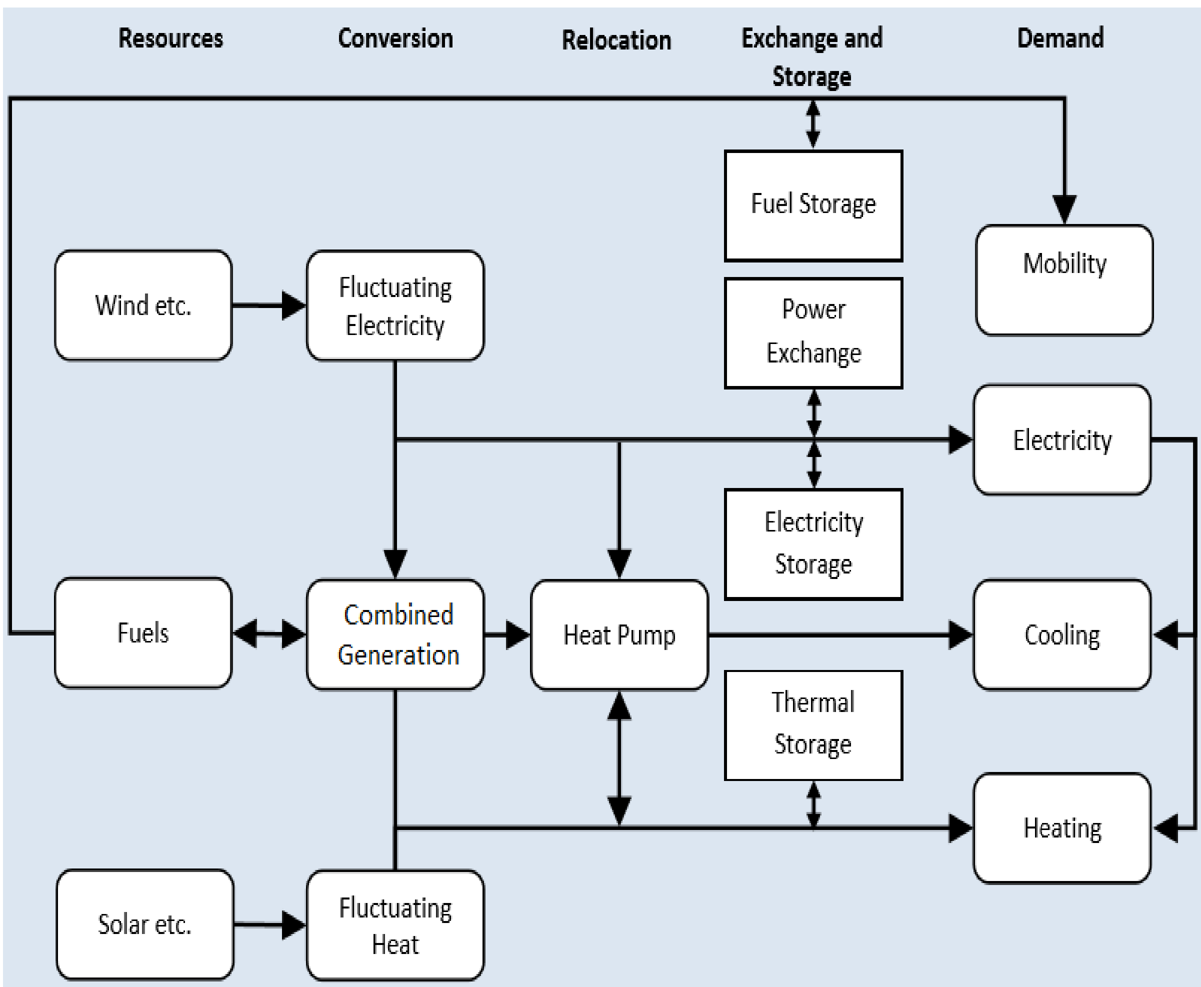

Figure 1: Smart Energy System network

1.2 Smart Grid Systems

To be able to build such system as in Figure 1, the distribution system also needs to be upgraded. Thanks to the Information and Communication Technologies ICT for enabling the concept of Smart Grid. Smart Grid SG is the future of the traditional power distribution system, featuring the ability to optimize electricity distribution according to usage by means of utilizing the high-end ICT techniques. Such system benefits from the reduced costs, energy savings, Carbon emission reduction, and a higher efficiency. On the other hand, firstly SG is not an easy implementation, as many components and layers are included within, as shown in Figure 2. Secondly, SG needs to collect information about users and their usage patterns to optimize the energy distribution and costs. This could result in completely new issues of privacy invasion. Thirdly, many parties cooperate to make the SG function as intended, and hence it differs from the older and traditional distribution company. Fourthly and finally, SG is all about data acquisition, analytics, and the massive data generated. For these reasons and many others the design of SG systems should be done carefully at a prior stage, thus to ensure functionality, serviceability, and an adequate level of protection for all of the involved parties.

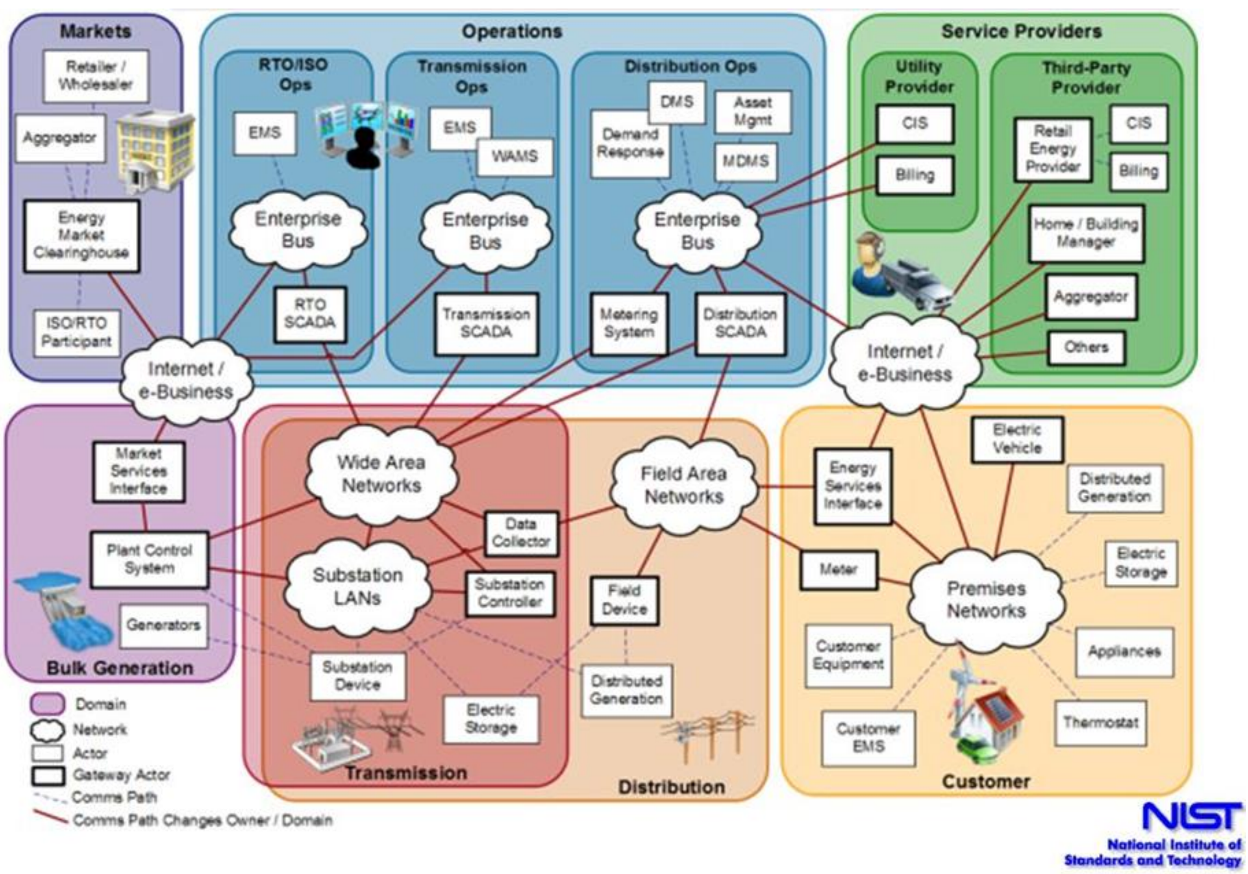

Figure 2: Smart Grid architecture model, NIST

2 Introduction to Security

2.1 Protection Levels

Protection is a generic term that can describe many concepts within. However, protection's actual meaning can be described using one of the three terms, safety, security, or privacy. In Figure 3, a hierarchical relationship between the given levels is established. As shown, safety is the foundation for protection, by providing measures against accidental and unintentional danger, while security comes at a higher level, to deal rather with intentionality and the causal means for danger. At the top, privacy provides for absolute protection, by concerning advanced measures to protect the freedom of individuals from all sorts of unauthorized intrusion or the public's attention. *It is worth mentioning that privacy is however not absolute or not achievable yet in practice.*

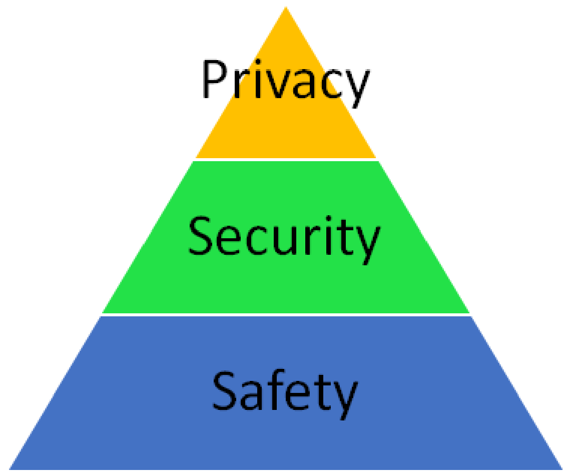

Figure 3: Different levels of protection

2.2 Security Models

Many models exist to disassemble security to its main elements. The most fundamental security model comprises of three elements, namely Confidentiality, Integrity, and Availability, as in CIA. Other models as the Parkerian Hexad and the ISO model suggested more elements to the security process. Hereafter, definitions of the security elements are given, as we will use them frequently across this report.

CIA Model:

1. Availability is the readiness and reliability for resources to be accessed and used when needed.
2. Confidentiality is the property of information that is not made available or disclosed to unauthorized individuals, entities, or processes.
3. Integrity is the consistency and the assurance of data against any sort of modification or alternation.

Parker:

4. Utility refers to the usefulness, and worthiness of the exchanged data, that is by making sure they follow the right format and the standards.
5. Data possession, or control protection concerns protecting and controlling information in the physical assets, i.e. communication devices.
6. Authentication, Authorization, and Accounting (AAA) concepts provide means to identify users and approve their permissible activities. Authentication mechanisms validate the user's identity; authorization validates the privileges, services, permissions, and resources assigned to the user; and then finally accounting keeps tracking of the user's activities for further considerations.

ISO:

7. Repudiation is the denial by one of the entities involved in a communication of having participated in all or part of the communication. Non-repudiation is required to prevent an entity from denying their communication activities.

The importance of the given elements depends solely on the application, as these elements apply to physical, personal, industrial, operations and management, communications, network, information, and data security. For instance: office security views focuses more on confidentiality than availability, while industrial security in contrast concerns availability of resources and services than confidentiality. As a result, it is clear the need to define precisely the scope of applicability, thus to match the right level of protection.

Siemens AG Recommendations

Siemens proposes layered security architecture to protect automation plants, as in Figure 4. In their proposal, physical security comes as the outermost shell that prevents outsiders from gaining access or reaching out critical components. In the next layer, network and office security measures come into practice, by controlling interfaces, protocols, devices, and performing isolation and segmentation. The next protection

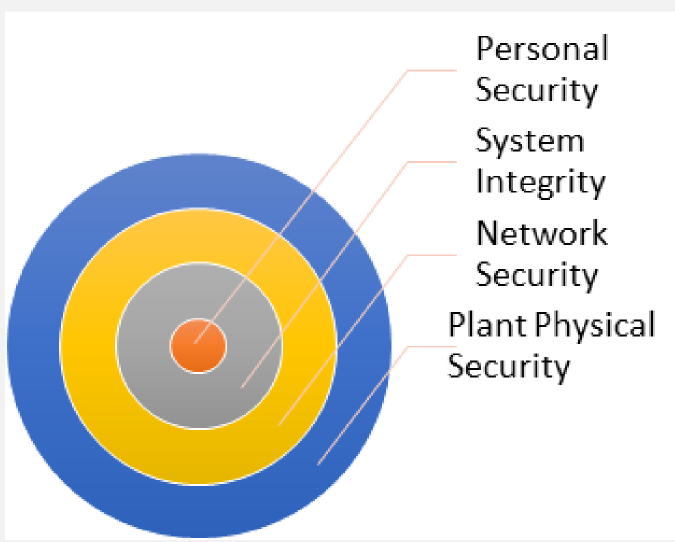

Figure 4: Siemens layered security architecture

layer, system integrity, comes to protect Operating Systems OSs, data, backup, software, updates, batching, antivirus, and malware. Finally, the core protection comprises of agreements, policies enforcement, training, and other personal security measures. Siemens suggests the following requirements for industrial security:

1. 24/7/ 365 availability.
2. Open standards for seamless communication.
3. Common automation standards.
4. Performance, operability, and real-time monitoring measures.
5. Protection against faults and damage.
6. System and data integrity.
7. Real-time data transfer.
8. Logs for change management.

Before we proceed to the main further, we briefly will go through the following simple attack scenario.

Simple attack scenarios

1. The highest measures of security are applied, however an employee got access to a laptop that contains critical information. He could not access the system, but instead he could shut down the device and remove the hard disk, for further actions later>>>>> Physical and Information Security
2. Two visitors got access to different buildings, then while being unwatched they exchanged their access tokens, which allows them to access the unauthorized buildings>>>>> Physical Security
3. An employee shares his connection from his legitimate device by means of a bridge or a switch device >>>>> Information and device Security, and misconfiguration
4. An authorized person stays during the off hours, then leaving on the next on hours, thus gaining unauthorized access without being questioned>>>>> Access control misconfiguration
5. Monitoring a firm, to collect valuable information about activities scheduling, rush hours, and the best times to run an intrusion attack>>>>> Monitoring and Physical Security
6. …

The given examples are of such simplicity that they can occur at many organizations. However, these could never happen if physical security is well placed. The SysAdmin, Audit, Network, and Security SANS institute's paper titled "Physical Security and Why It Is Important" explicitly states that no matter which security measures are applied, physical security remains the ultimate and absolute foundation for the whole security process. The next section briefly goes over the physical security components and the security design program.

2.3 Physical Security

"Physical Security is that part of security concerned with physical measures designed to safeguard people, to prevent unauthorized access to equipment, facilities, materials and documents, and to safeguard against damage and loss". The Electronic Security Systems ESS comprises of all means that can secure a place physically. These include systems that are able to record events, detect activities, prevent access, and send alarms when preset conditions are triggered. The ESS includes but not limited to Fences, Scanning Systems SS, Access Control System ACS, Intrusion Detection System IDS, Surveillance Systems SS, and Intercommunications System IS. These systems are integrated together with the other safety system from the Security Control Center SCC room that includes all the control systems. Systems should be connected to perform the required level of identification and verification, so that they comply with the Homeland Security Presidential Directive HSPD-12, and Federal Information Processing Standard FIPS-201 requirements.

We will not go over details here, but rather we proceed to results. From the "Best Practices" guidelines, combining recommendations of the top standardization organizations, as the National Institute of Standards and Technology NIST, Canadian Standard Association CSA, International Systems Audit and Control Association ISACA, and SANS, we present the tools required to maintain physical security in the Table 1, and we classify them into three categories, Facility, Assets, and Transport.

Table 1: Physical Security Measures

PHYSICAL SECURITY	FACILITY	Gateways and Entry Points	Employee Entry/Exit	
		Visitors Entry/Exit	Lighting Systems	Locking Systems
		Identification Methods	Segmentation	Authorization
		Perimeter Security	Access Control	
		Motion Detection	Surveillance Camera Systems	
		Monitoring and Positioning Systems	Alarms	
	ASSET	Counting	Tracking	Disposals
		Other assets	Labelling	Packaging

These systems are defined as following:

- Gateways and Entry Points Systems: To secure the areas where entry is possible.
- Employee Entry/Exit: The system that manages employee access, this normally is an automatic system to record and ease the entry/exit process.
- Visitors Entry/Exit: It is a separate system to check visitors, the purpose of the visit, the host, and the related security requirements.
- Lighting systems: To provide the minimum required illumination to the pathways, thus to enhance security, and to help other services to well function.
- Identification Systems: To provide employee and visitors with identification tags, so that others would know immediately about the personnel functional level. In addition, to automate the access process by implementing identification criteria as smart tags, or biometric means.
- Segmentation: To partition an organization into smaller areas, thus to perform an adequate level of restriction.
- Authorization: To give the right privileges to the right personnel, according to their job title, task, and functional level.
- Perimeter Security: To implement controls to mitigate outer risks. This concerns defining the functional borders, deploying the means to stop the unauthorized access, and taking measures against malicious activities that can run from outside while affecting components inside the firm.
- Access Control: To implement electronic control on all entry/exit points where critical content is present.
- Motion detection: To detect any activity and relate it to the time and space, thus helping to determine malicious activities for reporting and alarming.
- Surveillance Camera Systems: For recording events for further investigation, identification, verification, and a means of proof as required by the authority organizations.
- Monitoring and Positioning Systems: Radio Frequency Identification RFID tags and monitoring systems, to reach out personnel and to know about their location and current activities upon needs.
- Alarms: To function as a warning system. This can take the form of siren, automated SMS, or a recorded call to the personnel in charge or the action authority.
- Locking systems: To centrally lock or unlock the entries and gates upon preset threat criteria triggered.
- Counting: To keep record of the inventory components up-to-date.
- Tracking: to track all inventory and devices, thus to locate items with the least effort, and ensuring all devices are achievable when needed.
- Disposals: The system that handles all damaged or rejected items, thus to protect against them being mixed with the legitimate devices.

- Other assets: To isolate and store other items, like own personnel items that should not be allowed in. This helps mitigating malicious replacements.
- Labelling: The system that performs tagging, so that information can be easily extracted about the different items when required.
- Packaging: To ensure the ordered items were not replaced, that is by performing the right means to protect packages including seals and secure containers.

The given measures and their applicability depend solely on the applied protection level, and the importance of the assets. In a following section, the topic of asset evaluation and risk management is discussed.

2.4 Information Security vs. Cybersecurity

Information Security InfoSec/IS aims protecting information in all forms either physically or electronically, by implementing the right means to prevent all sorts of destruction, modification, or the unauthorized access. InfoSec is generic in the context of protection, as it works against both malicious and accidental incidents. Accordingly, human errors, machines' failures, transactional errors, etc., are all included under the umbrella of InfoSec. InfoSec comprises of many domains, as shown in the Table 2 below.

Table 2: Information Security domains

InfoSec Domains ISO 27001	Security Policy
	Organization of information security
	Asset management
	Human resources security
	Physical and environmental security
	Communications and operations management
	Access control
	Information systems acquisition, development and maintenance
	Information security incident management
	Business continuity management
	Regulatory compliance

On the other hand, cybersecurity is a more generic term that encompass InfoSec within. Cybersecurity deals with all data and assets in all of their forms, to rather protect against malicious and intentional means, as well as to prevent risks. Many definitions exist for cybersecurity, and here we are concerning the one from the main dictionaries:

1. Merriam Webster: Cybersecurity is defined as the measures taken to protect a computer, or computer system (as on the Internet) against unauthorized access or attack.
2. Oxford: Cybersecurity is the state of being protected against the criminal, or the unauthorized use of electronic data.
3. Cambridge: Cybersecurity is the ways of protecting computer systems against threats such as viruses.

It is clear from these definitions that cybersecurity concerns only the digital means, as in information and networking. Hence, cybersecurity protects against all possible threats, taking the forms of the unauthorized access, attacks, and computer viruses. Still, cybersecurity is not only about security measures, it is rather an all-inclusive concept that incorporates risk assessment and governance measures as well, as discussed in the next chapter.

2.5 Cybersecurity Current State

In Figure 5, survey results of the general malicious activities occurred during of 2016, and the rate of occurrence are given. As seen, a large number of threats goes unrecognized, also aside from the intentionality, a large number of activities aim to cause damage, or to steal intellectual properties or identities for further consideration. In the next chapter, vulnerabilities, threats, and attacks are defined.

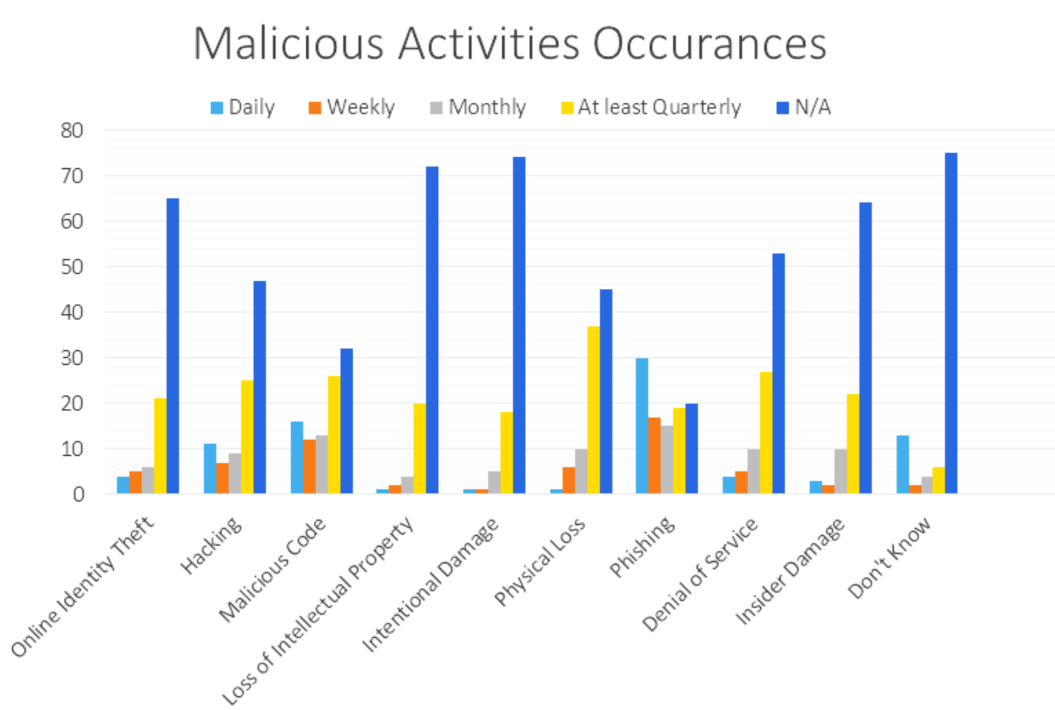

Figure 5: Cyber threats, as in 2016

3 Vulnerabilities, Threats, and Risks

3.1 Definitions

In many ways, the terms vulnerabilities, threats, risks, and attacks are mixed in many contexts. This consequently results in either misunderstanding, or in providing for a wrong solution when it comes to application. Here we are providing precise definition for these terms.

Table 3: Definitions

Asset	*"Something having value, such as a possession or property that is owned by a person, business, or organization".* Assets in an organization are the machinery, devices, people, and the valuable information, that need to be protected.
Vulnerability	"The quality or state of being exposed to the possibility of being attacked or harmed, (either physically or emotionally)". Here, vulnerability concerns the exposed area and the existing weaknesses.
Threat	"A person or thing likely to cause damage or danger". Threats result from the existing vulnerabilities being exploited.
Attack	"A violent act intended to hurt or damage someone or something". Attacks are intentional act to perform malicious activities, in the form of damage, access, or getting control over assets.
Risk	"The possibility that something will be harmed, damaged, or lost".

These can be formulated as following

Assets + Vulnerabilities = Threats
Threats + Attacks = Risks

Alternatively, *"All vulnerabilities should be identified, so that threats get mitigated, otherwise attacks will cause assets potential risks".*

3.2 Threat, Risk and Vulnerability Analysis

A threat, risk, and vulnerability analysis aims providing the adequate level of security to the network without sacrificing the functionality and operability levels. From the analyzing approach, there are two distinctive analysis that can be conducted, Risk Analysis, and Vulnerability Analysis. Risk Analysis is a general analysis that can be conducted on regular basis to find the main risks that might affect the network, enterprise, or the organization under investigation. On the other hand, Vulnerability Analysis is more specific and it works with predefined scenarios, thus the analysis defines what to be searched, but rather searches where it could apply. In any case, both analyses include assets identification/description, along with assets roles, impact, and importance. As well, they do specify the exposed surfaces and the possible weaknesses, and finally plan the strategies to protect against the threats and risks. Many systematic approaches exist on the way to conduct the analysis. In Figure 6, the practices we concern the most are combined and illustrated.

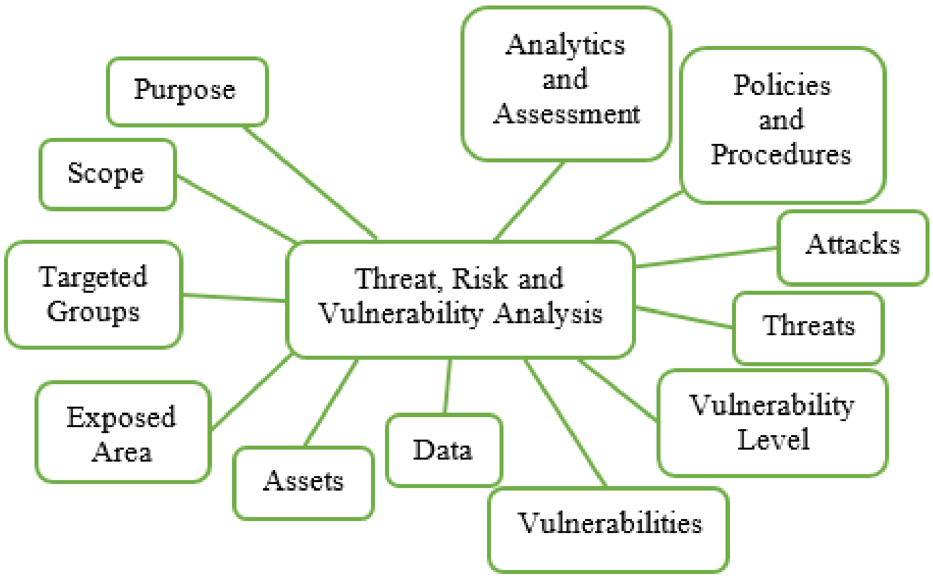

Figure 6: Threat, risk, and vulnerability analysis approache

3.2.1 Purpose

To define the explicit reasons, and intentions, for conducting the analysis. These could be regulatory auditing, regular follow-ups, discovery of new threats, performance check-up, ensuring functionality after settings modification, coping with other standards or regulatory authorities, or just a general evaluation process.

3.2.2 Scope

To set the boundaries, and limitations for the analysis process. The scope explicitly specifies what needs to be covered by the analysis, items that require protection, sensitivity and criticality, divisions, systems, applications, which regulatory organizations and standards to follow, and finally the targeted bodies by this assessment. Defining the scope in prior is of high importance, as it could save time consumed on other side tasks.

3.2.3 Targeted Group

The groups, and the associated risks that are under concern, should be specified in prior. This could help narrowing the analysis and set more restrictive criteria. Two approaches exist here, in which the first is to define a group of interest, then study which risks they are mostly to face, and with which norms. In the second approach, the process goes by specifying the risks, then finding out which groups might be affected by them. Groups here can mean anything, as it does not mean personnel only. Groups can be employees of different function levels, devices and appliances, organizations, divisions, or others.

3.2.4 Exposed Area

This specifies which parts of the network are more prone to malfunction or attacks. This in addition could specify the surface's importance level, which could be used for risk prioritization, and setting the acceptable risks' levels.

3.2.5 Assets

Assets are why the analysis is conducted, so that they could be protected. Assets do not need to mean systems and appliances only, but they also can mean information. Assets should be identified, labeled, revised, and updated information about them should be available.

3.2.6 Data

Data collection is important, as it provides documentation about the organization, the applied procedures, policies, and the adopted standards. The process will show which parts of the work are well functioning, and which parts still in need for revising. At this point, explicit agreements are required, as the process is also of privacy invasion, especially by knowing critical sensitive data, in addition to the functional levels of the divisions and personnel.

3.2.7 Vulnerabilities

Vulnerabilities are the weaknesses or holes that exist in a system, which can form easy access or damage with the least effort. Vulnerabilities with casual accidents are a major threat, while with attacks cause a serious risk. Vulnerabilities can be set into three categories, namely technical, configurational, or policy-related vulnerabilities. Table 4 gives an example of these vulnerabilities.

Table 4: Vulnerabilities categorization

Technical	Operating systems	Operating systems or service packs that are well known with flaws affecting security and data access.
	Protocols and ports	Across the OSI layers, some of the deployed protocols suffer from security problems, or lack security functions completely. This happens across many of the Application, Transport, and Network layers. For instance, FTP has two better alternatives that should be used instead, FTPS, and SFTP.
	Networking and Devices	Firstly, not all devices are suitable for all organizations, as devices are either consumer, Small-and-Medium-Business SMB, large-business, or Enterprise grade. Devices have different capacities and support different functions. Some devices are legacy, or lack the recommended security practices, with passwords or authentication criteria. In addition, some networking protocols have major flaws, which can be exploited to perform redirection attacks.
Configurational	Accounts	Information about accounts are exposed across the network.
	Servers	Servers are misconfigured, thus not applying the recommended security practices, or cause performance errors and delays.
	Defaults	Default settings kept without changing, letting others to change systems' configurations.
	Remote Access	Misconfigurations can let outsiders access the system, databases, storage, change settings, or cause general service disruption.
	Network	Misconfigured network devices, for example the segmentation and isolation can let wrong users to access the system, or to block legitimate ones. Other issues include authentication to the network, encryption of the traffic, access to configuration pages, and flaws in the access portal or redirection techniques.
Policy-related *(Policies in a later section)*	Authority or Division	Wrong/imprecise authority, or division of the standard, thus lacking the most adequate recommendations
	Agreements	Missing agreements, or lack of transparency

	Response and Actions	Response delays, and unclear counter actions
	Auditing and Monitoring	Continuous auditing and monitoring should be conducted on regular basis, either for evaluation or to shut any holes that might be found in the system
	Conflict of Interest	With the existence of multiple parties, it is crucial to make agreements about the different issues in prior, otherwise the conflict of interest between the different parties might cause serious issues.
	Change Management	Declaring how the change procedures are prepared, handled, and mentioning the tools and programs required for the process.
	Batching and Updates	Timely updates policies on regular basis, and upon high impact flaws discovery.
	Recovery plan	Plans for disasters and out of control situations, to perform recovery of the main assets, and to bring services to an acceptable level of functionality.
	Education, Training, and Awareness	People, work force, or employee, are a major key driver, thus awareness and training should be given, to ensure policy enforcement and compliance.

3.2.8 Vulnerability Level

One of the most effective approaches is to classify vulnerabilities according to their severity, and applicability area. This helps in prioritization of the mitigation actions, thus taking the right protection measures. In Figure 7, such categorization is performed. As illustrated, Vulnerabilities falling within the golden zone are the most common to occur, and they should be considered before the ones falling within the green zone, which are either less effective, or less occurring. On the other hand, the red zone is extremely severe and requires immediate intervention to fix the existing vulnerabilities before major risks coming into place.

3.2.9 Threats

Threat analysis is conducted after defining vulnerabilities and closing the security holes that might exist in a system. Threats are directly connected to damages and disruptions, affecting devices or the service in general. On the other hand, attacks are the intentional manipulation of the existing threats within the network. Threats can be categorized into two categories, namely internal or external, at which each can be further categorized into unstructured or structured threats. These are defined in Table 5 below.

Table 5: Threats categorization

Internal Threat	It happens by those who have rights to access a certain system, but they maliciously try to use these rights to gain more advantages, or to acquire information they are not supposed to acquire. Human factor and employees are main drive for threats, and they represent at least 60 percent of the threat.
External Threat	This happens by non-authorized ones from out of the organization accessing the network by Internet or simply trying to figure out communication, activities, or other valuable information. This forms directly an attacking threat, as discussed in the next section.
Unstructured Threat	It is conducted by personnel with low skills and using available tools, to break through the system or gain access to files or data. This threat is intentional but lacks the experience.
Structured Threat	It is conducted directly by hackers with intention, skills, tools, and experience. They perform high analysis to gain knowledge about the existing vulnerabilities, try to get control over them, and run high-end procedures to break into the system.

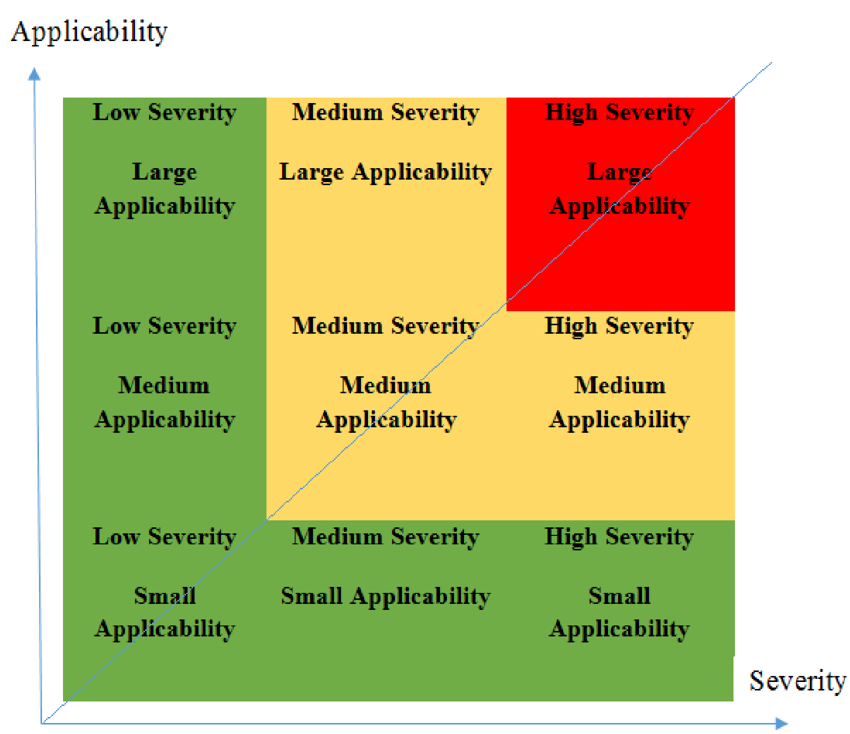

Figure 7: Vulnerabilities severity levels

3.2.10 Attacks

Attacks combine intentionality, with the structuredness, to cause threats, or to escalate them to the risk level. Attacks can target any of the predefined security measures to gain access, to cause disruption, or damage. For example, eavesdropping is against confidentiality, and authorization, while Denial of Service DoS attacks targets the availability of the resources. Generally, attacks can be classified into active or passive, and on the security level, they are furthermore classified into reconnaissance, access, denial of service, and malicious software/apps attacks. Definitions are given in Table 6 below.

Table 6: Attacks categorization

Passive Attacks	Here, the attacker only listens to the exchanged traffic, in aim of gaining valuable information, or trying to draw a map of the network by figuring out the communication patterns. In this form of attacks, the intruder will not affect the service directly, or change the data during its exchange.
Active Attacks	Active attacks use all possible means to change data or to cause disruption by means of manipulating resources and affecting operations. Active attacks require higher skills than the ones required for passive attacks.
Reconnaissance Attacks	It is a network discovery attack to learn about the network topology, gather information, and find the existing vulnerabilities. This type of attack is a passive one, and mostly it is followed by other forms of attacks, taking the active form.
Access Attacks	It is about accessing the system without using the authorized credentials, e.g. accounts or access tokens. This is an active attack, and is run by professionals using hacking tools to gain control over resources.
Denial of Service DoS Attacks	This attack directly affects the services and the whole firm by disabling resources that need to be accessed on demand, thus targeting the availability of the network. The attack can be as complicated as damaging the resources, or as easy as sending a huge number of legitimate messages from infected devices, thus consuming the network resources by keeping them busy in a reply mode.
Malicious Software/Apps Attacks	These are maliciously installed in a system for many purposes, as discovering vulnerabilities, creating holes for malicious access, causing damage, disruption, or collecting and directing information. They are also associated with Spam, Phishing, and can be used as a base for other attacks.

In more details, the first level of attacks is the reconnaissance attacks, which mainly consist of electronic sniffers that perform the role of eavesdropping systems. These attacks can come in many forms and with many tools, e.g. packet sniffers, ping queries, or port and protocol scanners. Unluckily there is no way to prevent these attacks, as they are done passively and totally hidden. However, mitigation can protect against these to some extent. Practices include restriction for either transmitted signals, and disabling protocols and ports that are not in use. Encryption techniques are as well feasible here, since they render the eavesdropped information useless for outsiders who do not hold the decryption keys. On the other hand, reconnaissance tools can be used inoffensively to help finding the existing vulnerabilities for a better risk management and security design procedure. Tools used here are any variant of network or protocol analyzer, e.g. Wireshark, Kisment, Aircrack-ng, and many others.

Access attacks are the next stage after gathering information enough to run an advanced attack. Access attacks take advantage of the found vulnerabilities to form a backdoor to access the system, to proceed with their original intent. Access attacks take many forms, as:

- Authentication attacks: These try to break the authentication mechanism to gain access. They are in the form of password guessing attacks as offline-dictionary attacks, brute-force, or rainbow attacks. The attack as well can take the form of forgery, that is by performing identity and password theft, combing eavesdropping and encryption cracking techniques. Another method is to try exploiting the weaknesses in authentication protocols, as EAP protocols of different flavors, FTP, HTTP, SSL, etc., and/or the 3-way-handshake procedure.
- Trust relationships exploitation: Trust relationships are built between systems that interact or function together, these systems fall within the same servers' and management farm, and share some of the firewall rules. These might include the Active Directory AD, Domain Name System DNS, Dynamic Host Configuration Protocol DHCP, Group Policy GP, and/or other systems. Attacks might take advantage of the weak/misconfigured relationships or systems, or manipulating the less secure systems to get access to the system under concern. In the worst-case scenario, the attack can even impersonate legitimate infected systems, thus gaining access and control over the exchanged data.
- Man in the Middle MitM: In this attack, an attacker inserts his system in between communicating systems without performing any changes to the communication criteria. This form of attacks takes advantage of getting a copy of the traffic, while being totally hidden/undetected. This attack requires direct access to the network under concern, to be able to install the MitM device between the legitimate devices.
- Redirection: Unlike MitM attacks, redirection attacks change the communication criteria by inserting malicious systems/software tools that direct the traffic through a malicious node. This attack can take the form of routing, or port redirection, to change

the path or the destined device for the traffic. Another form of the redirection attack is the DNS redirection, which changes the default TCP/IP settings including DNS and other services, thus performing queries and information redirection to malicious hosts/systems. The third form of the attack uses Uniform Resource Locator URL links or portal redirection, to direct users to malicious pages that save the authentication credentials, to rather perform identity and access credentials theft, as explained in a previous section.

- Phishing and Spam: Phishing is a malicious impersonation, in which an activity impersonates the legitimate one in sake of finding access credentials. The attack uses spam emails that seem coming from a trusted party, and ask to reply with sensitive information.
- Social Engineering: This is rather a technique to gather information than an attack. Here, the attack proceeds with conducting surveys, or masquerading administrators/authorities, to get access to valuable information they are not entitled to.

Denial of Service DoS is one of the most dangerous attacks as it targets the core of any service, availability. DoS works by sending large number of requests to one of the nodes, thus consuming its processing power, resources, and time needed to handle these requests. This can result in delayed services, or in a worse case render the infected node completely unavailable to proceed with the legitimate requests. Two categories exist here, with the traditional DoS only one system is used to run the attack, while in its Distributed version DDoS many systems are used simultaneously to run the attack mechanism. What makes DoS/DDoS frustrating is that the attack comes in the form of legitimate requests or queries, thus there is no way in differentiating innocent requests from the malicious ones, but only by monitoring resources and setting threshold criteria. DoS attacks come in three categories, as Volume-based with the intent of filling the network bandwidth so that other activities get delayed, Protocol-based which targets resources directly, finally Application-based which targets web servers trying to bring them down. DoS attacks may take but not limited to the following forms:

- Flood attacks, in the form of UDP, SYN, HTTP, ICMP or other management/control frames.
- IP exploitation attacks, in the form of Smurf, Ping of Death, or Fraggle attacks.
- IP Spoofing attacks.
- Resources exploitation as Slowloris web server attacks.
- Protocol attacks as NTP.
- Fragmentation attacks as with HTTP connections.

The last type of attacks takes the form of malicious software/application, in which a malicious code is written with the intent to cause damage, steal information, or corrupt the system. The code will spread across the connected systems trying to infect as many systems as it can reach, also it might include other functions as recording and directing sessions, capturing passwords, blocking services, or causing vulnerabilities, thus to ease other attacks. As previous attacks, malicious software/applications attacks come in many forms, as:

- Computer Virus: It is a code that works with the other installed programs, to control functionalities, or to change some of the system's settings, without the user's knowledge or approval.
- Trojan Horse: It is an application that masquerades another, while performing other functions that were not intended. The application is installed and given permissions by the user to perform its intended purpose, while in the background it performs other tasks fully hidden from the user. For instance, an e-reader app that also checks log files and gather information about the user.
- Worm: On a higher level, a worm is a self-replicated and self-executed code that requires zero human intervention unlike viruses. Worms do spread across the infected systems, trying to discover vulnerabilities and to exploit them. They later replicate themselves to the attached systems to initiate the processes again. Worms might perform an automated damage, or give attackers access privileges, so that they can control the infected systems remotely.

3.2.11 Policies and Procedures

Policies and procedures are of very high importance when it comes to security design, since they explicitly specify how to protect the organization and its assets, the acceptable actions, and the ways to apply the security measures. Policies and procedures are not the same, here policies do provide for the general planning, while procedures go through details and provide specifications and recommendations. Typically, an organization firstly agrees upon the standards matching with its business and core services. Later, standards are modified to fit with the organization's requirements and to bring security tightness into place.

In SANS, security policies are given, and classified into general, network security, server security, and application security policies, as shown in the following table, Table 7.

Table 7: Policies categorization

General	Acceptable Encryption Policy Acceptable Use Policy Clean Desk Policy Data Breach Response Policy Disaster Recovery Plan Policy

	Digital Signature Acceptance Policy Email Policy Ethics Policy Pandemic Response Planning Policy Password Construction Guidelines Password Protection Policy Security Response Plan Policy End User Encryption Key Protection Policy
Network Security	Acquisition Assessment Policy Bluetooth Baseline Requirements Policy Remote Access Policy Remote Access Tools Policy Router and Switch Security Policy Wireless Communication Policy Wireless Communication Standard
Server Security	Database Credentials Policy Technology Equipment Disposal Policy Information Logging Standard Lab Security Policy Server Security Policy Software Installation Policy Workstation Security Policy
Application Security	Web Application Security Policy
Other Policies	Antivirus Guidelines Server Audit Policy Automatically Forwarded Email Policy Communications Equipment Policy Extranet Policy Internet DMZ Equipment Policy Internet Usage Policy Mobile Device Encryption Policy Personal Communication Devices and Voicemail Policy Removable Media Policy Risk Assessment Policy Server Malware Protection Policy Social Engineering Awareness Policy

	DMZ Lab Security Policy Email Retention Policy Employee Internet Use Monitoring and Filtering Policy Mobile Employee Endpoint Responsibility Policy Remote Access Mobile Computing Storage Virtual Private Network Policy

As a practice, it is important to specify which security models are followed, prior selecting policies. This will help achieving the highest security while keeping balance with functionality. Security models are the way the security will be designed in an organization, they can concern enterprise, application, or both. Three models exist, namely open, closed, or restrictive. In the open model, users are trusted and minimum security practices are applied. This model is acceptable when an organization or a place upon protection is well isolated. In the closed model, there is no trust and the highest security practices are in place, this applies to open environments where public can benefit from the network. The last one is the restrictive model, which combines both models and control the security level upon device, location, and usage, without trading off functionality.

3.2.12 Analytics and Assessment

Now since all information regarding the organization is available, analytics is carried on to perform the security assessment for the organization. Many tools of varying complexity are used for this purpose, some only run single tasks, while others comprise of packages of multiple tasks running along. Tools include the following functions:

- Authentication cracking tools.
- Encryption cracking tools.
- Network utilities.
- Firewalls.
- Updates and patching tools.
- Monitoring platforms.
- Intrusion and anomaly detection.
- Scanners and packet sniffers.
- Policies evaluation.
- Forensics gathering.
- Reporting, integration, importing and exporting.

The analytics result with the final report, which includes the found strengths and weaknesses, recommendations, the adjustments, future plans, auditing, policies, and the technical, operational, and management procedures. Some of the famous platforms/software/OS that include:

- Linux distributions as KALI for security and REDHAT for big computation.
- OpenSOC project, Cisco.
- Symantec Security Analytics, Symantec.
- Secure Analytics, Juniper.
- SECURITY & BEHAVIORAL ANALYTICS, RSA.
- ArcSight Analytics, MICRO FOCUS of HPE.
- Security Solutions, IBM.

Analysis Survey Questionnaire

Questionnaires are given as a part of the security survey, to help visualizing the status of the organization upon analysis. Here are some of the given survey questions, in aim of gathering as much information as possible about the organization, to later plan for security perfectly.

1. What is the organization's main industry/activity?
2. Which standards or authorities are followed?
3. What needs to be protected?
4. What are the security solutions in place?
5. For whom the protection is done?
6. From whom the protection is done?
7. What are the existing risks?
8. What is the acceptable level of threats?
9. What is the sensitivity of the organization's data/information?
10. What the existing, and desired security levels?
11. Which skills the security officers hold?
12. Which equipment are in place, and if legacy devices are present?
13. The upgrade plans.
14. The existence of blueprints of the network.
15. Segmentation of the network.
16. Backup plans.
17. Parallel connections.
18. Physical security solutions.
19. Policies and agreements.
20. Transparency.
21. Training.
22. Customers and outsiders.
23. Auditing

4 Security Architecture in Enterprise

Many approaches exist on the way to apply security, however one of the most effective approaches is the layered security one.

4.1 Layered Security Approach

In this approach, multiple layers of defense exist simultaneously, thus more effort is required to break into the system than when only one layer is in place. However, following this approach needs carefulness, and well design, otherwise the different layers might affect operations and functionality by causing network burden. In Figure 8, the main security layers are given in a hierarchical form, and then explained briefly afterwards.

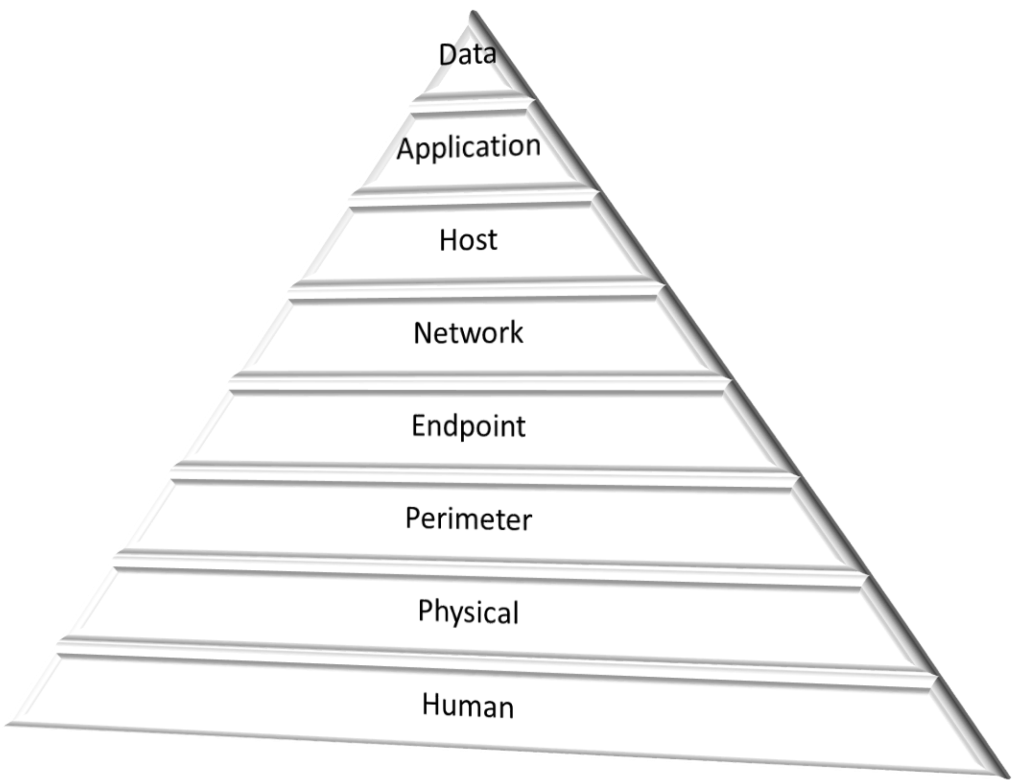

Figure 8: Security layers

- Human: At this layer come awareness, education, training, and the follow of the common sense practices regarding information and its spread. Here, all sorts of social engineering and fraud techniques should be mentioned for future avoidance. Employees should be tested on regular basis to update their security knowledge, especially the ones that hold critical roles that can affect the enterprise functions upon a successful security breach.

- Physical: As mentioned in section 2-3 earlier, physical security is one of the main foundations of the whole security process. Having access to a system physically makes it easier to cause damage, alter functions, or prevent services. It is necessary to ensure only the authorized ones can access the right places, at the right times, i.e. physical access control criteria. As well, installation of surveillance and monitoring devices across the hallways and pathways is a practice to keep track of the normality and to detect any anomalies. Recordings should be available within a specified period, so that they could be used for forensics when required.
- Perimeter: Here we concern the data flow, and perimeter represents the entry/exit points/gates from an organization to the outside world. Typically, a perimeter is protected by means of isolation, control, and examining the traffic. For these criteria, firewall appliances/software/servers are installed at the edge of the network, to block any incoming traffic from entering, unless it is a reply to an internally originated traffic. Firewalls here perform many functions, as checking the traffic headers, checking for anomalies, and with a built in malware software they can detect malicious traffic, also they do hide the IP addresses of the internal devices from the outside world by means of Network Access Translation NAT. Another function is to protect servers by isolating the servers' farm from outsiders, by creating a demilitarized zone DMZ, thus no malicious traffic can pass through. As well, it is a practice to use proxies here, thus servers will issue requests on behalf of client devices, furthermore proxy or historian servers can be used to save copies of the most accessed content, thus to save the bandwidth for queries, and process them internally. Figure 9 below shows how firewalls and DMZ typically function.

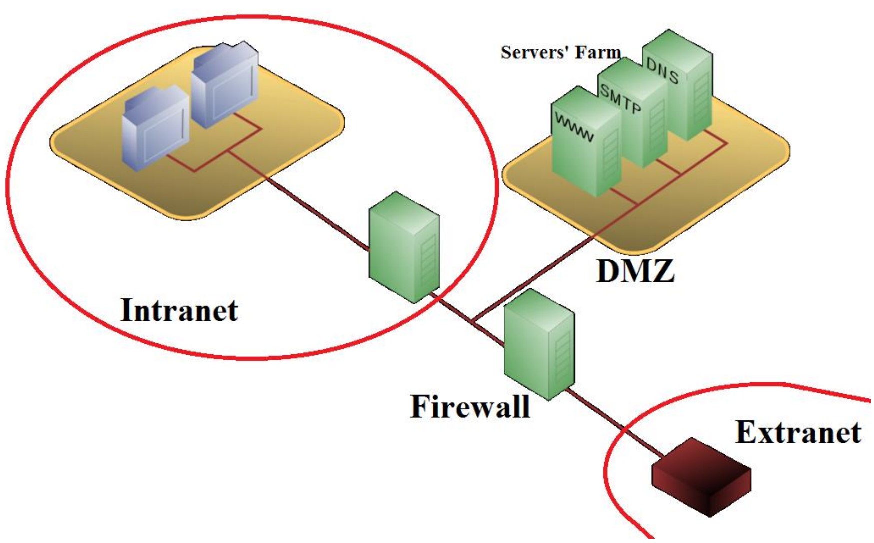

Figure 9: Firewall placement in an enterprise network

- Endpoint: This measure is imperative to protect devices that are used somewhere else rather than the secure network, however it is good to keep endpoint security always in place even within a secure environment. Endpoint devices carry sensitive data that upon compromise can cause harm or damage to the whole organization, and thus these devices need independent measures for protection. Many solutions should be used here, as disk encryption to protect against losing devices, anti-virus software installation, patching and updates, installation restriction by means of group policy management, virtualization of applications, and the use of Virtual Private Network VPN agents when accessing the network from outside of the premises. Endpoint protection as well includes many parts from human education and general policies that need to be specified in advance.
- Network: This refers to protecting the nodes within the Intranet from the Extranet and the Internet. Many measures exist to serve this purpose, for instance, firewalls to form restricted and controlled access, Network Access Control NAC and Network Access Protection NAP techniques to check the health of connecting devices prior connection, VPN to perform an adequate level of traffic tunneling between remote offices and the headquarters, and Intrusion Detection Systems IDS or Intrusion Prevention Systems IPS to detect anomalies, or to perform preset automated actions.
- Host: This layer aims protecting all host devices across the network, from servers, network devices, to end users’ devices. The main goal is to keep devices independently healthy, prevent data loss, and maintain functionality. Many solutions are used for this. Firstly, the most important practice is to change defaults, thus to prevent malicious access to devices. After that, authentication and authorization should be in place, thus to make sure the right ones access the right devices at the right times with the right privileges. Depending on the criticality of devices and information, Multi-Factor Authentication MFA can be used, as something you have as tokens, something you know as a PIN code, and something you are as a biometric identity. The next step is by deploying an anti-malware solution to ensure devices’ freedom from malicious code and/or activities. Data Loss Prevention DLP techniques are used here as well to perform backup and sync functions, also to classify data according to criticality, and thus provide the right access to it. DLP follows the concepts of Data at rest/ in move/ in use, to provide the best means to access data and to keep it fresh. Other solutions include monitoring, logs, group policies, and deploying host-based IDS systems also could be used.
- Application: This layer ensures that applications perform their intended functions with no other hidden ones, they run smoothly, and without any code breaches that might result in accessing or damaging data. Unfortunately, applications are designed without security in mind, and thus they might need security solutions to work with them to cover the lack of security. Application firewalls are of good use here, as they fully integrate with applications, yet they do check the traffic for attack patterns or

malicious activities. Authentication as well applies here, especially when accessing an organization's portal that would provide access to its data and servers. One of the most recommended practices is to deploy applications using secure connections, that is by communicating natively over "S" secure protocols, as HTTPS and FTPS/SFTP. Other practices include running legacy apps by means of virtualization, thus to isolate them from the network.

- Data: The data security layer ensures the integrity and consistency of data, protection in the form of confidentiality, and that data is always available to the right ones when necessary, e.g. CIA. Encryption is a key factor here, as data should be always encrypted in a way or another according to its criticality. This goes along with authentication and authorization measures as Single Sign-On SSO, or Federated Identity FI, to provide access with adequate restriction according to the policies in force. For availability, parallel connections, backup, and freshness procedures as DLP should be considered.

To sum this up, Figure 10 shows the concepts and technologies for a successful layered security implementation. It is worth noticing that, the human factor is of high criticality for the security process.

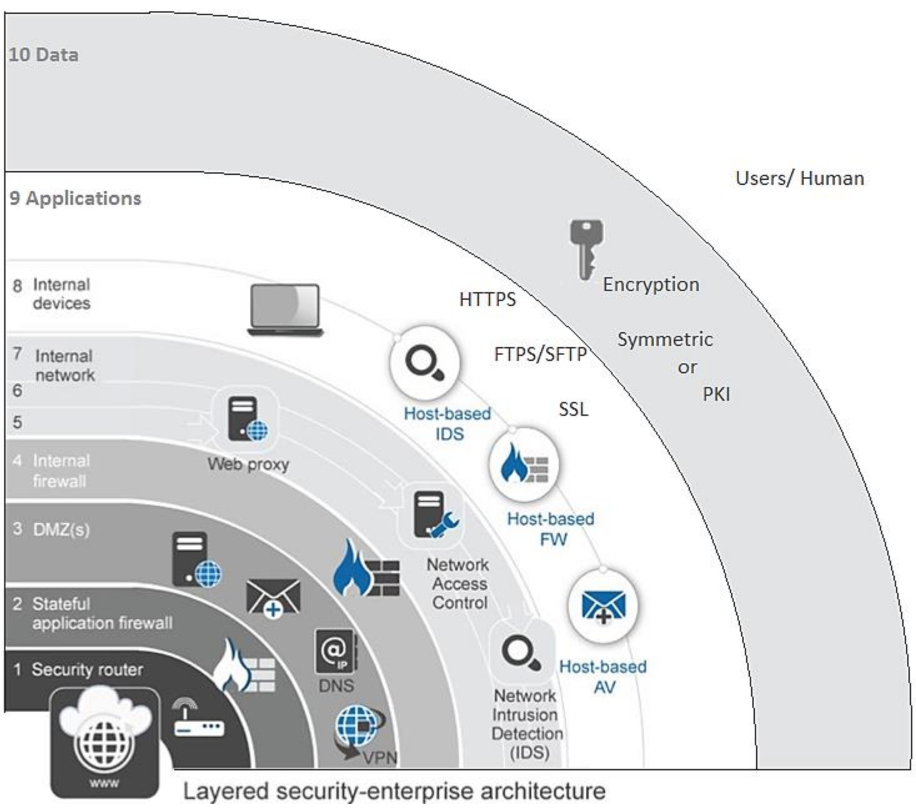

Figure 10: Layered security and technologies

4.2 Cabled Network Security

Among the other networking technologies, the cabled/wired network still plays the most significant role to connect nodes, process data, and exchange traffic in an organization. Thanks to its versatility, its speeds, and the high level of security it offers. As the wired network utilizes physical connections, it spans to take different forms according to the size, and the intended application. For instance, it can take the form of LAN, to connect co-located devices as in Small Office Home Office SOHO networks. It also can go further to include Campus Area Network CAN to connect devices in a campus or a larger building, and Metropolitan Area Network MAN to connect devices rather in a municipality or vicinity of a city. Finally, the network can span globally as in WAN, which goes beyond these limits to include remote sites and the Internet. *Technologies regarding these forms are beyond the scope of this report, and only we shall consider security here*. Since the cabled network is confined within a physical media, it possesses an adequate level of security, though it is not the case anymore. Currently the cabled network is open to the outer world, to share, access and store data, and many functions are performed using remote access methods from somewhere else. Consequently, tight control measures should be applied, and most of the security practices should be followed to mitigate any security shortages.

Briefly, within a localized organization, the cabled network typically takes the form of LAN or CAN. These forms offer private communication, with high data rates, and access to databases and services. Previously, the cabled network was isolated enough to keep it well protected, however it currently forms the foundation for the whole communication, in which other technologies build upon. This in turn introduced many threats and risks that should be considered during the network early design phase. Here, threats and risks include wiretapping, unauthorized access, data extraction, data modification, damage to the network components, and/or blocking and disabling services. To solve against these issues, the typical security countermeasures discussed earlier as confidentiality, integrity, availability and authenticity should be in place.

From the OSI standard's perspective, the network and its components fall within the first three layers of the OSI model, namely the Physical, Data Link, and Network Layers. In Table 8, the major threats to these layers are given:

Table 8: OSI layers' threats

Physical layer	Wiretapping Interference Denial of Service Man in the Middle
Data Link Layer	Spoofing

	Denial of Service Port Redirection DHCP attacks
Network Layer	Routing and Redirection attacks Spoofing Denial of Service

Practices to overcome these threats include:

1. Network Topology and farm distribution: This is a fundamental practice to ensure the network is fully up and running. Network topologies concern the layout at which the network is designed, this can take the form of bus, mesh, star, or star of stars fashion. Typically, all layouts are used together to provide for high performing network, as a single layout will not be able to provide this. Depending on the application and the criticality the layout need to be tuned, for instance extra mesh links should be implemented to serve the availability of the services in high demand, also to protect against security threats by having ready functioning connections. Star links ease the central management and are robust to control, however they can cause network burden, form a single point of failure, and ease the distribution of threats. Bus connections are good solution for peer-to-peer connections and for Extranet, but they are not for large implementations of any kind. Regarding distribution, sensors should be distributed over the network for continuous monitoring, and severs should be close to the users or distributed evenly. This set-up provides protection against excessive loads, as well a stand-by ready solution.
2. Cabling: The network is as fast as its slowest link, and is as secure as its weakest link. Thus, high category CAT cablings need to be considered, as they provide for high speeds, and protect against data emanation and/or interference. Typically wired should be used as last-mile solution, and it is highly recommended to run the long links using optical fiber links, as they provide for very high speeds, and protecting against interference.
3. Isolation: Firstly, it is recommended not to fully open the network to the public one, and/or the Internet. No devices that can function internally should be connected externally, to serve for security, and to protect against network burden. On the other hand, for the devices that need connectivity, firewalls, DMZs, and the continuous utilization of VPNs should be in use. This will ensure that the network is fully isolated from the public, and the traffic cannot be intercepted or seen.
4. Segmentation: Even within the same network, it is recommended to perform a level of segmentation, by dividing the network into smaller subnetworks. This on the design level can be done by implementing the right topologies, while on the hardware level by using of different L2 and L3 switches, or by means of Virtual LANs VLANs

implementation. This segmentation protects against peer attacks, reduces the risk, decreases the area exposed to threats, protects against the network burden, and reduces the exchanged traffic.

5. Encryption: With the current cyber security situation and the spread of cyber threats, it is better to encrypt the traffic between all nodes, even if they are connected physically by means of wires/cables. On a higher level, it is necessary to encrypt the traffic between conduits and nodes, to serve isolation, and to force security.
6. Layer 2 and Layer 3 Access Control Lists ACLs: Access control has always been one of the most recommended security practices. Here, devices will be recognized according to their MAC and IP addresses at first, then get their roles and permissions assigned. This will set rules for communication, force restriction, isolation, and will act as an embedded level of authentication and authorization. Layer 2 ACLs deal with devices within the same subnets, while layer 3 ACLs will concern the ones of different networks.
7. Authentication: To protect against spoofing attacks, and MAC address impersonation, authentication should be done prior granting network access, even with physical connectivity. By providing the right credentials for access, only the right devices will be able to connect. It is important here to escalate the authentication according to the resources' criticality, for instance MFA should be used to access the management, operation, and control infrastructure rather than SSO.
8. Parallel Links: Availability should be maintained, especially for the critical devices that cannot handle delays or disconnection. Parallel links can be used to provide for bandwidth aggregation, or work as a stand-by solution to protect against network failure.
9. IDS and IPS: Sensor devices should be installed or integrated to the network nodes to monitor the traffic for anomalies, and to detect any issues regarding security or performance. IDSs will report the found issues without taking any further actions, while the more advanced IPSs will perform a counterattack on the infected devices for mitigation and isolation, thus to protect the other nodes.
10. Physical Security: As discussed earlier, information security measures without the physical means to protect the services render the security process useless. Physical access control devices, Closed Circuit TV CCTV, motion detection, physical locks, smoke detectors, fire suppression, and all of the other methods for physical security should be present.
11. Port Scanners: This is used to detect the unnecessary open ports for further mitigation actions. However, this normally is integrated as a part of security package as IDS/IPS or analysis software.

4.3 Wireless Network Security

Wireless networking has emerged for few decades already, and with the advancements in the technology, it proves itself as the future of communication. Wireless networking comes mainly in two general categories, Wi-Fi, which falls within the LAN and CAN umbrella, and mobile technologies, which form MAN and WAN networks. Many benefits the wireless communication offers, not only limited to the easiness of implementation, the cabling cost reduction, the mobility, but it also extends to versatility and the fact that it can adapt with different scenarios at the same time. On the other hand, unlike the wired/cabled communication, which uses a confined media, wireless uses unbounded media for communication. This makes it more susceptible to security threats, interference, visibility, and discovery. Moreover, wireless communication still cannot offer the same speeds as the wired communication. For these issues, implementation of wireless networking within an organization should be well tuned to mitigate any risks and to meet its requirements. In the following paragraphs, these issues and solutions are discussed.

Firstly, since wireless communication takes place in unbounded media, all other wireless devices can intercept the communication. This means that also outsiders' devices, or malicious devices can listen to the exchanged traffic. Here, many forms of attacks can take place, e.g. eavesdropping to listen to the communication passively, and cracking attacks, which to retrieve the information from the exchanged traffic. A very common issue as well is the DoS, in which an easy interference can render the whole wireless network useless. DoS here can be intentional as in jamming attacks in which a signal generator is used to disrupt the communication, or unintentional as with the interference with the existing devices as microwave ovens, Bluetooth, and cordless phone devices. To mitigate these issues, firstly a thorough survey should be conducted prior to the implementation of the network, in which all wireless devices and sources of interference should be indicated and removed. Secondly, the wireless signal should be tested for emanation outside the organization's perimeter, to adjust the transmission powers, to prevent outsiders from receiving the leaked signals. Still, the use of amplifiers and high-gain antennas can find the smallest leak, thus it is recommended to install a shield, e.g. Faraday shield, around the perimeter, or where the critical communication occurs. This will help preventing any signal leakage permanently.

The second issue that can occur is the problem of Near-Far communication. Here, communication devices render hidden and lose the ability to communicate because of the signal weakness, which directly affects the availability of devices. The issue is generally related to misconfiguration and mismanagement. High-end network devices as routers and switches have the ability to send with higher power compared to the devices with Network Interface Cards NICs installed, as desktops, laptops, or mobile devices. This allows the receiving devices to receive the signal, while their reply messages are not delivered. Excessive retransmission and network failure is the result of that. To mitigate this issue, the networking devices should not transmit using their full power, in other words, the transmission power should match with the device of the least transmission power. The same problem exactly occurs with the unmatched transmission rates, in which devices use different modulation schemes of different rates, rendering some devices unavailable, out of being unable to communicate. Once more, it is a problem of misconfiguration and mismanagement, and for mitigation, devices should match with the modulation schemes and the rates with the device of the least capability. Another solution is to allow devices to change their modulation and data rates automatically over the management frames, however this might affect the total network speeds. It is recommended here to upgrade the legacy devices to match higher data rates.

Related to the second issue, signal quality is also a very important issue to consider. Generally, the ISM band is the one in place regarding wireless communication. ISM includes frequency bands at the 900 MHz, 2.4 GHz, and 5 GHz. Many technologies exist here, as 802.11/a/b/g/n/ac, Bluetooth devices, cordless phones, microwave devices, and others. Typically this can render the signals of low quality, and increase the retransmission rates, which in some cases can cause partial DoS. Specifically, recently many devices operate in the 2.4 GHz band. In a study, it was found that more than 300 types of devices operate in the 2.4 GHz band. This indicates that the band is fully occupied already, and cannot handle more communicating devices, in addition to the fact that it cannot offer but limited data rates as in 802.11g/n. Band steering is the solution, in which devices will be directed to use the higher band of 5 GHz instead. This means that devices should be equipped with 802.11n/ac chips. The result is higher data rates, and the implementation of the security mechanisms that are only available with these high technologies. Still, many other solutions to come, as 802.11 ad operating in the 60 GHz band, 802.11 ax operating in the 2.4 GHz band, however these are still under research.

The third issue to take care of when implementing wireless networking is encryption and authentication. With wireless, data is transmitted freely in the air, so anyone with proper devices can intercept the signal. Authentication is of critical importance here as it only allows the right devices to connect to each other, and typically it is one step ahead of encryption, as the encryption algorithms are dependent on the authentication ones. Many authentication methods exist for wireless communication, starting from Open-System Authentication OSA with no authentication at all, Wired Equivalent Privacy WEP, to the more advanced Wi-Fi Protected Access WPA I and II, with its versions, personal, and enterprise. WEP is the most implemented wireless authentication method globally, while it is the least secure. WEP uses shared keys of 64 bits or 128 with its update. The problem with WEP is that it has 24 bits of Initialization Vector IV of inactive bits sent in clear from the devices' manufacturer driver. This reduces the active bits used for authentication. The authentication is done using the method of challenge and reply messages, sending a message in clear and comparing its reply with its encrypted version. The used encryption method is Ron's Code RC 4, which is already cracked, and capturing the exchanged authentication messages makes it a matter of minutes to render the authentication key, i.e. the shared key/password. Moreover, with WEP, the authentication key is the same one used for encryption, thus the whole communication can be intercepted. This security method should never be used and all devices that are still using it should be replaced, as these devices are of potential threat for the organization. WPA was introduced to replace WEP, with more advanced authentication and encryption schemes. WPA uses a passphrase, or Pre-Shared Key PSK that is 256 bit in length, which tremendously improves the security, however the actual power of WPA comes from its encryption schemes. Unlike WEP, which uses static keys for encryption, WPA generates dynamic keys derived from the authentication keys, mixed with nonce frames, and devices' addresses, in a special equation for two rounds. This creates unique encryption keys to each device in the network, thus no two devices would share the same encryption keys anymore. WPA comes in two versions, WPA I, and WPA II. In its first version, the encryption method is the Temporal Key Integrity Protocol TKIP, which is an improvement of RC4, while in WPA II it goes to the very robust encryption algorithm Counter Mode – Cipher Block Chaining – Message Authentication Code- Protocol CCMP, which utilizes the Advanced Encryption Standard AES cipher. With both releases, WPA comes in two versions, Personal and Enterprise. WPA personal targets the SME, in which authentication servers are not used, thus utilizing a manually entered PSK. In the Enterprise version, WPA utilizes 802.1X Port-Based Authentication, which uses authentication server, and can incorporate all the security means by implementing EAP authentication methods of different flavors, including token and biometric authentication. This introduces the highest security available for wireless networking. In Table 9, all combinations of wireless authentication and encryption are given.

Table 9: Wireless security algorithms

Standard	Authentication	Encryption	Cipher	Key Generation	Evaluation
WEP	Open System Authentication OSA	WEP	RC4	Static	Acceptable when combined with other measures, but not recommended
	Shared Key	WEP	RC4	Static	Should never be used
WPA I	PSK Personal	TKIP	RC4	Dynamic	Strong
	802.1X/EAP Enterprise	TKIP	RC4	Dynamic	Strong
WPA II	PSK Personal	CCMP	AES	Dynamic	Robust
		TKIP	RC4		
	802.1X/EAP Enterprise	CCMP	AES	Dynamic	Robust
		TKIP	RC4		

The next issue to consider regarding wireless communication is the speed, or data rates. Wireless communication speeds depend on the utilized Modulation and Coding Schemes MCS that combine the coding rates and the modulation, the number of combined channels, and the use of normal or Short Guard Interval SGI. These combinations make the MCSs to differ in the speeds they offer. Two factors need to be considered here, interference, and the failure rate. Interference caused by the surroundings or the environmental conditions affect the communication drastically, and tend to change MCSs from higher to lower ones for a better performing but slower network. The other factor is the failure rate, as the high modulation schemes as 256-QAM, are sensitive to the RF noise. Typically, for 802.11 technologies, the speed can vary from as low as 1 Mbps with 802.11b to reach almost 6.9 Gbps with 802.11ac with Multi-User Multiple In Multiple Out MU-MIMO technologies in place. Table 10 shows the different MCSs for 802.11n and 802.11 ac, and the way they affect the network speed.

Table 10: MCSs for 802.11 n and 802.11 ac

MCS Index - 802.11n and 802.11ac

802.11n 802.11ac

HT VHT					20MHz		40MHz		80MHz		160MHz	
MCS	MCS	SS	Modulation	Coding	No SGI	SGI	No SGI	SGI	No SGI	SGI	No SGI	SGI
0	0	1	BPSK	1/2	6.5	7.2	13.5	15	29.3	32.5	58.5	65
1	1	1	QPSK	1/2	13	14.4	27	30	58.5	65	117	130
2	2	1	QPSK	3/4	19.5	21.7	40.5	45	87.8	97.5	175.5	195
3	3	1	16-QAM	1/2	26	28.9	54	60	117	130	234	260
4	4	1	16-QAM	3/4	39	43.3	81	90	175.5	195	351	390
5	5	1	64-QAM	5/6	52	57.8	108	120	234	260	468	520
6	6	1	64-QAM	3/4	58.5	65	121.5	135	263.3	292.5	526.5	585
7	7	1	64-QAM	5/6	65	72.2	135	150	292.5	325	585	650
	8	1	256-QAM	3/4	78	86.7	162	180	351	390	702	780
	9	1	256-QAM	5/6	n/a	n/a	180	200	390	433.3	780	866.7
8	0	2	BPSK	1/2	13	14.4	27	30	58.5	65	117	130
9	1	2	QPSK	1/2	26	28.9	54	60	117	130	234	260
10	2	2	QPSK	3/4	39	43.3	81	90	175.5	195	351	390
11	3	2	16-QAM	1/2	52	57.8	108	120	234	260	468	520
12	4	2	16-QAM	3/4	78	86.7	162	180	351	390	702	780
13	5	2	64-QAM	5/6	104	115.6	216	240	468	520	936	1040
14	6	2	64-QAM	3/4	117	130.3	243	270	526.5	585	1053	1170
15	7	2	64-QAM	5/6	130	144.4	270	300	585	650	1170	1300
	8	2	256-QAM	3/4	156	173.3	324	360	702	780	1404	1560
	9	2	256-QAM	5/6	n/a	n/a	360	400	780	866.7	1560	1733.3
16	0	3	BPSK	1/2	19.5	21.7	40.5	45	87.8	97.5	175.5	195
17	1	3	QPSK	1/2	39	43.3	81	90	175.5	195	351	390
18	2	3	QPSK	3/4	58.5	65	121.5	135	263.3	292.5	526.5	585
19	3	3	16-QAM	1/2	78	86.7	162	180	351	390	702	780
20	4	3	16-QAM	3/4	117	130	243	270	526.5	585	1053	1170
21	5	3	64-QAM	5/6	156	173.3	324	360	702	780	1404	1560
22	6	3	64-QAM	3/4	175.5	195	364.5	405	n/a	n/a	1579.5	1755
23	7	3	64-QAM	5/6	195	216.7	405	450	877.5	975	1755	1950
	8	3	256-QAM	3/4	234	260	486	540	1053	1170	2106	2340
	9	3	256-QAM	5/6	260	288.9	540	600	1170	1300	n/a	n/a
24	0	4	BPSK	1/2	26	28.9	54	60	117	130	234	260
25	1	4	QPSK	1/2	52	57.8	108	120	234	260	468	520
26	2	4	QPSK	3/4	78	86.7	162	180	351	390	702	780
27	3	4	16-QAM	1/2	104	115.6	216	240	468	520	936	1040
28	4	4	16-QAM	3/4	156	173.3	324	360	702	780	1404	1560
29	5	4	64-QAM	5/6	208	231.1	432	480	936	1040	1872	2080
30	6	4	64-QAM	3/4	234	260	486	540	1053	1170	2106	2340
31	7	4	64-QAM	5/6	260	288.9	540	600	1170	1300	2340	2600
	8	4	256-QAM	3/4	312	346.7	648	720	1404	1560	2808	3120
	9	4	256-QAM	5/6	n/a	n/a	720	800	1560	1733.3	3120	3466.7

It is clear that only within the Wi-Fi technologies, only 802.11n and 802.11ac are the only standards that can meet the current data rates' requirements. It is strongly recommended to upgrade the wireless cards to the ones only work with these technologies.

The last issue to consider regarding wireless security is the compatibility issue. Since the wireless technology changed in fast pace, many of the technologies that were used few years back should be now obsolete, as they do not match with the current speed and security demands. However, the fact is that many of these technologies are still in use, especially in the SME, and SOHO environments. Moreover, the new advanced technologies all feature backward compatibility, so that they can coexist with the older devices. The main drawback here is, with backward compatibility these advanced devices shift their speeds and security features back to match with the older devices, thus losing all the advancements they have. Moreover, once there is a need to shift back for compatibility reasons, it forces the whole network to follow this, not only the devices that deal directly with legacy devices. This simply means that it is enough to install one legacy device to completely affect and disrupt the whole network. To mitigate this, there are two solutions, in which the first is to upgrade all legacy devices and to set the networking devices' modes manually, thus to prevent the fallback option. The second solution is to lock the legacy devices to the same subnetwork, and to implement a VPN solution, thus to form a level of network isolation, and to protect all other devices from threats that legacy devices might bring.

Regarding mobile telecommunication technologies, as mentioned earlier they fall under the MAN and WAN umbrella, and could be used to connect to remote offices or for remote access. Different speeds vary here depending on the technology, for instance the 3G could offer up to 60+ Mbps, the 4G up to 300+ Mbps, while the forthcoming 5G promises fiber-like speed experience. It is worth mentioning here that these speeds are only in the optimal conditions. Mobile technologies offer a versatile ready-to-run solution, and starting from the 3G they come with great security features. Thanks to the strong security and encryption features they incorporate. It is still recommended to use secure Access Point Names APNs from the service providers, thus to separate the organization's traffic from the public's, also to implement VPN solution, thus to ensure end-to-end security even over the wired part of the service providers.

Summing it up, wireless communication is an easy to deploy solution, but it is never meant to replace the cabled network. Wireless networks should be installed only on the edge of the network to provide for network access, or to provide for remote access using WAN mobile technologies, however wireless is not for the core communication, due to its limited speeds, and instabilities from other factors. Regarding speeds, it is recommended to go with 802.11ac or 802.11n, to force band steering, and to utilize the 5 GHz band. Regarding security, 802.1X PBAC is the recommended means of authentication, and CCMP is the recommended encryption, thus Robust Security Network RSN requirements are met.

Secure Wireless Network, An Innovative Solution by Siklu©

Siklu is an innovative company working with the wireless technology. They introduced a unique solution to provide for a high speed and secure wireless communication, by utilizing the new 802.11ad technology. The solution is named mmWave Wireless. In brief, mmWave Wireless deploys narrow beam signals in the 60 GHz band. Unlike the other wireless deployments, with this solution only the targeted devices will get the signal, i.e. no more signal broadcasting. This in turn protects against eavesdropping, interference, and monitoring. Moreover, mmWave Wireless network is well immune, and provides fiber-like experience.

The solution is illustrated in Figures 11-a, and 11-b below.

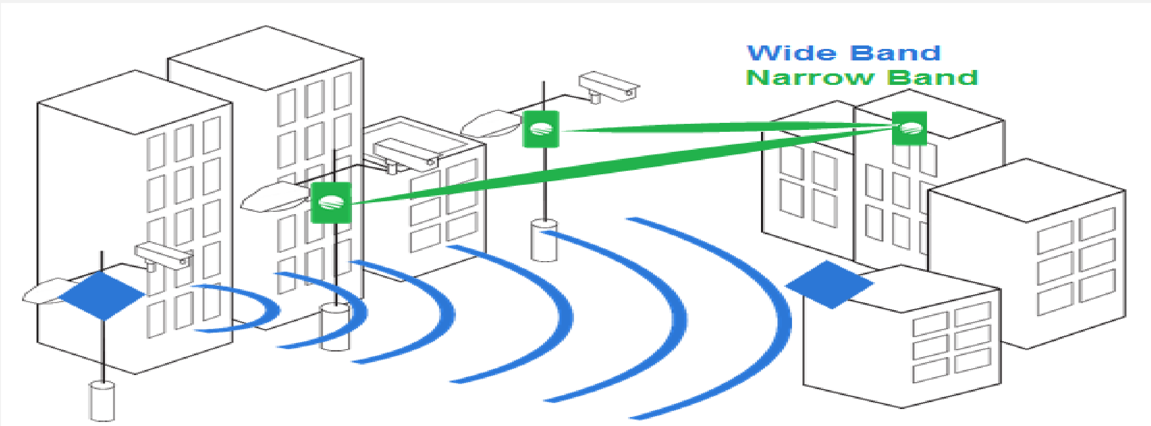

Figure 11-a: Narrow Band Vs. Wide Band communication

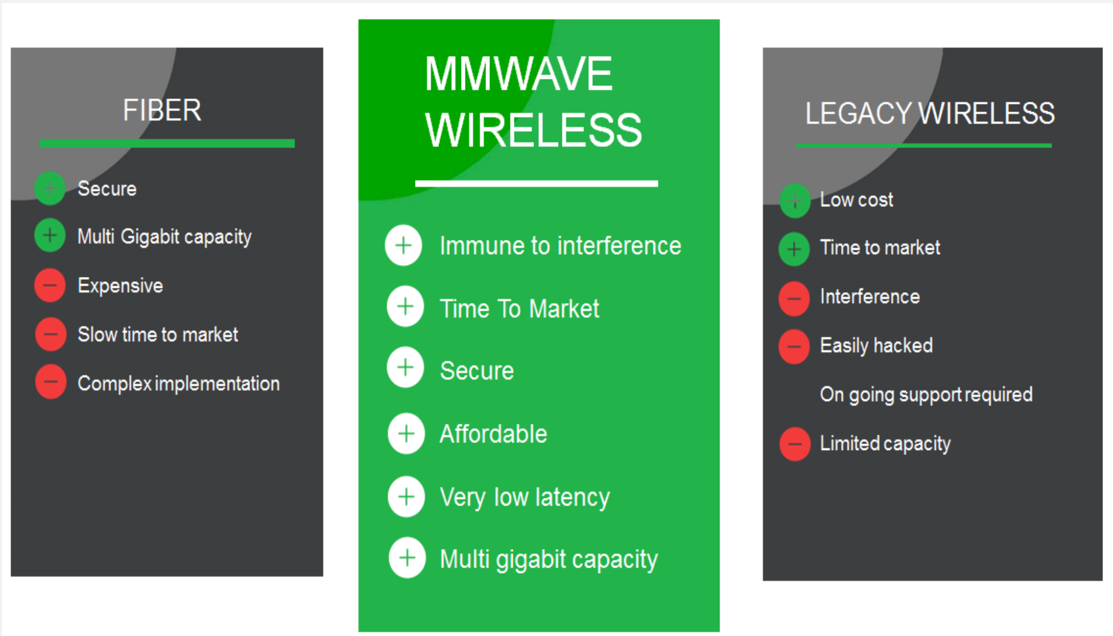

Figure 11-b: Fiber optics Vs. mmWave Wireless Vs. Legacy wireless

This solution as well supports the demands of the future network, which features the following, as in Figure 11-c.

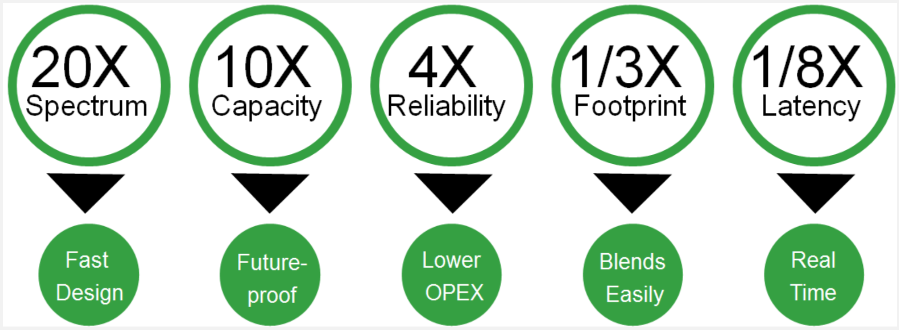

Figure 11-c: The future network demands

5 Appendix of Standards

5.1 ISA99 – IEC62443 Risk Assessment

IEC62443 is a standard used to provide security capabilities to the Industrial Automation and Control Systems IACS systems, that lack security functions out of its alongside deployed Supervisory Control and Data Acquisition SCADA non-security native systems. The standard applies the common foundational security concepts, as Authentication, Integrity, Confidentiality, Use Control, and Availability. As shown in Figure 12, IEC62443 logically comprises of thirteen standards and reports, categorized into four main categories, namely General, Policies and Procedures, System, and Component.

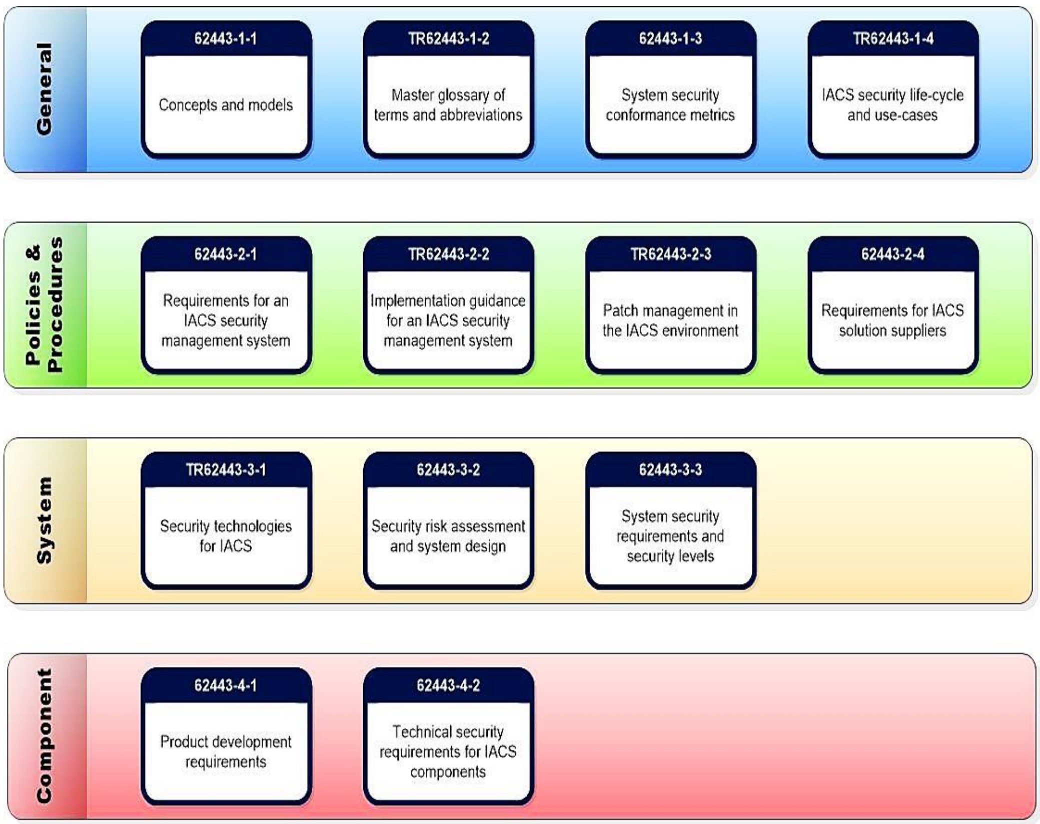

Figure 12: IEC62443

IEC62443 classifies security levels into four categories:

1. Unintentional, casual, or accidental violation.
2. Intentional violation with simple means, resources, and skills.
3. Intentional violation with sophisticated means, resources, and skills.
4. Intentional violation with sophisticated means, and using extended resources.

The standard mainly focuses on the concepts of zones and conduits, thus to have full control over the systems, while maintaining an adequate level of protection. According to the standard, a zone is the grouping of assets that share the same security requirements, or have the same security capabilities. Zones can take many forms as control, operation, industrial, enterprise, remote access, process information, internal, external, management, wired, wireless, end-user, or any other form. Moreover, a zone can include subzones with inherited properties. It is imperative to define zones clearly prior to the network implementation, thus to mitigate any future potential risks. The other main part of the standard is conduits, which are the links that connect between the different zones. It is explicitly mentioned that all the communication passing through conduits should be protected by means of encryption algorithms. Like this, the standard goes with the aforementioned concepts of isolation and segmentation, and proves itself for robustness and applicability across the industrial systems.

On the downside, IEC62443 is too generic, as it addresses all of the ICAS forms. The standard as well is more to risk assessment than to cybersecurity, thus it might require other standards to operate jointly to provide for a high level of protection. Finally, the standard is neutral, as it focuses mainly on the concepts without giving explicit guidance, and practices are left for individual's implementation.

About implementation, when physical security and standby solutions are in place, then Level 1 protection is met, and thus Level 2 and above are the ones exclusively under concern. The standard's reports can be adjusted and customized to match with the organization's requirement, and the desired protection level. Here, we listed and reordered the eight reports we see highly important from the cybersecurity perspective, as following:

1. Requirements for an IACS security management system (TR 2-1)
2. System security requirements and security levels (TR 3-3)
3. Security risk assessment and system design (TR 3-2)
4. System security conformance metrics (TR 1-3)
5. Technical security requirements for IACS components (TR 4-2)
6. Security technologies for IACS (TR 3-1)
7. Implementation guidance for an IACS security management system (TR 2-2)
8. Patch management in the IACS environment (TR 2-3)
9. ***Security risk assessment and system design (TR 3-2)***
10. ***System security conformance metrics (TR 1-3)***

As seen in this proposal, TRs 3-2 and 1-3 are repeated after the whole process, as they are required to perform a further check about robustness of the system, its conformance, and compliance.

5.2 ISO/IEC 27033 Information Technology – Security Techniques – Network Security

ISO 27033 is a standard dedicated to information technology and the required security practices. It focuses on the network security, and it covers well many related aspects and issues. Additionally, it addresses the main threats and risks, and proposes guidance and practices to mitigate them. The standard comprises of six TRs or sub-standards, in which each concerns a specific point to study thoroughly, and then gives the recommended implementable practices. TRs are as following:

1. Part 1: Overview and Concepts, (TR 27033-1): The report provides the general overview and the definitions related to network security, and it acts as a roadmap to the other reports. It as well "
   a. *Provides guidance on how to identify and analyze network security risks and the definition of network security requirements based on that analysis.*
   b. *Provides an overview of the controls that support network technical security architectures and the related technical controls, as well as those non-technical controls and technical controls that are applicable not just to networks.*
   c. *Introduces how to achieve good quality network technical security architectures, and the risk, design and control aspects associated with typical network scenarios and network technology areas (which are dealt with in detail in subsequent parts of ISO/IEC 27033), briefly addresses the issues associated with implementing and operating network security controls, and the on-going monitoring and reviewing of their implementation."*
2. Part 2: Guidelines for the design and implementation of network security, (TR 27033-2): *"gives guidelines for organizations to plan, design, implement and document network security"*
3. Part 3: Reference networking scenarios -- Threats, design techniques and control issues, (TR 27033-3): *"describes the threats, design techniques, and control issues associated with reference network scenarios. For each scenario, it provides detailed guidance on the security threats, the security design techniques, and controls required to mitigate the associated risks."*
4. Part 4: Securing communications between networks using security gateways, (TR 27033-4): *"gives guidance for securing communications between networks using security gateways (firewall, application firewall, Intrusion Protection System, etc.) in accordance with a documented information security policy of the security gateways, including:*
   a. *Identifying and analyzing network security threats associated with security gateways.*

b. *Defining network security requirements for security gateways based on threat analysis.*
c. *Using techniques for design and implementation to address the threats and control aspects associated with typical network scenarios.*
d. *Addressing issues associated with implementing, operating, monitoring, and reviewing network security gateway controls."*

5. Part 5: Securing communications across networks using Virtual Private Networks (VPNs), (TR 27033-5): "*gives guidelines for the selection, implementation, and monitoring of the technical controls necessary to provide network security using Virtual Private Network (VPN) connections to interconnect networks and connect remote users to networks.*"
6. Part 6: Securing wireless IP network access, (TR 27033-6): *"describes the threats, security requirements, security control and design techniques associated with wireless networks. It provides guidelines for the selection, implementation and monitoring of the technical controls necessary to provide secure communications using wireless networks. The information in this part of ISO/IEC 27033 is intended to be used when reviewing or selecting technical security architecture/design options that involve the use of wireless network in accordance with ISO/IEC 27033-2."*

5.3 NIST Cybersecurity Framework CSF, Framework for Improving Critical Infrastructure Cybersecurity

NIST's CSF is a part of a governmental project that focuses on protecting the physical and virtual assets from any threats or expected risks. NIST by concern focuses on technologies and the practical issues, thus their reports as well follow the same direction. NIST's CSF is a technology neutral technical report that incorporates many standards, practices, and guidelines to provide for the best security solutions. The framework targets level 2 or Executive Officer EO level, thus it will not mention specifically which devices or solutions to select, rather it tells about the technical specifications and the required configurations to achieve the desired level of protection. The following are the contributions of the framework to organizations: "

1. *Describe their current cybersecurity posture*
2. *Describe their target state for cybersecurity*
3. *Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process*
4. *Assess progress toward the target state*
5. *Communicate among internal and external stakeholders about cybersecurity risk."*

The framework is composed of three parts, namely Core, Implementation Tiers, and Profiles, as described briefly in the following paragraphs.

The core mainly focuses on the "*activities and the desired outcomes*", it also gives compliance with the standardization organizations of a specific industry. "*The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level."* The most important about the core that it includes functions for the five domains, Identify, Protect, Detect, Respond, and Recover, or the IPDRR functions. These functions give the standard its robustness as they concern all of the required operations in details. The definitions of these functions are as follows: *"*

1. ***Identify**: Develop an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.*

2. ***Protect**: Develop and implement appropriate safeguards to ensure delivery of critical 329 infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event.*
3. ***Detect**: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events.*
4. ***Respond**: Develop and implement appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident.*
5. ***Recover**: Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident.*

Moreover, the given functions are mapped into Categories to address the "*needs and particular activities"*, Subcategories that go more in depth, and finally Informative References to refer to the standards and practices.

The second part of the framework is the Implementations Tiers part, which is about the organization's views and the way that the cybersecurity risks could be managed. Depending on the case and its complexity, one or more tiers could be applied. Tiers are classified into Partial, Risk Informed, Repeatable, and Adaptive. The four classes in fact address the same criteria, which are the risk management process, the integrated risk management program, and the external participation, but rather from different perspectives. The partial tier acts as an ad hoc and reactive, to address some issues or gaps in the security practices. In this tier, practices are still under development or not adopted yet, there is "*limited awareness"*, and finally the organization operates independently without further collaboration with externals. On the risk informed tier, cybersecurity risks are well known, and the policies are in the informative phase than being enforced, and the organization collaborates with entities but does not share own information. On the repeatable tier, cybersecurity is expressed as enforced policies force, that are conducted on regular basis. Here, processes are "*defined, implemented as intended, and reviewed"*. As well, a complete collaboration exists with third-party entities. On the final tier, adaptive, it goes beyond a normal cybersecurity risk management to cover predictive incidents. Here, the previous tiers are also used but with a wider scope, since the organization collaborates with external entities, and performs a "*real-time or near real-time"* analysis to keep the processes fresh and ready for all risks.

The third and last part of the framework is Profiles. *"A profile is the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization. A Profile enables organizations to establish a roadmap for* *reducing cybersecurity risk that is well aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities. Given the complexity of many organizations, they may choose to have multiple profiles, aligned with particular components and recognizing their individual needs"*. Profiles are used mainly to describe the current situation and the targeted one, thus to reveal the gaps, and to set up for the future goals. This mainly helps in organization and prioritization of the activities.

Table 11 below gives an overview about the NIST CSF framework, the concerned topics, the detailed practices, and the way it helps managing cyber threats.

Table 11: NIST CSF overview

CSF Part 3		
Profiles	Current Profile	
	Target Profile	
CSF Part 2		
Tiers	Partial	
	Risk Informed	
	Repeatable	
	Adaptive	
CSF Part 1		
Function	Category	Subcategory
Identify	Asset Management	Physical devices and systems
		Software platforms and applications
		Organization communication and data flow
		External information
		Resources
		Cybersecurity roles and responsibilities
	Business Environment	The role in the supply chain
		The place in critical infrastructure and industry sector
		Priorities (mission, objectives, and activities)
		Dependencies and critical functions
		Resilience requirements
	Governance	Organizational information security policy
		Coordination of information security roles and responsibilities
		Legal and regulatory requirements
		Governance and risk management processes

	Risk Assessment	Asset vulnerabilities
		Threats
		Potential business impacts
		Risks (threats, vulnerabilities, likelihoods, and impacts)
		Risk responses
	Risk Management Strategy	Risk management processes
		Risk tolerance determined
		Risk tolerance informed
Protect	Access Control	Identities and credentials management
		Physical access management
		Remote access management
		Access permissions, and privileges
		Network integrity protection
	Awareness and Training	Users informed and trained
		Users understanding or roles and responsibilities
		Third-party understanding of roles and responsibilities
		Senior executives understanding of roles and responsibilities
		Security personnel understanding of roles and responsibilities
	Data Security	Data-at-rest protected
		Data-in-transit protected
		Assets management
		Availability maintained
		Data leak protection
		Integrity checking mechanisms for software
		Development and testing environment isolation
		Integrity checking mechanisms for hardware
	Information Protection Process and Procedures	Baseline configuration
		System development life cycle
		Configuration change control
		Backups
		Policy and regulations
		Data destruction policy
		Continuous protection processes
		Effectiveness of protection technologies
		Response and recovery plans management
		Response and recovery plans tested

		Cybersecurity inclusion in human resources practices
		Vulnerability management plan implementation
	Maintenance	Organizational assets maintenance and repair plans
		Remote assets maintenance and repair plans
	Protective Technology	Audit/log records implementation and documentation
		Removable media protection and user restriction policy
		The least functionality principle incorporated
		Communication and control networks protection
		Pre-defined functional states for availability maintenance
Detect	Anomalies and Events	Network operation and data flow baselining
		Detected events analysis
		Events data collection and correlation
		Events impact
		Incidents alerts and thresholds
	Security Continuous Monitoring	Network monitoring
		Physical environment monitoring
		Personnel activity monitoring
		Malicious code detection
		Unauthorized mobile code detection
		External service providers’ activities monitoring
		Monitoring of the unauthorized personnel, devices, and software
		Vulnerability scans
	Detection Processes	Roles and responsibilities for detection
		Detection activities compliance
		Detection processes tested
		Event detection communication
		Detection processes improvement
Response	Response planning	Response plan execution
	Communications	Personnel response awareness
		Reporting
		Information sharing
		Response plans coordination
		Cybersecurity awareness and information sharing
	Analysis	Detection systems notification and investigation

		Incident impact understanding
		Forensics
		Incident categorization
		Processes establishment
	Mitigation	Incidents containment
		Incidents mitigation
		Mitigation and documentation of newly identified vulnerabilities
	Improvement	Response plans build up on previous incidents
		Response strategies update
Recover	Recovery Planning	Recovery plan execution
	Improvements	Recovery plans build up on previous incidents
		Recovery strategies update
	Communications	Public relations management
		Reputation gaining
		Recovery activities communicated

5.4 ISF Standard of Good Practice for Information Security SoGP

The Information Security Forum ISF is an independent, not-for-profit association that concerns the information security from a neutral perspective. What makes their work of high reputation is that in contrast to the other standards that focus more on concepts, ISF targets the real implementations and technologies. The goal of this standard is to provide for high security in practice, and thus the name “Standard of Good Practice”.

ISF has its own security model, which comprises of six levels, namely Governance, Risk, Compliance, People, Process, and Technology, as defined as follows:

1. *Governance is the framework by which policy and direction is set, providing executive management with assurance that security management activities are being performed correctly and consistently.*
2. *Risk is the potential business impact and likelihood of particular threats materializing – and the application of controls to mitigate risks to acceptable levels.*
3. *Compliance is the policy, statutory and contractual obligations relevant to information security, which must be met to operate in today’s business world to avoid civil or criminal penalties and mitigate risk.*
4. *People are the executives, staff and external parties with access to information, who need to be aware of their Information Security responsibilities and requirements, and whose access to systems and data need to be managed.*
5. *Process is the business processes, applications, and data that support the operations and decision-making.*
6. *Technology is the physical and technical infrastructure, including networks and endpoints, required to support the successful deployment of secure processes.*

About the standard, SoGP mainly focuses on how the IT and IS can benefit the organization’s business, and support its processes. The standard covers six aspects of IS, Security Management SM, Critical Business Applications CB, Computer Installation CI, Networks NW, Systems Development SD, and End User Environment UE. *“Computer Installations and Networks provide the underlying infrastructure on which the Critical Business Applications run. The End User Environment covers the arrangements associated with protecting corporate and desktop applications, which are used by individuals to process information, and support business processes. Systems Development deals with how new applications are created and Security Management addresses high-level direction and control”.* Furthermore, these aspects are classified into areas that cover the general concepts, and further sections that extensively go more in depth. The structure of the SoGP standard, and the relationships between the different aspects are shown in Figure 13, and in Table 12 afterwards the areas and sections are also given.

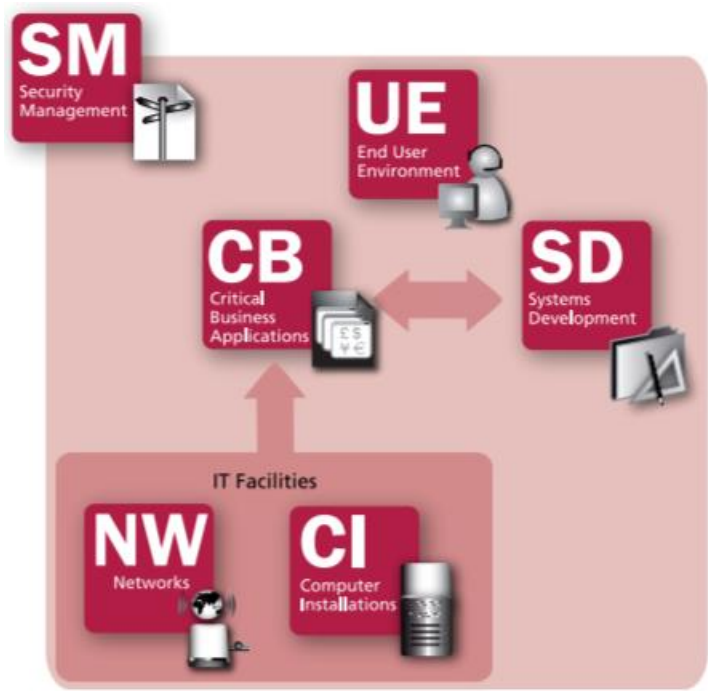

Figure 13: The relation between the SoGP aspects

Table 12: ISF SoGP overview

Aspect	Area	#	Section
Security Management	High-Level Direction	SM1.1	Management commitment
		SM1.2	Information security policy
		SM1.3	Staff agreements
	Security Organization	SM2.1	High-level control
		SM2.2	Information security function
		SM2.3	Local security co-ordination
		SM2.4	Security awareness
		SM2.5	Security education / training
	Security Requirements	SM3.1	Information classification
		SM3.2	Ownership
		SM3.3	Managing information risk analysis
		SM3.4	Information risk analysis methodologies
		SM3.5	Legal and regulatory compliance
	Secure Environment	SM4.1	Security architecture
		SM4.2	Information privacy

		SM4.3	Asset management
		SM4.4	Identity and access management
		SM4.5	Physical protection
		SM4.6	Information security incident management
		SM4.7	Business continuity
	Malicious Attack	SM5.1	General malware protection
		SM5.2	Malware protection software
		SM5.3	Intrusion detection
		SM5.4	Emergency response
		SM5.5	Forensic investigations
		SM5.6	Patch management
	Special Topics	SM6.1	Cryptographic solutions
		SM6.2	Public key infrastructure
		SM6.3	E-mail
		SM6.4	Remote working
		SM6.5	Third party access
		SM6.6	Electronic commerce
		SM6.7	Outsourcing
		SM6.8	Instant messaging
	Management Review	SM7.1	Security audit / review
		SM7.2	Security monitoring
Critical Business Applications	Business Requirements for Security	CB1.1	Confidentiality requirements
		CB1.2	Integrity requirements
		CB1.3	Availability requirements
	Application Management	CB2.1	Roles and responsibilities
		CB2.2	Application controls
		CB2.3	Change management
		CB2.4	Information security incident management
		CB2.5	Business continuity
		CB2.6	Sensitive information
	User Environment	CB3.1	Access control
		CB3.2	Application sign-on process
		CB3.3	Workstation protection
		CB3.4	Security awareness

	System Management	CB 4.1	Service agreements
		CB4.2	Resilience
		CB4.3	External connections
		CB4.4	Backup
	Local Security Management	CB5.1	Local security co-ordination
		CB5.2	Information classification
		CB5.3	Information risk analysis
		CB5.4	Security audit / review
	Special Topics	CB6.1	Third party agreements
		CB6.2	Cryptographic key management
		CB6.3	Public key infrastructure
		CB6.4	Web-enabled applications
Computer Installation	Installation Management	CI1.1	Roles and responsibilities
		CI1.2	Service agreements
		CI1.3	Asset management
		CI1.4	System monitoring
	Live Environment	CI2.1	Installation design
		CI2.2	Security event logging
		CI2.3	Host system configuration
		CI2.4	Workstation protection
		CI2.5	Resilience
		CI2.6	Hazard protection
		CI2.7	Power supplies
		CI2.8	Physical access
	System Operation	CI3.1	Handling computer media
		CI3.2	Back-up
		CI3.3	Change management
		CI3.4	Information security incident management
		CI3.5	Emergency fixes
		CI3.6	Patch management
	Access Control	CI4.1	Access control arrangements
		CI4.2	User authorization
		CI4.3	Access privileges
		CI4.4	Sign-on process

		CI4.5	User authentication
	Local Security Management	CI5.1	Local security co-ordination
		CI5.2	Security awareness
		CI5.3	Information classification
		CI5.4	Information risk analysis
		CI5.5	Security audit / review
	Service Continuity	CI6.1	Contingency plans
		CI6.2	Contingency arrangements
		CI6.3	Validation and maintenance
Networks	Network Management	NW1.1	Roles and responsibilities
		NW1.2	Network design
		NW1.3	Network resilience
		NW1.4	Network documentation
		NW1.5	Service providers
	Traffic Management	NW2.1	Configuring network devices
		NW2.2	Firewalls
		NW2.3	External access
		NW2.4	Wireless access
	Network Operations	NW3.1	Network monitoring
		NW3.2	Change management
		NW3.3	Information security incident management
		NW3.4	Physical security
		NW3.5	Back-up
		NW3.6	Service continuity
		NW3.7	Remote maintenance
	Local Security Management	NW4.1	Local security co-ordination
		NW4.2	Security awareness
		NW4.3	Information classification
		NW4.4	Information risk analysis
		NW4.5	Security audit / review
	Voice Networks	NW5.1	Voice network documentation
		NW5.2	Resilience of voice networks
		NW5.3	Special voice network controls
		NW5.4	Voice over IP (VoIP) networks
Systems	Development Management	SD1.1	Roles and responsibilities
		SD1.2	Development methodology

Development		SD1.3	Quality assurance
		SD1.4	Development environments
	Local Security Management	SD2.1	Local security co-ordination
		SD2.2	Security awareness
		SD2.3	Security audit / review
	Business Requirements	SD3.1	Specification of requirements
		SD3.2	Confidentiality requirements
		SD3.3	Integrity requirements
		SD3.4	Availability requirements
		SD3.5	Information risk analysis
	Design and Build	SD4.1	System design
		SD4.2	Application controls
		SD4.3	General security controls
		SD4.4	Acquisition
		SD4.5	System build
		SD4.6	Web-enabled development
	Testing	SD5.1	Testing process
		SD5.2	Acceptance testing
	Implementation	SD6.1	System promotion criteria
		SD6.2	Installation process
		SD6.3	Post-implementation review
End User Environment	Local Security Management	UE1.1	Roles and responsibilities
		UE1.2	Security awareness
		UE1.3	User training
		UE1.4	Local security co-ordination
		UE1.5	Information classification
	Corporate Business Applications	UE2.1	Access control
		UE2.2	Application sign-on process
		UE2.3	Change management
	Desktop Applications	UE3.1	Inventory of desktop applications
		UE3.2	Protection of spreadsheets
		UE3.3	Protection of databases
		UE3.4	Desktop application development
	Computing Devices	UE4.1	Workstation protection
		UE4.2	Hand-held devices
		UE4.3	Portable storage devices

	Electronic Communications	UE5.1	General controls
		UE5.2	E-mail
		UE5.3	Instant messaging
		UE5.4	Internet access
		UE5.5	Voice over IP (VoIP) networks
		UE5.6	Wireless access
	Environment Management	UE6.1	Information privacy
		UE6.2	Information security incident management
		UE6.3	Backup
		UE6.4	Physical and environmental protection
		UE6.5	Business continuity

On threats, the SoGP gives a comprehensive threat classification according to their source and intentionality. This is shown in the table below.

External attack	Carrying out denial of service attacks
	Hacking
	Undertaking malicious probes or scans
	Cracking passwords
	Cracking keys
	Defacing web sites
	Spoofing web sites
	Spoofing user identities
	Modifying network traffic
	Eavesdropping
	Distributing computer viruses (including worms)
	Introducing Trojan horses
	Introducing malicious code
	Carrying out social engineering
	Distributing SPAM
Internal misuse and abuse	Gaining unauthorized access to systems or networks
	Changing system privileges without authorization
	Changing or adding software without authorization
	Modifying or inserting transactions, files or databases without authorization
	Misusing systems to cause disruption

	Misusing systems to commit fraud
	Downloading or sending of inappropriate content
	Installing unauthorized software
	Disclosing authentication information
	Disclosing business information
Theft	Software piracy
	Theft of business information
	Theft of identity information (e.g. as a result of Phishing)
	Theft of computer equipment
	Theft of portable computers and storage devices
	Theft of authentication information
	Theft of software
System malfunction	Malfunction of business application software developed in-house
	Malfunction of business application software acquired from an external party
	Malfunction of system software
	Malfunction of computer / network equipment
Service interruption	Damage to or loss of computer facilities
	Damage to or loss of communications links / services
	Loss of power
	Damage to or loss of ancillary equipment
	Natural disasters
	System overload
Human error	User errors
	IT / network staff errors
Unforeseen effects of changes	Unforeseen effects of introducing new/upgraded business processes
	Unforeseen effect of changes to software
	Unforeseen effect of changes to business information
	Unforeseen effect of changes to computer / communications equipment
	Unforeseen effects of organizational changes
	Unforeseen effects of changes to user processes or facilities

5.5 Other standards

It is not only limited the above-mentioned standards, there are many others that share the same concepts, but target specific industries or criteria. For instance:

1. IEC/ISO 27001
2. IEC/ISO 27002
3. IETF RFC 2196
4. ISACA COBIT 5
5. Congress Cybersecurity Enhancement Act CEA of 2014