D1.3. Report on taxonomy of the CI environments

WP1. Adaptation of security components to Critical Infrastructure environments

CIPSEC

Enhancing Critical Infrastructure Protection with innovative SECurity framework

Due date: 31-10-2016

Actual submission date: 28-10-2016

HORIZON 2020. WORK PROGRAMME 2014 – 2015			Project No	700378
Call			Instrument	Innovation action
Digital Security: Cybersecurity, Privacy and Trust			Start date	May 1st, 2016
Secure societies. Protecting freedom and security of Europe and its citizens			Duration	36 months
DS-03-2015: The role of ICT in Critical Infrastructure Protection			Website	www.cipsec.eu
Public	Confidential	Classified	Lead contractor Atos SPAIN S.A.	

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement no 700378.

Document contributors

Editor	FORTH		
Contributors			**Reviewers**
Vasilis Prevelakis		AEGIS	Ilias Spais
Fernando Carmona		ATOS	
Ciprian Oprisa		BD	
Amir Atzmon		COMSEC	
Vittorio Vallero		CSI	
Christian Schlehuber		DB	
Panagiotis Sifniadis		EMP	
Sotiris Ioannidis, Christos Papachristos, Antonis Krithinakis		FORTH	
Ferran Rodriguez		HCPB	
Markus Heinrich		TUD	Neeraj Suri
Eva Marín, Xavi Masip, Sarang Kahvazadeh		UPC	
Kostas Lampropoulos		UOP	
Andrea Bartoli		WOS	

Document history

Version	Date	Author	Notes
0.1	10-10-2016	Ilias Spais	Internal review
0.2	25-10-2016	Neeraj Suri	Internal approval
1.0	28-10-2016	Fernando Carmona	Final check

Index

1 Acronyms

ACH	Automated Clearing Houses
ATM	Automated Teller Machine
AWWA	American Water Works Association
BYOD	Bring Your Own Device
CATO	Corporate Account Takeover
CD	Compact Disc
CI	Critical Infrastructure
COTS	Commercial Off-The-Shelf
CSET	Cyber Security Evaluation Tool
CSSP	Control Systems Security Program
CSWG	Cyber Security Working Group
DCS	Distributed Control System
DDOS	Distributed Denial of Service
DER	Distributed Energy Resources
DHS	Department of Homeland Security
DMZ	Demilitarized Zone (Computing)
DNP3	Distributed Network Protocol
DoD	US Department of Defense
DVD	Digital Video Disc
ENISA	European Network and Information Security Agency
ERNCIP	European Reference Network for Critical Infrastructure Protection
EU	European Union
HCB	Hospital Clinic de Barcelona
HL7	Health Level Seven International
HMI	Human Machine Interface
ICS	Industrial Control Systems
ICTC	Information and Communications Technology Council
ICT	Information and Communication Technology
IDS	Intrusion Detection Systems
IED	Improvise Explosive Device
IED	Intelligent Electronic Devices
IPS	Intrusion Prevention Systems
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
ITU	International Telecommunication Union
LAN	Local Area Network
NCSS	National Cyber Security Strategy

NERC	North American Electric Reliability Corporation
NIPP	US National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
OT	Operational Technology
PACS	Picture Archiving and Communication System
PCI-DSS	Payment Card Industry Data Security Standard
PDF	Portable Document Format
PLC	Programmable Logic Controller
RFID	Radio Frequency Identification
RF	Radio Frequency
RSC	Nuclear Roadmap Steering Committee
RTU	Remote Terminal Units
SCADA	Supervisory Control and Data Acquisition
SoA	Statement of Applicability
SQL	Structured Query Language
USB	Universal Serial Bus
US	United States
VLAN	Virtual Local Area Network
VOIP	Voice over Internet Protocol
WAN	Wide Area Network
WMD	Weapon of Mass Destruction
WSSC	Water Sector Coordinating Council
XSS	Cross-Site Scripting

2 Executive summary

CIPSEC proposes a security framework for Critical Infrastructures (CI). Partners contributing security solutions will demonstrate the added value of their solutions when applied on the Critical Infrastructures that are provided by the respective pilot partners. Pilot partners include the Health, Transportation, and Environment CI domains. Deliverable D1.3 “Report on taxonomy of the CI environments”, presents a taxonomy on Critical Infrastructures in general as well as their major cyber security related issues. Specifically, the report:

- Identifies CI domains as defined by various national and other reports.
- Identifies commonalities and differences among the various CIs.
- Presents the interdependencies of the various CI domains.

The sources used to compile the document clearly present that CIs are suffering from many external and internal threats. CIs are more and more relied upon by new ICT technologies to improve efficiency and increase productivity. This has increased the attack surface of our systems and services for malicious users. The report presents each CIs requirements for additional security measures at various levels.

3 Introduction

This deliverable describes a taxonomy of different CI environments according to their needs and what their respective communities expect should be protected against Cyber-attacks. The current report will be used in order to properly tailor the CIPSEC design to the set of target CIs.

Although the "*Critical infrastructure is the backbone of our nation's economy, security, and health*"[1] more than 50% of the companies and industries that use or own Critical Infrastructures have been affected by data theft (fig. 1), industrial espionage or sabotage as presented in the report titled "The challenge of Cyber security"[2].

Figure 1 Percentage of companies by industry affected by data theft, industrial espionage, or sabotage within the past two years

[1] https://www.dhs.gov/topic/critical-infrastructure-security

[2] http://www.oliverwyman.com/content/dam/oliver-wyman/global/en/2016/feb/2016_Oliver_Wyman_Perspectives_The_challenge_of_cybersecurity.pdf

The above provide a clear view of the status of the various CIs regarding the Cyber-attacks and threats that they face, and the importance of addressing Cybersecurity. On average, more than 50% of the companies surveyed (from various CI domains) have been victims of such Cyber security issues. The CI domains are more and more relying on the ICT domain (which is also identified as a CI domain in many reports). Their interdependence with the ICT domain is something that all sectors need in order to evolve and grow in a market which goes global. So special care should be provided to services used for communication and data exchange via public/private and other networks.

We initially conducted surveys for the state-of-the-art utilizing reports for various countries in order to gain an overview insight of the various types of the CI domains. The more comprehensive reports we studied include US reports and ENISA reports which include information about a great number of EU countries. That way, we identified common CI domains that are of high importance. Based on those domains we further searched and studied specific reports for each one of these CIs. There is a large volume of information for those CIs covering many aspects beside Cyber Security. We went a step further and filtered out the information which is relevant for the CIPSEC project. The aim was to include Cybersecurity-related aspects for those CIs that are important for the CIPSEC goals. For completeness, the document also reports on domains that are narrow focused, identified by e.g. one country without any accompanying Cybersecurity-related information . Based on the findings we extract information with common Cybersecurity concerns and identify what is important for the CIs that need to be protected against potential Cyber-attacks and threats. This is graphically presented by matrices and graphs in the last section of this report. The Acronyms section can be found on the first pages of the document.

The report was structured as following. The reports presenting various CIs per country are summarized in Sections 4 and 5). Section 6 studied, analyzed and presents eleven CI domains regarding their Cybersecurity related concerns and needs. Section 7 was based on the findings of Section 6 and presents the common Cybersecurity elements and services for the CI domains.

4 Critical Infrastructure domains (EU)[1]

In the last couple of years many European countries published strategic contributions[2] aimed at identifying their Critical Infrastructures and how they should proceed to tackle with possible Cybersecurity risks, referred to as National Cyber Security Strategy (NCSS) documents. NCSS is a key policy document including the means and procedures each state should deploy to face Cybersecurity risks. Nowadays, twenty (20) European Union Member States have already published a NCSS. In the next paragraphs we present various Critical Infrastructures on a per EU country basis, thus showing a clear snapshot of different Critical Infrastructures existing in EU and non-EU countries.

According to the relevant ENISA document[1], countries like Austria, Cyprus, Czech Republic, Estonia, Finland, Hungary, Latvia, Lithuania, Slovenia, Switzerland and United Kingdom[3] have compiled such reports and identified their CIs, though not listed in the ENISA report. On the other hand, CI for countries like France, The Netherlands, Poland and Spain have been listed in the ENISA report. This was performed by retrieving information from the respective NCSS documents. The following subsections include Critical Infrastructures for some EU countries (mainly reported in the ENISA report and other sources) and Critical Infrastructures for some non-EU countries as well, for completeness (Section 5). Then we produce some tables/matrices similar to the one ENISA has provided in their document. Although the naming is different in each country, in most of cases they tend to represent similar infrastructures and concerns. The CI domain naming used in the following country-related sections is the same as the ones used in the respective ENISA and NCSS documents. In order to simplify and better represent the results and findings, some CI domains have been grouped in the comparison tables.

4.1 France Critical Infrastructures

The list below presents the CI domains that are most important for France. Those domains are listed in the ENISA report.

1. Civil activities
2. Judicial activities
3. Military activities
4. Food
5. Electronic, audiovisual and information communications
6. Energy
7. Space and research
8. Finance
9. Water management
10. Industry
11. Health
12. Transportation

4.2 The Netherlands Critical Infrastructures

The Netherlands also presents its own CIs. The common ones include: Energy, ICT, Water, Food, Health, Finance, Public administration and armed forces.

[1] https://resilience.enisa.europa.eu/enisas-ncss-project/CIIPApproachesNCSS.pdf

[2] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/

[3] http://www.cpni.gov.uk/about/cni/

1. Energy: electricity, natural gas and oil
2. Telecommunication and ICT: land line and mobile telephony, radio, broadcasting and the internet
3. Drinking water: the water supply
4. Food: the food supply (including in supermarkets) and food safety
5. Health: emergency and hospital care, medicines, vaccines
6. Financial sector: payments and money transfers by public bodies
7. Surface water management: water quality and quantity (control and management)
8. Public order and safety
9. Legal order: the courts and prisons; law enforcement
10. Public administration: diplomacy, public information, the armed forces, decision-making
11. Transport: Amsterdam Schiphol Airport, the port of Rotterdam, highways, waterways, railways
12. The chemical and nuclear industries: the transport, storage, production and processing of materials.

4.3 Poland Critical Infrastructures

Poland has identified eleven CI domains that is interested in. The common with other countries include: Energy, Communication (ICT), Finance, Food, Water, Health, Transportation, Public administration and Chemical domain.

1. Energy, fuel and energy supply systems,
2. Communication systems,
3. Tele-information network systems,
4. Financial systems,
5. Food supply systems,
6. Water supply systems,
7. Health protection systems,
8. Transportation systems,
9. Rescue systems,
10. Systems ensuring the continuity of public administration activities,
11. Systems of production, storing and use of chemical and radioactive substances, including pipelines for dangerous substances.

4.4 Spain Critical Infrastructures

Spain has also identified the twelve CI domains that is interested in and the common ones include: Administration, Chemical, Energy, Finance, Food, Health, ICT, nuclear (with France only), Transportation and Water.

1. Administration
2. Chemical Industry
3. Energy
4. Financial and Tax System
5. Food Supply Chain
6. Health

7. Information and Communication Technologies (ICT)
8. Nuclear Industry
9. Research Laboratories
10. Space
11. Transport
12. Water

The ENISA report goes a step further and produces a matrix (Figure 2) with CI domains that exist in each country. The CI domain names used in Figure 2 are more generic and used to aggregate the various names used for the CIs which more or less represent similar infrastructures. We will initially use the ENISA approach which provides more comprehensive and easy to understand results.

	Energy	Water	Food	Health	Finance	Transport	Public admin.	ICT	Civil admin	Space & research
AT	x	x	x	x	X	x	x	x	x	
CY	x	x		x	X		x	x	x	
CZ	x	x	x		X	x	x	x	x	
EE	x	x	x	x	X	x	x	x	x	
FI	x	x	x	x	X	x	x	x		
FR	x	x	x	x	X	x	x	x	x	x
HU	x	x	x	x	X	x	x	x		
LV	Not applicable									
LT	x	x	x	x	X	x		x		

NL	x	x	x		X	x		x	x	
PL	x	x	x	x	X	x		x		
SI	x	x	x	x	X	x		x		
ES	x	x	x	x	X	x	x	x	x	x
CH	x	x	x	x	X	x	x	x	x	
UK	x	x	x	x	X	x		x		

Figure 2 Critical Infrastructures pes EU country that has published a NCSS

Regarding the Latvian case, the report mentions the following: “The Latvian approach to CI does not rely on specified critical sectors; rather, any infrastructure found to meet the criteria of criticality can be designated as critical infrastructure.”

4.5 Germany Critical Infrastructures[1]

According to the Germany Federal government the definition of CI is the following: “Critical infrastructures are organizational and physical structures and facilities of such vital importance to a nation’s society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences.” Organizations and facilities that are involved in the below areas are characterized and identified as CIs. Those areas include:

1. Energy
2. Health
3. Information Technology and Telecommunication
4. Transport and Traffic
5. Media and Culture
6. Water
7. Finance and Insurance
8. Food
9. State and Administration

4.6 Italy Critical Infrastructures[2]

We have also included Italy’s CI domains in order to produce a new graph similar to that in the ENISA document. According to the “Network Security in Critical Infrastructures” produced by many stakeholders of Italy the following eleven CI domains have been identified:

1. Energy transmission and distribution networks (electricity, gas, etc.)
2. Telecommunication networks
3. Transport systems (goods and passengers)
4. Emergency services
5. Defense infrastructures
6. Banking and financial circuits
7. National health care services
8. Water transport, distribution and treatment systems
9. Media and public information networks
10. Farming and food processing industries
11. Government networks

[1] http://www.kritis.bund.de/SubSites/Kritis/EN/introduction/introduction_node.html

[2] http://www.isticom.it/documenti/news/pub_003_eng.pdf

4.7 Greece Critical Infrastructures

The formal NCSS framework for Greece is not available yet. There is a study from a non-profit organization[1] which summarizes infrastructures of Greece that could be identified as critical. The study mentions 13 possible infrastructure domains that could potentially be identified as CI domains.

1. Energy
2. ICT – Communications
3. Water
4. Food
5. Health
6. Finance
7. Public safety and security
8. Transportation
9. Industry
10. Public administration
11. Civil administration
12. Environment
13. Defense

Below, there is an extended table with information from the ENISA reports. We have added three more EU member countries and their Critical Infrastructures. These countries are Germany, Italy and Greece.

Country	Energy	Water	Food	Health	Finance	Transport	Public Admin	ICT	Civil Admin	Space & Research
AT	X	X	X	X	X	X	X	X	X	
CY	X	X		X	X		X	X	X	
CZ	X	X	X		X	X	X	X	X	
EE	X	X	X	X	X	X	X	X	X	
FI	X	X	X	X	X	X	X	X		
FR	X	X	X	X	X	X	X	X	X	X
HU	X	X	X	X	X	X	X	X		
LT	X	X	X	X	X	X		X		
NL	X	X	X		X	X		X	X	
PL	X	X	X	X	X	X		X		
SI	X	X	X	X	X	X		X		

[1] http://www.dianeosis.org/wp-content/uploads/2016/06/infrastucture_paradoteo2_Version_020616_3.pdf

Country	Energy	Water	Food	Health	Finance	Transport	Public Admin	ICT	Civil Admin	Space & Research
ES	X	X	X	X	X	X	X	X	X	X
CH	X	X	X	X	X	X	X	X	X	
UK	X	X	X	X	X	X		X		
+ EU										
DE	X	X	X	X	X	X	X	X	X	
IT	X	X	X	X	X	X	X	X	X	
GR	X	X	X	X	X	X	X	X	X	

Figure 3 Extended list of EU countries and their CI domains. DE IT and GR have been included

There is a clear overlap between the CI domains identified by the three added countries with the CI domains reported in the ENISA table (for the remaining EU countries). Some countries prefer to split CI domains in more than one, like the ICT case, where other countries handle IT and Communications separately, such are handled as one in this report. Moreover, we also see that the Transportation and Health pilots of CIPSEC are included in all countries. We can claim the same for the Environment pilot which is included probably under the large Water CI domain. This means that the CIPSEC framework, through the provision of security solutions via its three pilots, will be able to offer its services to the majority of the EU countries and their CIs as reported in the table above.

5 Critical Infrastructure domains (Non-EU)

5.1 Critical Infrastructure domains (US)[1]

The United States, and specifically the Department of Homeland Security[1], have identified sixteen distinct Critical Sectors. They have compiled documents for each Critical Sector in order to properly describe them. The reported documents include information about what is included in each sector, their features, security issues (in general) that should be taken into consideration while some of them also address aspects related to Cybersecurity. Reports for specific CI domain are not available for EU and other countries. Below, we list the set of identified sectors, some of them not yet reported by public EU documents:

1. Chemical Sector
2. Commercial Facilities Sector
3. Communications Sector
4. Critical Manufacturing Sector
5. Dams Sector
6. Defense Industrial Base Sector
7. Emergency Services Sector
8. Energy Sector
9. Financial Services Sector
10. Food and Agriculture Sector
11. Government Services Sector
12. Healthcare and Public Health Sector
13. Information Technology Sector
14. Nuclear Reactors, Materials, and Waste Sector
15. Transportation Sector
16. Water and Wastewater Systems Sector

5.2 Critical Infrastructure domains (Japan)[2]

In 2009 the Information Security Policy Council of Japan compiled a document named “The Second Action Plan on Information Security Measures for Critical Infrastructures”. The report was created by organizations interested in Critical Infrastructures or already operating them. The government and the 10 sectors of Critical Infrastructure were identified for Japan. The report aimed at “minimizing the occurrence of IT malfunction in Critical Infrastructures. The ten CIs identified are the following:

1. Information communication
2. Finance
3. Aviation
4. Railway
5. Electric power

[1] https://www.dhs.gov/critical-infrastructure-sectors

[2] http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v2.pdf

6. Gas
7. Government and administrative services
8. Medical
9. Water service
10. Logistics

5.3 Critical Infrastructure domains (Australia)[1]

In 2014 five countries (US, Australia, New Zealand, Canada and United Kingdom) compiled a document that includes information about their CIs. The reported information was used for "identifying common CIs, similarities in definition, approach, concept, and implementation in order to arrive at a shared understanding of critical infrastructure." We retrieved information about the Australian and Canada (see subsection 5.4) CIs from that report.

1. Banking and Finance
2. Communications
    a. Broadcast media
    b. Postal services
    c. Telecommunication networks
3. Energy
    a. Electricity systems
    b. Offshore oil and gas
    c. Onshore oil and gas
    d. Coal supply
4. Food chain
5. Health
6. Transport
    a. Aviation
    b. Land based mass passenger transport
    c. Land freight
    d. Maritime: Shipping and ports
7. Water services
8. Other CIs
    a. Labs holding high risk biological agents
    b. Chemical manufacturing industry
    c. Defence industries
    d. Emergency Service

[1] http://www.infrastructure.govt.nz/publications/critical5/crit5-narrative-v2.pdf

5.4 Critical Infrastructure domains (Canada)[1]

From the same report (like in the case for Australia) we list the CIs for Canada:

1. Energy and Utilities
2. Information and Communication Technology
3. Finance
4. Manufacturing
5. Food
6. Safety
7. Government
8. Transportation
9. Health
10. Water

5.5 Critical Infrastructures per country

Based on the aforementioned sections which present the Critical Infrastructures per country we provide below an extended ENISA style table with enhanced information gathered from non-EU countries like United States, Japan, Australia and Canada. According to the table, we observe that most of the CIs are present to those non-EU countries as well and match to the ones identified by the EU countries.

Country	Energy	Water	Food	Health	Finance	Transport	Public Admin	ICT	Civil Admin	Space & Research
AT	X	X	X	X	X	X	X	X	X	
CY	X	X		X	X		X	X	X	
CZ	X	X	X		X	X	X	X	X	
EE	X	X	X	X	X	X	X	X	X	
FI	X	X	X	X	X	X	X	X		
FR	X	X	X	X	X	X	X	X	X	X
HU	X	X	X	X	X	X	X	X		
LT	X	X	X	X	X	X		X		
NL	X	X	X		X	X		X	X	
PL	X	X	X	X	X	X		X		
SI	X	X	X	X	X	X		X		
ES	X	X	X	X	X	X	X	X	X	X
CH	X	X	X	X	X	X	X	X	X	

[1] http://www.infrastructure.govt.nz/publications/critical5/crit5-narrative-v2.pdf

Country	Energy	Water	Food	Health	Finance	Transport	Public Admin	ICT	Civil Admin	Space & Research
UK	X	X	X	X	X	X		X		
+ EU										
DE	X	X	X	X	X	X	X	X	X	
IT	X	X	X	X	X	X	X	X	X	
GR	X	X	X	X	X	X	X	X	X	
+ non-EU										
US	X	X	X	X	X	X	X	X		
JP	X	X		X	X	X	X	X		
AU	X	X	X	X	X	X		X		
CA	X	X	X	X	X	X	X	X		

Figure 4 Extended list with non-EU countries and their CI domains. US, JP, AU and CA have been included

As a conclusion from the various National reports presenting the CI domains of each country we can observe that there is clear overlap for many of them. It is evident that each country may select (based on its priorities) whether an infrastructure will be identified as a CI or not thus some CI domains are not visible to all countries (e.g. nuclear is visible only for Spain and France). Another observation is that there is no common naming strategy for the CI domains.

There are cases where Government Services and Public Administration more or less refer to the same institution. Moreover, we found valuable information regarding Chemical sectors which also may apply to Manufacturing sectors. The CI domains that can be marked as common by many of the countries from the reports studied, are the following: **Energy**, **Finance**, **Food**, **Water**, **Health**, **Transport**, **ICT** (including communications), **Administration** (including public/civil administration).

This deliverable aims to produce not only a taxonomy of CIs per country but also a taxonomy of CIs that could use the CIPSEC framework to improve their security against Cyber-threats and attacks. Thus, the next sections focus on those discrete CI domains and identify common features and elements that may be vulnerable to Cyber-attacks. By using this information, the CIPSEC partners will be able to provide Cybersecurity solutions to CI domains beyond the three already included in the consortium.

The respective reports we found addressing Cybersecurity aspects are related to the following CIs: **Energy**, **Finance**, **Food**, **Water**, **Health**, **Transport**, **ICT, Chemical, Manufacturing, Emergency services** and **Nuclear domain.** These are the CIs we used to identify what is important for them and how they address the Cybersecurity aspect.

6 Critical Infrastructure taxonomy

Previous sections presented CIs identified for some European and some non-European countries. Those CIs are mainly reported in their National Cyber Security Strategy (NCSS) documents. Sections below provide information about specific CIs and include (i) a brief description of each CI and what is included in each one of them and (ii) any reported characteristics or specific elements of those CIs that are vulnerable to Cyber-attacks and should be protected against them. Most of the NCSS documents refer to a list of the CI domains, while the US Homeland Security department has gone a step further and reports on specific characteristics of each CI domain. In some cases, those are security-related characteristics interesting for the current CIPSEC report. So in this section we list and analyze CI domains which address the aspect of Cyber Security. This is not the complete list of CIs but is a list of CIs for which we have found Cyber Security related information (Fig 5).

The target of this process was to identify commonalities between the CI domains. By studying all CI domains and their security related needs we were able to identify cases of CIs with common needs where CIPSEC security solutions could be directly (or with some modifications) applied and offer enhanced protection against threats and cyber-attacks. Those common concerns have been included in the next subsections for each CI domain studied and are summarized as a matrix in the next section (Section 7).

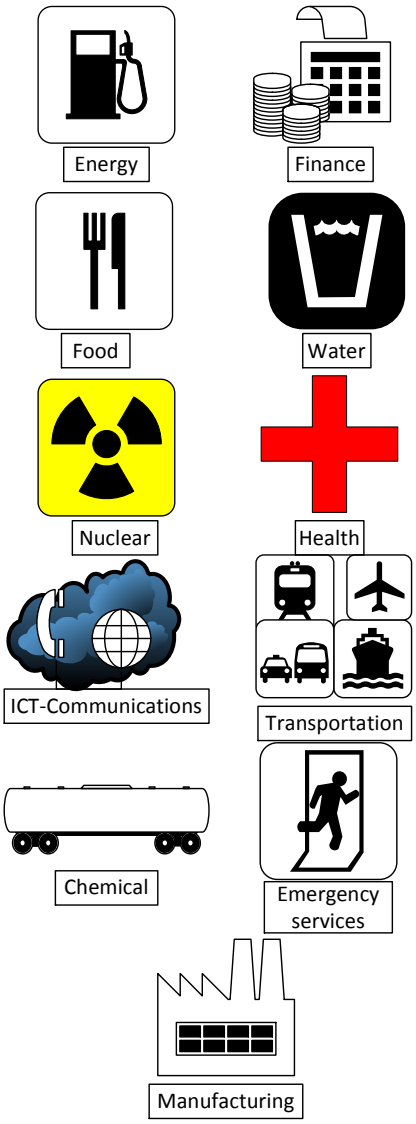
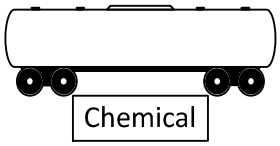


Figure 5 Common CIs identified per country.

6.1 Chemical industry



6.1.1 Overview and what is included

Although the Chemical CI is not a common CI among various countries according to the NCSS documents, we have found valuable Cybersecurity information and this is the reason to include it in this section. The domain of Chemical services is quite large and includes many sub-categories like agricultural chemicals, pharmaceuticals and consumer products. All of them make use and own CIs that should be protected against Cyber Security threats.

The Chemical Sector-Specific Plan-2015[1] that was released by the Department of Homeland Security[2], USA, identifies threats and sectors that should be taken under special care in order to improve the Cybersecurity of the Chemical Critical Infrastructure domain and its services. Those threats include:

- Insider Threats
- Cyber Threats
- Natural Disasters and Extreme Weather
- Deliberate Attacks and Terrorism
- Biohazards and Pandemics

The bullets marked in bold address the Cybersecurity related aspect that is interesting for the CIPSEC project thus we include the respective information in the sections below:

Insider Threat

This seems to be a quite common concern in many businesses and organizations. There are many common practices to establish Cyber and physical security systems that are able to prevent many of the well-known so called outsider threats. In case someone wants to address the issue of an insider threat then the case is different. There may be insiders with access to facilities and systems that could harm the services and the infrastructure either intentionally or unintentionally. Such businesses like the Chemical sector provide contracts to third parties for a variety of reasons thus providing to them access to services and facilities. Those contractors may not have been passed the same screening process such as the permanent staff.

Cyber Threats

The Chemical Sector includes systems that belong in the range of internal Industrial Control Systems (ICSs), to large national and international secure networks thus facing a variety of attacks including

- man-made deliberate attacks,
- technological failures,
- human errors and,
- supply chain vulnerabilities.

Any disruption to these systems and services could result to loss of operational capacity, chemical theft or release or theft of intellectual property. Although it is reported that ICSs which are updated through Internet accessible systems and third-party applications are not a lot, it does not mean that the risk of Cyber-attacks is not existent.

[1] https://www.dhs.gov/sites/default/files/publications/nipp-ssp-chemical-2015-508.pdf

[2] https://www.dhs.gov

Deliberate Attacks and Terrorism

The products and the materials used in the Chemical CI domain are target for attacks due to the damage that could perform (to people and the environment) if used for terrorism purposes. Chemical facilities, services and materials are also target for theft and diversion standalone or in a Weapon of Mass Destruction (WMD) and Improvise Explosive Device (IED).

The "Chemical Sector-Specific Plan-2015" report also studies the interdependencies and dependencies that the Chemical industry has with other CI domains. Those include Information Technology, Emergency Services, and Food and Agriculture. It is specifically noted that the Chemical sector is heavily relied upon new IT technologies, thus the interdependence with the ICT domain (and the technologies used) should be carefully studied in order to be protected against possible Cyber threats. The report mentions: "Information technology is a critical component of day-to-day chemical facility operations, including process control, supply tracking, storage of sensitive information, and automated safety and security systems control". The Chemical sector services should be protected against disruption in order for many other interdependent CIs and services to operate smoothly as well. For examples the Chemical CI also provides its products to Manufacturing (also reported as CI according to US).

6.1.2 Critical elements to protect

According to Guidance for Addressing Cyber Security in the Chemical Industry[1] the following nineteen items are important and should be addressed for the Chemical industry.

Importance of Cyber Security in Business, **Scope of Cyber Security Management System**, Security Policy, Organizational Security, Personnel Security, Physical and Environmental Security, Risk Identification, Classification, and Assessment, Risk Management and Implementation, Statement of Applicability (SoA), Incident Planning and Response, Communications, Operations and Change Management, Access Control, Information and Document Management, System Development and Maintenance, Staff Training and Security Awareness, Compliance, Business Continuity Plan, Monitoring and Reviewing CSMS, Maintaining and Implementing Improvements.

Among those aspects, the guide presents a "**Cyber Security Management System**" and what should be included in that. Such a system should also address the following (among other) and have practices for each one of those aspects:

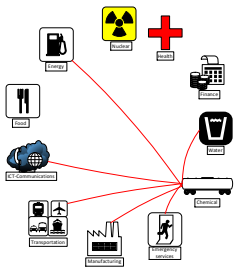
- Information systems (including operating systems, databases, applications of the company, including joint ventures and other third party business activities.
- Manufacturing and control systems (including Supervisory Control And Data Acquisition (SCADA), Programmable Logic Controller (PLC), Distributed Control System (DCS) and configuration workstations).
- Networks, local area networks (LANs), wide area networks (WANs) (including hardware, applications, firewalls, intrusion detection systems)
- User responsibilities (including policies to address authentication and auditability)
- Information protection (including access requirements and individual accountability)
- Risk management (including processes to identify and mitigate risks and document residual risk)
- Training requirements

Chemical CI domain is more or less interdependent with all the other CI domains either providing products and services or requesting products and services to continue its smooth operations. Reports mention that four of them are more crucial for the Chemical domain. Those CIs include Water, Transportation, Communications, and Energy as domains, services and resources that are essential for the Chemical domain.

[1] https://scadahacker.com/library/Documents/Best_Practices/CIDX%20-%20Guidance%20for%20Addressing%20Cybersecurity%20in%20the%20Chemical%20Sector.pdf

6.1.3 Sector dependencies

The following critical dependencies are identified for this sector:



- **ICT – Communications**: contact with transporters and daily business operations are conducted via communication networks. Moreover, operation such as process control, supply tracking, storage of sensitive information, and automated safety and security systems control are provided by the ICT sector.
- **Energy**: electricity and critical feedstocks, such as natural gas, are provided by the energy sector.
- **Transportation**: raw materials and chemicals products are transferred with transportation services.
- **Water**: manufacturing of chemicals requires large amounts of process and cooling water
- **Manufacturing**: electrical equipment, heavy machinery, transport equipment, and metals for use in chemical products or as catalysts in chemical processes are produced by the manufacturing sector.
- **Emergency Services**: for example, in an unexpected accident involving hazardous chemicals, emergency services can help ensure that adverse consequences will be minimized.

6.2 Information and Communications Technologies (ICT)

6.2.1 Overview and what is included

There are countries that identify two different CI domains, the Communications domain and the IT domain (Information Technologies) while other countries handle both domains as one. The same case applies for the reports that we have studied. We think that this domain is closely dependent to each other so we will handle it as one. The Communications Sector is a crucial component for the economy worldwide, and almost all businesses and operations are heavily relying on it. Over the last years, Communications have evolved enormously. The Communications sector started mainly as a voice service provider and has now (with the IT support) interconnected many business sectors and industrial systems. This target has been achieved using wired, satellite, and wireless transmission communication systems.

Among the many physical incidents that the sector should address like, major earthquakes, hurricanes, and space weather the sector also has to deal with many Cyber-disruptions. Cyber-disruptions of Communications and IT systems present unique challenges due to global connectivity. The exploitation of vulnerabilities can easily affect critical communications components in a couple of minutes thus affecting almost all of the other CIs as well.

IT alone from the other hand is currently an essential part of almost all the identified Critical Infrastructures. It is also the important glue that interconnects many components that form those CIs and the mediator of the CIs themselves. Additionally, IT is identified as one of the CI domains in almost every country as presented in the previous sections of this document. Many of the CI domains are heavily dependent on ICT thus establishing the need to secure ICT of high importance.

6.2.2 Critical elements to protect

The ITU National Cybersecurity Strategy Guide[1] has identified important technical measures that Telecommunications and Communications Sectors as a whole should consider in order to provide uninterruptable services to citizens and businesses.

- Uniform Access Management:
  - Centralized Authentication. The mechanism removes the need for local or host-based storage of credentials (passwords or certificates).
  - Centralized Authorization. This approach ensures that access to system resources is managed in a transparent and auditable way.
  - Secure logging of all events with respect to authentication and authorization.
  - Enforcement of complex passwords rules. Usage of strong passwords
  - Secure storage of all passwords.
- Secure Communications. Strong cryptographic ciphers should secure data, voice and mobile networks.
- Usage of DMZ. Provide variable depth security or zoning for untrusted services.
- Defense in Depth: use of multiple controls and different security products to mitigate security threats. (e.g firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and anti-virus software.
- Network Survivability. Should fulfill a minimum set of essential functionality in order to recover in a timely manner in case of attacks.

Cyber vulnerabilities is one of the four risks that affect the Communications domain according to "Communications Sector-Specific Plan, an Annex to the NIPP 2013[1]". Internet has been identified as the basic

1 http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

component used to integrate networks, service providers and suppliers that are part of the Communications Sector. It is clearly stated that ongoing attention and monitoring is needed to avoid failures of its hardware, software and operating systems.

Other important things to protect in this CI domain against cyber-attacks and threats are the following:

- Protect critical functions against threats. Especially those that will degrade confidentiality, integrity and/or the availability of them.
- Try to avoid unintentional activities that could e.g. disrupt the ISP services and intentional activities that could result in loss of interoperability of the systems.
- Another need that arises from industry about the ICT CI domain is related to attacks targeting Internet-based identity that may lead to financial losses and identity theft. Identities can then be used for
  - criminal activities and
  - unauthorized access to classified information and facilities.

According to a Cyber Security ICTC White Paper[2] the top three attack methods hackers employ to retrieve sensitive information are (i) Remote Access Application (ii) Third Party Connectivity and (iii) SQL Injection.

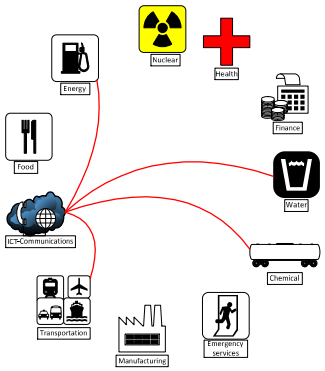
European Commission has also compiled a "Study on the availability and robustness of electronic communication networks"[3] presenting vulnerabilities of ICT infrastructures. A thorough list of vulnerabilities has been compiled including power, environment, software, hardware, payload, network, human and policy vulnerabilities. Four of those eight categories that could be vulnerable to potential threats could be used by potential cybersecurity attacks. Those are:

- Software vulnerabilities: the category include the complexity of programs used, errors in coding logic, the often need to patch existing code.
- Payload vulnerabilities: including authentication, encapsulation of malicious code, encryption (which prevents observability)
- Network vulnerabilities: including interoperability, interdependence and points of concentration subject to congestions and prone to DDoS attacks
- Human vulnerabilities: including, like other CIs, malicious users and misuse either intentionally or unintentionally.

6.2.3 Sector dependencies

The following critical dependencies are identified for this sector:

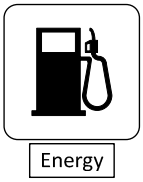
- **Chemical Industry**: provides chemicals needed for manufacturing electronic components such as microchips and displays.
- **Energy**: any ICT and communications infrastructure requires electric power to operate. Moreover, backup generators require fuel to operate.
- **Transportation**: networking equipment (routers, fiber-optic cable, etc.) is co-located along existing transportation routes, the destruction of which may impact service availability in wide geographic areas.
- **Water**: cooling processes



[1] https://www.dhs.gov/sites/default/files/publications/nipp-ssp-communications-2015-508.pdf

[2] http://www.ictc-ctic.ca/wp-content/uploads/2012/10/ICTC_CyberSecurityReport1.pdf

[3] http://ec.europa.eu/information_society/newsroom/cf/document.cfm?action=display&doc_id=290



6.3 Energy

6.3.1 Overview and what is included

The Energy Sector includes three subcategories. The US Homeland Security report includes electricity, oil, and natural gas under the Energy category. The same categories have been identified by the European Critical Infrastructure Directive[1]. According to ICIT[2] (Institute for Critical Infrastructure Technology) which is a "next-generation cybersecurity think tank cultivating a cybersecurity-centric renaissance" for Critical Infrastructure community, there is quite large and broad spectrum of threats[3] ("The Energy Sector Hacker Report") that could harm the Energy Sector. Those include insider threats, zero-day vulnerabilities, botnets, basic attack chain (e.g. sequence of simple events that exploit a vulnerability), and many more as listed below.

6.3.2 Critical elements to protect

The report of ICIT splits the Cybersecurity aspect in three (3) categories:

- Threat landscape,
- Threats, and
- Threat actors.

We will present below the most relevant one for our report including a short description for each one of them. The tables below include information about the first two categories ("Threat landscape and Threat types). The third category which is related to "Threat actors" includes hacktivists, cyberterrorists, and cybercriminals which have been identified as potential actors for attacks in the Energy CI domain. The tables below include additional information to assist the reader.

Threat Landscape	
IT-OT Convergence	ICT applications are more and more interconnected with SCADA, PLC, ICS and sensor systems
Human Machine Interface (HMI)	HMIs have unavoidable direct connections to backends which are also directly connected to PLCs. All are vulnerable to attacks (one target, multiple-side attacks).
Engineering Workstations	Workstations are usually interconnected and connected to the Internet, thus making them easy targets for the attackers
Programmable Logic Controllers	Like in the Engineering Workstations case, some PLCs can be accessed via inappropriately secured networks.
Historian Systems	Used to store data produced by sensors. Usually managed through the Enterprise network.

[1] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN

[2] http://icitech.org/

[3] http://icitech.org/icit-brief-the-energy-sector-hacker-report-profiling-the-hacker-groups-that-threaten-our-nations-energy-sector/

Threat Landscape	
Synchrophasor Technology	It is explicitly mentioned that this technology that is used for real-time operations is subject to cyber-attacks when not combined with Cybersecurity tools. The technology includes valuable information (regarding grid reliability) that could be exploited for a number of different purposes.
Distributed Energy Resources (DER)	Energy is produced by distributed facilities that are operated through networks for remote management and monitoring.
Smart Grid Technologies	Smart Grid Technologies are mostly used to increase the reliability of Grids. They are heavily dependent on automated processes which are often potential targets for attackers.
Cloud Computing Technologies	Cloud computing and storage enables the real time sharing of information between the relevant stakeholders. Such processes should be performed with special care because sensitive information is always a target for attackers. Cloud infrastructure is vulnerable to external and internal attacks as well.

Energy CI is heavily related to ICT to improve the efficiency and the reliability of the procedures involved in the production, distribution and billing of energy. This however has increased the attack surface that could be exploited by various threats. Some of them are the following:

Threat types	
Tools and techniques used	Although administrators are using firewalls to protect their systems, there are cases where their misconfiguration may enable malicious users perform more targeted attacks. There are cases where firewall misconfigurations may reveal sensitive information.
Basic Attack Chain	e.g. emails requesting for a victim's actions and activities that will reveal or create vulnerabilities.
Botnets	Engineer Workstations are likely to be infected by botnets. Common botnet malware found include TDSS, Carufax, ZeroAccess, Sality, and Banloa.
Network Discovery	Networks should be protected enough to deny malicious incoming traffic (e.g. port scanning)
Insider Threat	Insider Threats are indeed a fact due to intentionally or unintentionally misuse of the facilities.
Cross-site Scripting (XSS)	XSS is a method to infect a computer by installing malware on its applications server. Common XSS attacks usually capture credentials or install malware.
Drive-by download	In this case infected websites "offer" malicious software to everyone who visits them.
Watering Holes	This kind of threats usually combine and make use of other attack techniques like 0-day vulnerabilities, XSS, or drive-by download towards a particular target service.

Threat types	
Zero-day Vulnerabilities	Identifying such vulnerabilities could help a malicious user to gain access to critical systems.
Wrappers / Packers / Crypter	These are mechanisms to encapsulate the malicious code so that signature based applications and IDS fail to detect the malware
Polymorphic / Metamorphic Hash	This technique is hard to be detected by Intrusions Detection/Prevention Systems that are mostly based on signatures.
Ransomware	Ransomware attacks is getting more and more popular lately. In 2015, the Department of Homeland Security reported 295 incidents of infected Industrial Control Systems[1]

The ICS-CERT report that mentioned 295 incidents in ICS systems during 2015 has also reported that such attacks were increased by 20% since 2014. Energy companies seem to be of high value for attackers. Some reasons for that are the following:

- oil and gas exploration information
- the CIs they support
- customer information and financial processing systems
- kind of businesses that usually attract 'hacktivists'.

Among the variety of cyber-attacks that affected the Energy CI domain, include the Nightdragon, Stuxnet and Shamoon. In particular, oil and natural gas companies have been hit by a persistent targeted spear-phishing campaign which lasted for many months.

Of specific interest to attackers are the Industrial Control Systems[2] (such as process control, automation or SCADA systems) that operate mission and safety Critical Infrastructures such as oil and gas drilling; production refining; electricity generation, transmission and distribution.

The security risks will increase as the sector deploys new and more powerful technology through initiatives such as smart grids as mentioned in the tables above.

The “Sector Risk Snapshot”[3] document has also summarized similar elements that should be protected against Cyber-attacks:

- Electricity infrastructure that is highly automated and controlled by complex and sophisticated energy management systems.
- Control system networks that are connected to the enterprise network and, also, connected to the Internet.
- Insider threats, initiated by (current, former) employees intentionally or unintentionally.

[1] https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf

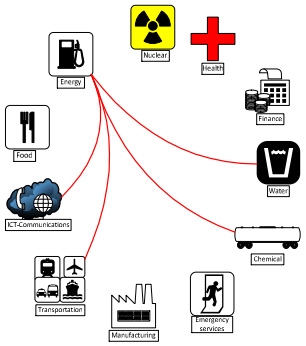
[2] http://www.paconsulting.com/industries/energy-and-utilities/cyber-security/securing-industrial-control-systems/

[3] https://www.hsdl.org/?view&did=754033

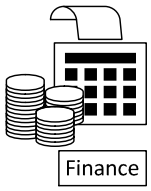
6.3.3 Sector dependencies

The following critical dependencies have been identified for this sector:

- **Chemical Industry**: chemical products (e.g., explosives) are provided for extracting coal or perforating gas and oil wells.
- **ICT – Communications**: remote control of operations, leak and breakage detection
- **Transportation**: delivery of workers and movement of raw materials, feed stocks, and products
- **Water**: cooling and production water



6.4 Financial services



6.4.1 Overview and what is included

The Financial Services Sector is a major and important component of each country's structure. Finance services are based on infrastructure that has also been identified as critical by both US and EU reports.

Financial institutions provide a broad spectrum of products and services to large and small organizations and credit unions. As reported in the respective US report ("Sector Risks Snapshot"[1]) and the US Department of the Treasury, these products are classified into four categories: (1) deposit, consumer credit, and payment systems products; (2) credit and liquidity products; (3) investment products; and (4) risk transfer products.

Traditionally, Financial Services Sector includes banks (acting either as depository institutions or as providers of investment products), insurance companies, financial regulators, trade associations, and other credit and financing organizations. US Department of Homeland Security also includes the providers of the critical financial utilities and services that support these functions, which has a special interest in terms of our research.

Meanwhile, the term Financial Service encompasses redistributing funds other than insurance, pension funding or compulsory social security for ENISA, that facilitates interaction between Finance companies and National Central Banks, European platforms and private networks operated by specialized managed providers. The resulting taxonomy categorizes:

- Stakeholders, according to four main categories: Banks, Service Providers, Professional Associations, and Authorities (National Supervisory Authorities and European Supervisory Authorities).
- Activities: Monetary Intermediation; Holding companies; Trust, funds and similar financial entities, and other financial service activities, except for insurance and pension funding.

Cyber threats

Financial Services are connected to private and public networks and are a potential target to terrorists, transnational criminals and other cyber-criminals who are aware and capable of using computer viruses, Trojan horses, worms, malware, sniffers, and other tools that can destroy, intercept and deny access to data and services. Specific cyber threats pertaining to the Financial services domain have been described in D.1.1, such as account takeovers, advanced persistent threat, ATM cash out, cloud-based attacks, corporate account take over (CATO), cryptolocker, cyberterrorism and state-sponsored attacks.

Insider Threats

Financial services may also suffer from insider threats. These threats may originate from former or current employees and organized crime members. Insider threats may have a significant impact to the brand name reputation of the financial institutions and pose significant concern since such employees usually have good knowledge of the systems in place and have direct access to the infrastructure and the services. Furthermore, any stakeholder (employee, contractor, supplier, or partner) might jeopardize company security, acting both intentionally or unintentionally, under the pervasive trends of BYOD and use of personal USB storage devices.

In the EU case ENISA has compiled two documents that also address the Cybersecurity aspect of the Financial Services Sector. Those documents are the "Secure Use of Cloud Computing in the Finance Sector[2]" and "Network and Information Security in the Finance Sector[3]". The first report analyses how cloud services can be used by the financial sector and the latter report describes the need for prevention and protection measures in the Financial Sector.

[1] https://www.hsdl.org/?view&did=754033

[2] https://www.enisa.europa.eu/publications/cloud-in-finance/at_download/fullReport

[3] https://www.enisa.europa.eu/publications/network-and-information-security-in-the-finance-sector/at_download/fullReport

6.4.2 Critical elements to protect

Depository institutions, by means of their technology service providers, are the main entrance to the sector for many individual customers when conducting transactions across the payments infrastructure, including electronic large value transfer systems, settlement platforms (e.g. TARGET2, STEP2, automated clearing houses (ACH), and automated teller machines (ATM).

Four main categories of networks are used in the finance sector:

- public, which are used mostly for customer interaction;
- shared leased / owned;
- business networks;
- leased / owned (private) lines that connect headquarters to local branches or to datacenters; provided lines related to a service or a platform.

Financial Services have been traditionally prone to attacks due to the employment of third parties to carry out activities in their business value chain, entailing operational risk due to technology failure, inadequate infrastructure or any setback in providing IT services by the service provider.

Another major aspect that might bring up risk for financial information to be abused is mobile banking, which involves accountholders accessing their accounts to check balances and to transfer money from their accounts using a mobile device. Lost / stolen devices, malware / viruses, and malicious applications are true threats to address for the end-user whereas Financial Services institutions cooperate with technical and operational methods of protecting Primary Account Information data, including expertise in the Payment Card Industry Data Security Standard (PCI DSS), and how security tokenization fits in terms of end-to-end architecture of exchanged payments.

Financial Services critical context is not only made up of infrastructure but of processes, too. Identifying actors (key infrastructure, processes, and institutions) in charge of performing critical operations for the sector is essential to ensure quick and appropriate responses and countermeasures to face disruptions. This is the rationale behind ENISA reported need for including the entire supply chain as part of principle security measures.

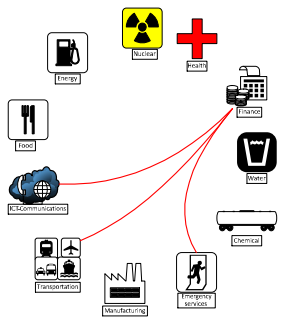
ENISA also pinpoints the lack of skilled and competence staff in the field of IT security in the Financial Services sector, which leads many finance operators to contract external experts to secure their infrastructures and communications in a critical development of their functions under non-disclosure agreements.

According with ENISA's report "Secure Use of Cloud Computing in the Finance Sector"[1], the European Financial Services industry is still in its early stages of cloud adoption. Furthermore, the services most often required by FIs from public Cloud Service Providers are email management and test environment that are not connected to core activities in their value chain. ENISAS's study shows a continued concern over security issues related to cloud, notably loss of control of the data, user account control, provider lock-in, isolation failures, compliance and legal issues, data confidentiality, integrity, availability, secure deletion, malicious insider, lack of auditing features, lack of transparency, data loss, data breach, user activity monitoring/logging and lack of forensics capabilities.

6.4.3 Sector dependencies

The following critical dependencies have been identified for this sector:

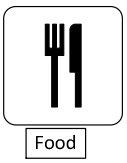
- **ICT** – **Communications**: rely on ICS services and communication networks in order to meet market demand for more efficient and innovative services and products.



[1] https://www.enisa.europa.eu/publications/cloud-in-finance

- **Energy**: is needed for the ICT infrastructure and other facilities for smooth operation
- **Transportation**: provide postal and shipping for essential paper transactions

6.5 Food industry



6.5.1 Overview and what is included

In the Food and beverages businesses as wells as in the food production and agriculture systems, developments in technology are vital for their successful operation while at the same time the risk of cyber threats and fraud increased over the last years.

The "2015 Global Security Report"[1] by Trustwave, indicated that 13% of all reported data breaches occurred in the Food and beverage industry. As in most of the sectors described in our taxonomy, standardization of computer systems is vital for the food sector as well. If a particular system suffers from a known security vulnerability, it can be easily spread through the whole enterprise network of food industries creating multiple cyber-attacks. For instance, the interconnectivity among franchises could lead a security flaw to create a chain of cyber-attacks across all branches thus multiplying the impact of the attack. A high percentage of hacked businesses in this area go out of business within a year due to such attacks resulting in great financial loss.

Apart from the financial loss, an intentional contamination of the Food Supply would cause harm or ever loss of human life. About two million people a year, most of them children, die from food-borne or water-borne illness and more than one-third, or about 1.3 billion tons, of the food produced for human consumption every year is wasted or lost because of spoilage. In the Food sector the use of ICS systems, such as SCADA, increase the risk of cyber-attacks. For example, if hackers gain access to the network of a food supplier, they could introduce dangerous amounts of chemicals to the food being treated. Even the ability to remotely shut down cooling systems which are vital for maintaining the food ingredients can be disastrous for the Food CI domain.

6.5.2 Critical elements identified

According to the "2015 Food and Agriculture Sector-Specific Plan"[2], the most commonly ICSs in the Food CI domain include SCADA systems, Distributed Control Systems (DCS), and Programmable Logic Controllers (PLC). These control systems help to regulate and manage the various distributed assets in the production process. In the past years, the ICSs were mostly isolated, running on special purpose hardware and developed with special software. Currently the trend is to use commodity hardware and replace those traditional ICSs with readily available and more cost effective solutions.

These new systems encourage corporate connectivity and include remote access capabilities, which are in line with best practices for industry efficiency, innovation and growth. However, the interconnection of all those ICSs presents an opportunity for malicious activities with harmful consequences. Some possible threats for the sector may include:

- Blocked or delayed flow of information through ICS networks (e.g. in case of DDoS attack)
- Unauthorized changes may be performed to instructions, commands, or alarm thresholds that could potentially damage, disable, or shutdown equipment
- Inaccurate information may be transmitted to system operators thus leading to false alarms and inappropriate corrective activities
- Modification of ICS software or settings, or infection of ICS software with malware

Security gaps in the area

ANX Corp.[3] identified eight major security gaps that affect food and beverage companies: outdated firewalls, insecure remote access, weak security configurations, operating system flaws, lack of staff training, flawed security policies, negligence, and poor change control procedures.

[1] https://www2.trustwave.com/rs/815-RFM-693/images/2015_TrustwaveGlobalSecurityReport.pdf

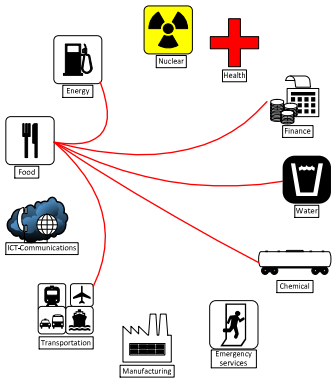
[2] https://www.dhs.gov/publication/nipp-ssp-food-ag-2015

[3] http://www.foodqualityandsafety.com/article/cybersecurity-in-food-and-beverage-industry/?singlepage=1&theme=print-friendly

After analyzing the usage and weakness trends of more than 2 million business passwords, Trustwave found that the most common password used by global businesses is "Password1" as it satisfies the default Microsoft Active Directory complexity setting.

6.5.3 Sector dependencies

According to the “2015 Food and Agriculture Sector-Specific Plan” created by the U.S. Department of Homeland Security the Food and Agriculture Sector has critical dependencies with many sectors, but particularly with the following:



- **Chemical Industry**: components used in modern food productions such as chemical fertilizers, pesticides, herbicides, and fungicides are provided by the chemical sector.
- **Energy**: to power the equipment needed for agriculture production and food processing
- **Financial Services**: provides the financial backbone for food
- **Transportation**: delivering inputs to the farm, including items such as seeds, seed stock, fertilizer, and feed required for agricultural production.
- **Water**: necessary for processing facilities, livestock production, and crop irrigation at the farm level

6.6 Health

6.6.1 Overview and what is included

Protecting the health care sector is very essential for international economy and human life. Protection includes actions to shield all health care assets, digital systems and personal data from exposure.

According to a survey from Sophos[1], health care sector had one of the lowest rates of data encryption, with only 31% of healthcare organizations reporting extensive use of encryption, while 20% said they do not use encryption at all. In the "2016 Cyber Security Intelligence Index"[2] from IBM Security Services, it is stated that the rate of attacks against the healthcare sector climbed to the highest level of all industries studied in 2015, after not making the top five in 2014, as healthcare leaped ahead of the Manufacturing, Financial services, Government and Transportation sectors. Five out of the eight largest healthcare security breaches since the beginning of 2010—those with more than one million records reportedly compromised—took place during the first six months of 2015. In fact, over 100 million healthcare records were reportedly compromised in 2015[3].

According IBM's "2015 Cost of a Data Breach" study, in 2014 the average cost of a data breach across all industries was $3.8 million, while the cost of each record in the health sector was $363 per record breached, more than twice the overall average of $154 per record.

Health records contain social security numbers, medicare numbers, credit card numbers, email and physical addresses and generally a lot of personal data of the patient. Attackers seek access to this information that can be used for medical identity theft and fraud.

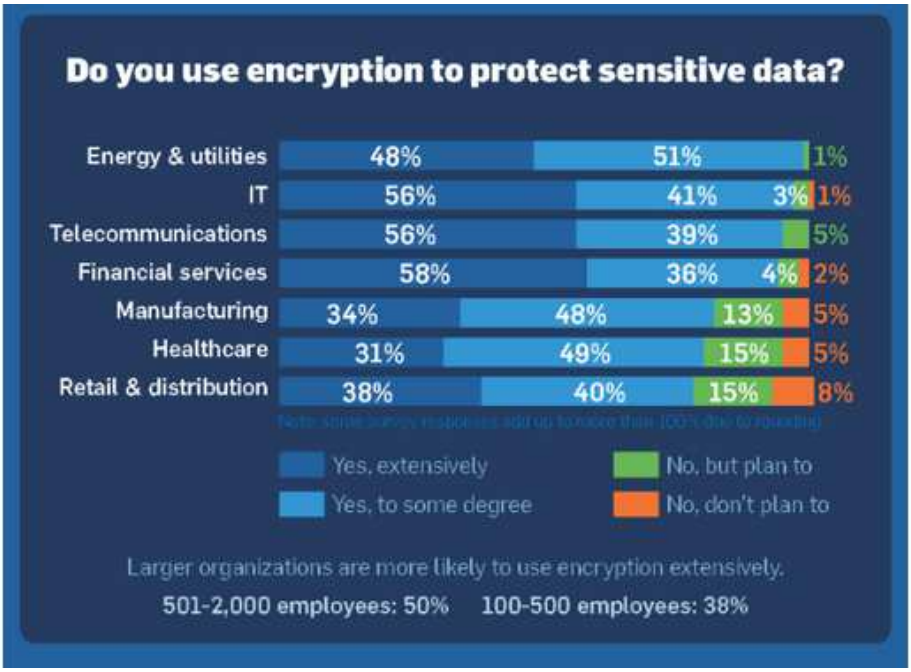


Figure 6 Sophos results on encryption usage by various CI domains

[1] https://blogs.sophos.com/2016/01/28/this-infographic-shows-the-state-of-encryption-today/

[2] http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03133USEN&attachment=SEW03133USEN.PDF

[3] https://nakedsecurity.sophos.com/2016/04/26/why-cybercriminals-attack-healthcare-more-than-any-other-industry/

6.6.2 Critical elements identified

Hospitals and clinics in the world are becoming more advanced in terms of technology. Health sector utilizes a variety of digital systems for example to satisfy staff and patient demands for real-time access to medical records (test results, upcoming examinations, etc.), monitor patient condition and drug usage, guarantee security to hospital infrastructures, ensure privacy in the personal data of patients, instantly react to emergencies.

HCB, the Hospital Clinic de Barcelona, which is also a CIPSEC member and one of the most recognized and representative largest public tertiary university hospitals in Spain and in the EU, has identified numerous of critical elements that should be protected and reported them in D1.2 ("Report on functionality building blocks"): Some of them include:

- Monitoring and therapeutic equipment connectable to dedicated VLAN Ethernet network on through Central Patient Monitoring Stations that receive the patient data and send the clinical parameters using HL7 standardized protocols
- Imaging equipment connected to dedicated VLAN Ethernet network interchanging mainly images to/from PACS storage reservoir
- Surveillance cameras which ensure security to the infrastructures of the hospital.
- Access control systems such as biometric controls which verify identity for secure access to electronic systems and ensure authorized access to the hospital premises.
- Temperature and gas concentration active RFID sensors
- Cold production equipment, boilers and air conditioners
- Nurse call system which is based on smartphones
- Databases storing medical records of patients and videos from surveillance cameras.
- Any data transmission network (Wifi, RF antennas, IP TV, VOIP)

Cybersecurity Risk Assessment

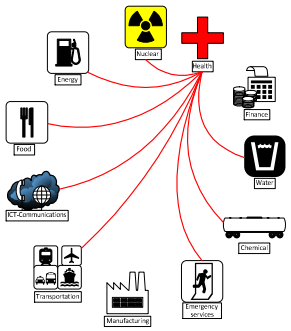
In the following table we can see common cyber threats, vulnerabilities, consequences, and mitigation strategies identified for the Health sector. For each one of these categories there is a column which includes a further detailed breakdown list for each one them.

Category	Breakdown list
Threats	■ Insider threat ■ External threats (e.g. hacking, and terrorism) ■ Network threats (e.g. Botnets, malware, phishing, and DDoS)
Vulnerabilities	■ Inadequate patch, configuration and password management. ■ Lack of antivirus IDS/IPS protection ■ Software vulnerabilities and SQL injections
Consequences	■ Loss of personally identifiable information and identity theft ■ Patient treatment errors ■ Inability to use patient data

Category	Breakdown list
Cascading Consequences	■ Forensic and system recovery service fees ■ Blackmail and fraud (medical and financial) ■ Loss of brand reputation ■ Loss of services ■ Loss of life
Mitigation Strategies	■ Redundant and failover systems and usage of backup sites ■ Background investigations ■ Identity management ■ Multifactor authentication ■ Usage of IDS/IPS systems to protect against DDoS ■ Authorization management (privileges) ■ Data encryption ■ Usage of appropriate anti-virus software ■ Auditing and logging mechanisms ■ Hardware lockdown (disable)

6.6.3 Sector dependencies

According to the "Healthcare and Public Health Sector-Specific Plan"[1], the following sectors provide services to the health sector to be operational.



- **Chemical Industry**: many items used in this sector, including pharmaceuticals, medical devices, medical supplies, and key industrial gases include operations from the chemical sector.
- **ICT – Communications**: use of business and clinical information systems. Also, communications infrastructure is required to maintain situational awareness and coordinate healthcare activities during steady state and emergency response.
- **Energy**: electric, natural gas, propane, and diesel fuel are required to power and run facility functions and vehicles
- **Food**: food production and distribution for healthcare and public health personnel and patients
- **Transportation**: movement of supplies, raw materials, pharmaceuticals, personnel, emergency response units, patients, and fatalities
- **Water**: potable water and wastewater for infection control, sanitation, renal dialysis, laboratory needs, sterilization, maintenance of blood and organ banks, drinking water for staff, etc.
- **Emergency Services**: coordination with first-responders and emergency medical services
- **Nuclear**: radioactive materials support medical applications to monitor, image, or treat metabolic processes or tissues in humans.

[1] https://www.dhs.gov/sites/default/files/publications/nipp-ssp-healthcare-public-health-2015-508.pdf

6.7 Transportation

6.7.1 Overview and what is included

In transportation, new technology is creating incredible opportunities to improve the safety and efficiency of airplanes, airports, trains, railways, vehicles, highways and maritime sector. However, new technologies and growing connectivity also represent new challenges in the area of security and Cybersecurity. Transportation systems have become increasingly digital dependent, with a wide range of data flowing across systems, tracking and monitoring both digital and physical networks. As more devices and control systems are connected online, more vulnerabilities and cyber threats will appear, increasing the potential for disruption to physical assets[1].

Air transportation

In the aviation industry, technical advances in navigation systems and airframe design have reduced the chances of an accident; however, the increasing reliance on computers poses a different kind of threat. As aircrafts move ever closer to becoming fully e-enabled and automation increases, pilot practices and training will need to adapt in the event of system failure or security breach[1].

Rail transportation

The rail industry also relies heavily on IT and automation. Systems which control the train movement, deliver power to the network, control signaling infrastructure, report on the condition of the rolling stock and associated infrastructure and support operational planning and timetabling, may be subject to cyber-attacks[1].

Road transportation

In this sector, important systems are electronic warning signs at road construction sites and traffic lights. Hacking the timing system of traffic lights might mean a lot of injuries and possibly loss of human life. Currently there is a trend from many automotive industries towards driverless cars which will increase the potential attack surface of the domain[2].

Maritime sector

Like the other subsectors, the maritime sector also supports the economy through the transportation of goods (such as energy, oil, gas, food, etc.) and the movement of people. Maritime sector is also based on new ICT technologies and should also address the Cybersecurity aspects like the other Transportation subsectors.

6.7.2 Critical elements identified

In all sectors of transportation, digital technologies play a major role in the improvement of customer service while they are subject to cyber-attacks. Systems for navigation, tracking, positioning signaling, communication and data and business management are interconnected through networks and remote access terminals which may allow cyber-attacks to take place.

In deliverable D1.2 (“Report on functionality building blocks”), CIPSEC consortium and the relative pilot (DB), identifies interlocking systems as the most important asset of the rail transportation sector, to be protected. Interlocking systems are responsible for signaling safe routes to the train conductor. An ESTW/ESTW-ZE is the core of the interlocking system. It contains all information about the required elements and maintains the current state of the field elements in the supervised area. Commands by surrounding systems are sent to the

[1] http://www.oliverwyman.com/content/dam/marsh/Documents/PDF/UK-en/Cyber%20Risk%20in%20the%20Transportation%20Industry-03-2015.pdf

[2] http://www.driverless-future.com/?page_id=384

ESTW-ZE that checks if the command can be performed safely or not. The ESTW-ZE is responsible for safe routes.

In the railway sector it is important to distinguish safety and security. A system is safe if it is free from unacceptable risks that cover faults and failures. Every safety-critical railway system must be admitted by a national security authority. During this admission, the requirements of the European Standards 50126, 50128, and 50129 are checked. Security is the system's ability to defend and detect intentional attacks against itself. It is necessary to maintain the safety of the railway system.

While the movement of trains needs to be performed safely, the overall system is also required to be available, in order to maintain an adequate level of operation. On the other hand, availability also supports safety as the unavailability of a critical system (e.g. light signals) can be a threat to safety.

The railway domain increasingly makes use of open communication networks. This also includes the train control level which is critical for safe train operation. Additionally, more and more commercial off-the-shelf (COTS) products are used in this area. They are more cost-efficient and support the faster realization of projects.

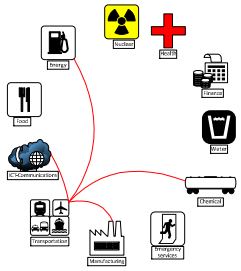
Contrary to the existing networks, which rely on closed or proprietary networking infrastructure or even electric circuits to transport information, open networks and COTS products must be protected against attackers who want to harm the infrastructure intentionally. Security is an ongoing process, in which the attack vectors and countermeasures need to be reevaluated on a regular basis, as new vulnerabilities are discovered over time.

The maritime subsector and the related Cyber security aspects have been identified in the respective ENISA report[1] named "Analysis of Cyber Security Aspects in the Maritime Sector". The report identifies that ICT technology is used among others to support maritime operation like port management and ship communications. The sector makes use of SCADA devices which in some cases are connected to the Internet so prone and vulnerable to Cyber-attacks. Attacks on these systems may affect the devices and the commonly shared infrastructure layers (e.g. databases, systems hosting sensitive information, etc.). Moreover, the report presents the lack of good practice, usage and other standards that would help the adoption of security procedures and measures needed.

A EC report named "Final Report on Study on Critical Dependencies of Energy, Finance and Transport Infrastructures on ICT Infrastructure"[2], that was produced on behalf of the DG Justice, Freedom and Security department, identifies as critical the following:

- high dependency on SCADA systems, LAN systems, (needed for Air, Rail and Road transportation)
- secure messaging services for data transfer between control systems, radio connections, satellite connections and mobile telecommunications (needed by Air transportation)
- radio communication to trains (needed by Rail transportation)

6.7.3 Sector dependencies



According to the "2015 Transportation Systems Sector-Specific Plan"[3], the following sectors provide services to the transportation sector to be operational.

- **Chemical Industry**: petrochemicals and other chemical products are needed in order to maintain operations
- **ICT – Communications**: reliable and secure transmission of information necessary for the efficient operation of the transportation network
- **Energy**: supply the fuel for all types of transportation
- **Manufacturing**: manufacturing of vehicles, commercial ships, aerospace products, trains, and buses.

[1] https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1

[2] http://ec.europa.eu/dgs/home-affairs/e-library/docs/pdf/2009_dependencies_en.pdf

[3] https://www.dhs.gov/sites/default/files/publications/nipp-ssp-transportation-systems-2015-508.pdf

6.8 Water systems and facilities

6.8.1 Overview and what is included

Safe drinking water is a prerequisite for protecting public health and all human activity. Properly treated wastewater is vital for preventing disease and protecting the environment. Critical infrastructures, such as Energy, Transportation and Food, depend on the Water infrastructure for sustaining the flow of crucial goods and services. Thus, ensuring security in this Critical Infrastructure is very essential to modern life.

According to the US Department of Homeland Security[1] there are approximately 153,000 public drinking water systems and more than 16,000 publicly owned wastewater treatment systems. More than 80 percent of the U.S. population receives their potable water from these drinking water systems, and about 75 percent of the U.S. population has its sanitary sewerage treated by these wastewater systems. European Union from the other side has an already established (30 years) drinking water policy. “This policy ensures that water intended for human consumption can be consumed safely on a life-long basis, and this represents a high level of health protection”. The policy among other aims to:

- Ensure that drinking water quality is controlled through standards,
- Secure an efficient and effective monitoring, assessment and enforcement of drinking water quality,

In Europe, many countries have included security plans about their water systems in their national security plans and have conducted vulnerability assets. The European Reference Network for Critical Infrastructure Protection (ERNCIP)[2] describes activities for securing water systems in Czech Republic, Estonia, France, Germany, Spain, Sweden and the United Kingdom.

6.8.2 Critical elements identified

Industrial control systems like SCADA, PLCs, and DCS are widely used in water and wastewater facilities in order to maximize resources and monitor operations. ICSs also perform data logging, alarming, and diagnostic functions so that large, complicated process systems can be operated in a safe manner centrally maintained by the staff in charge.

In Figure 7 we present the major components of a typical ICS in a water treatment and distribution facility. The major control components used in the water sector are the following:

- Central Control Station: This is the master unit of the ICS working in parallel with local processors located at remote field sites. Input/output (I/O) servers are used to collect, buffer, and provide access to process information from the local processors. Central control stations utilize one or more host computers to provide the graphical displays as well as the necessary computational and networking horsepower.
- Human Machine Interface: like in the case of Energy sector it allows personnel to monitor the state of a process under control, modify control settings, and manually override automatic control operations in an emergency. HMI also displays process status information, historical information, reports, and other information to operators, administrators, managers, business partners, and other authorized users.
- Local Processors: PLCs, Remote Terminal Units (RTUs), and Intelligent Electronic Devices (IEDs), allow for automatic control of process instruments and operating equipment. These devices acquire data, communicate to other devices, and perform local monitoring, processing, and control.
- Instruments and Operating Equipment: they provide online and offline measurements of chlorine, dissolved oxygen, color/turbidity, conductivity, pH, pressure, fluid level, flow rate, and other critical elements. In some water systems, sensors communicate with local processors to control valve, pump, and mixer operations

[1] https://www.dhs.gov/water-and-wastewater-systems-sector

[2] https://erncip-project.jrc.ec.europa.eu/component/jdownloads/send/9-chemical-biological-risks-in-the-water-sector/146-overview-of-standards-guidelines-and-current-practices-for-vulnerability-assessment-of-drinking-water-security-in-the-european-union

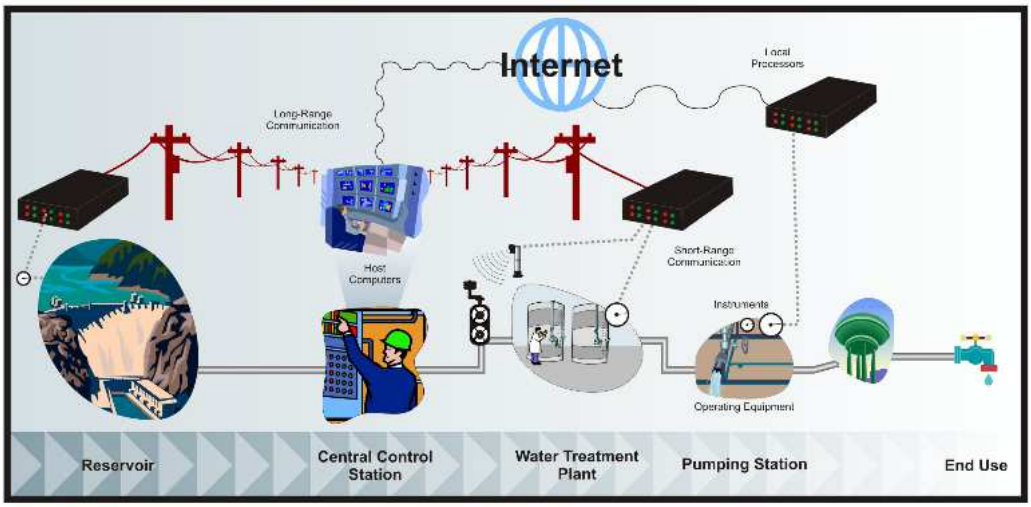


Figure 7- Components of a typical Industrial Control System in the Water Sector

Cyber security in water systems

In the 2008 “Roadmap to Secure Control Systems in the Water Sector”, developed by the Water Sector Coordinating Council (WSSC), the Cyber Security Working Group (CSWG) with the support of American Water Works Association (AWWA) and the Department of Homeland Security (DHS), a layered security architecture suggested, called the "Defense-in-Depth"[1]. This strategy takes into account that a properly configured combination of security technologies, controls, and policies and not a single security product is required to strengthen security in the water infrastructures.

System access security

Access control and physical security can help strengthen weak links in the security chain of the system. Tools like CSET (Cyber Security Evaluation Tool), (created by the Department of Homeland Security's (DHS) National Cyber Security Division's Control Systems Security Program (CSSP)), guides users through a step-by-step process to assess their control system and IT network security practices against recognized industry standards[2].. Such tools are capable of generating a list of recommendations for improving the organization's industrial control cyber systems. The recommendations come from a database of cyber security standards, guidelines, and practices and each one is linked to a set of actions that can be applied to enhance and strengthen cyber security controls.

Segmenting the network

Fully interconnected IP networks which connect the Industrial Control Systems to the Internet, could increase the danger of a cyber-attack from an external attacker. Networks connecting business equipment, should be segmented to simplify complex networks hard to maintain and secure. External traffic should not be mixed with the traffic used to communicate for example the SCADA HMI (Human Machine Interface) with a PLC. In any case, all external connections should be also monitored and analyzed for cyber threats.

[1] http://www.n-dimension.com/wp-content/uploads/NDSI-WATER-CybersecurityRoadmap08-1.pdf

[2] National Institute of Standards and Technology (NIST), North American Electric Reliability Corporation (NERC), International Organization for Standardization (ISO), U.S. Department of Defense (DoD), and others

Strong Authentication and role-based access control

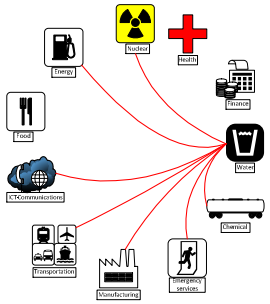
Within the organization, employees have to be assigned specific roles bind to specific activities on the systems. In order to securely provide role-based access control, strong authentication schemes should be applied. The most elementary step to be taken is the creation of sufficiently complex and regularly changed passwords.

Hardened Components

Network components and Industrial Control Systems should be inspected for unused functions that are not disabled or configurable options that are not set to their most secure levels. By hardening such components means locking down functionality to prevent unauthorized access.

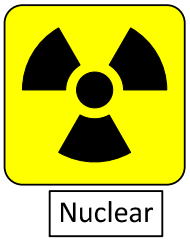
6.8.3 Sector dependencies

The following critical dependencies are identified for this sector:



- **Chemical Industry**: water purification and sanitation is provided by the chemical sector.
- **ICT – Communications**: monitoring operations and emergency communications with responders
- **Energy**: process power, pump, wells, treatment, operations
- **Transportation**: delivery of components and materials
- **Manufacturing**: operational and process equipment
- **Emergency Services**: emergency (medical and firefighting) responders
- **Nuclear**: power delivery

6.9 Nuclear



6.9.1 Overview and what is included

Any cyber infrastructure which provides monitoring or functional capabilities for the effective operation of the Nuclear sector, may be subject to cyber-attacks. Today's cyber systems in the Nuclear sector, use common standards for communication protocols and are highly network-based, compared to their ancestor systems which operated in isolated environments and typically relied on proprietary software, hardware, and communications technologies. Compromising these old systems, required physical access and specific knowledge of individual system architectures. Many cyber systems used in the Nuclear sector today, are connected in the Internet in order to increase the connectivity and the level of information interoperability required among modern infrastructure. Systems used to operate the nuclear power plant are often isolated from external networks and other systems. However, standard operating systems such as Windows or UNIX are increasingly used in other areas of plant operations. These may be connected to remote systems via private networks provided by telecommunications companies. Common telecommunications technologies such as the Internet, public -switched telephone networks, or cable or wireless networks may be used[1].

6.9.2 Critical elements identified

According to the "Roadmap to Enhance Cyber Systems Security in the Nuclear Sector"1, developed by the Nuclear Roadmap Steering Committee (RSC), Industrial Control Systems (ICS) in nuclear power plants affect every aspect of plant operation.

Their components and functions include the following:

- Sensors interfacing with the physical processes within a plant and continuously taking measurements of plant variables such temperature, pressure, and flow.
- Control, regulation, and safety systems that process measurement data to manage plant operations, optimize plant performance.
- Communication systems for data and information transfer through wires, fiber optics and wireless networks.
- Human-system interfaces to provide information and allow interaction with plant operating personnel.
- Surveillance and diagnostic systems that monitor sensor signals for abnormalities.
- Actuators (e.g., valves and motors) operated by the control and safety systems to adjust the plant's physical processes.
- Status indicators of actuators (e.g., whether valves are open or closed, and whether motors are on or off) providing signals for automatic and manual control.

In Figure 8 below it is illustrated how these systems fit together within the context of reactor system operations. The figure also presents the interconnection between all these systems and the need for security on each level and each one of them to ensure the safe operation of nuclear power plant.

[1] http://resources.nei.org/Documents/Roadmap.pdf

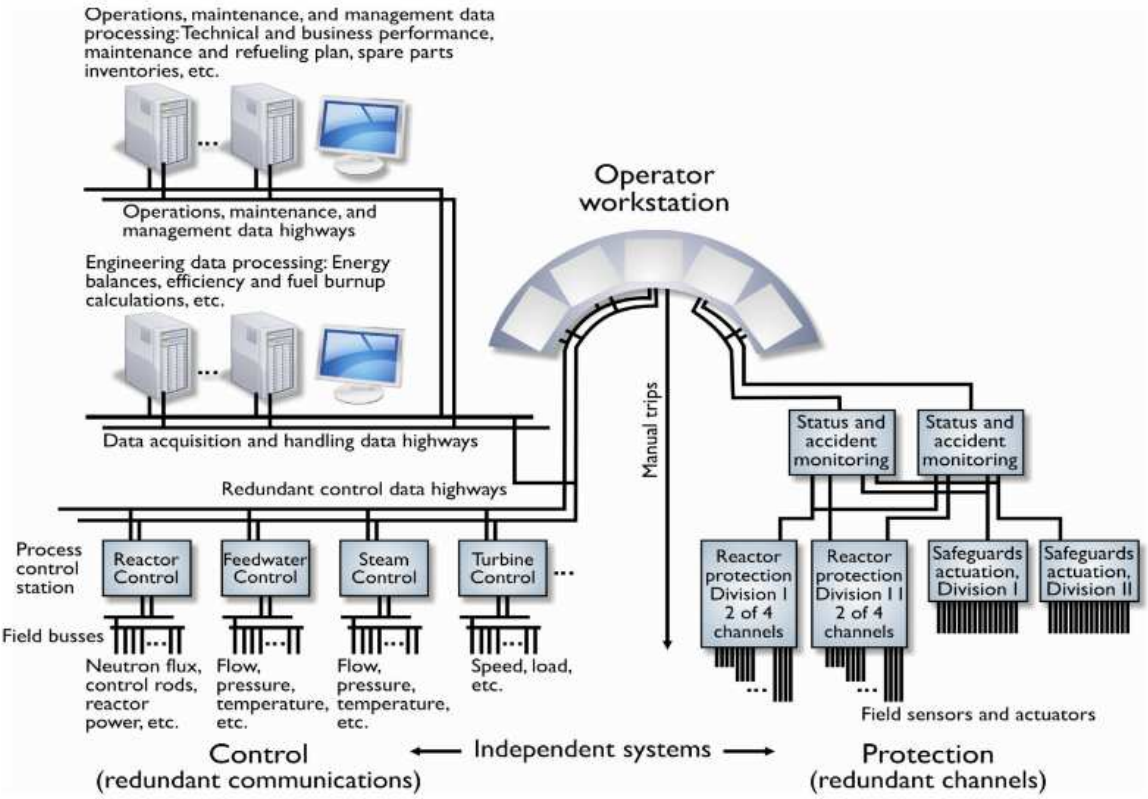
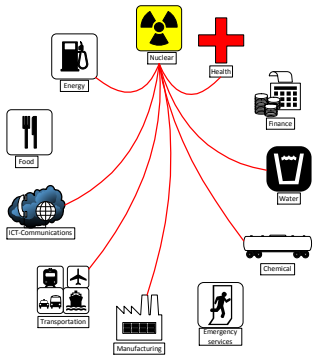


Figure 8 Components of Typical Industrial Control Systems in Commercial Nuclear Power plants

Cyber components mentioned in figure 8 should be adequately protected against cyber-attacks that aim to modify, destroy, or compromise the integrity or confidentiality of data or software. There should be appropriate mechanisms in place to deny access to systems, services and data, and as a consequence may have disastrous impact to the operation of systems, networks, and equipment.

6.9.3 Sector dependencies

The following critical dependencies are identified for this sector:



- **Chemical Industry**: chemicals are used in the production of electricity at nuclear power plants
- **ICT – Communications**: nuclear sector rely on uninterrupted Internet and communications network for both efficient operations and timely information sharing. ICS manage daily operation and used to store sensitive information.
- **Energy**: uninterrupted power supply is needed by nuclear facilities and power plants.
- **Health**: ensure workforce health
- **Transportation**: nuclear materials are shipped via trains, ships, trucks and airplanes.
- **Water**: large quantities of water need for cooling operations.
- **Manufacturing**: components including piping, valves and valve components, electrical cable, shielding materials.

6.10 Emergency services

6.10.1 Overview and what is included

Emergency services sector aims at protecting property and the environment, saving human lives, assisting communities impacted by disasters and aiding recovery during emergencies. Usually this sector is composed by five distinct disciplines which are:

- Law Enforcement,
- Fire and Emergency Services,
- Emergency Medical Services,
- Emergency Management and
- Public Works.

According to United Nations Office for Disaster Risk Reduction (UNISDR[1]), Emergency services include "The set of specialized agencies that have specific responsibilities and objectives in serving and protecting people and property in emergency situations". There are three distinct disciplines/functions under this definition, police, fire and rescue, and emergency medical services which seem to be somewhat aligned with the US case.

Emergency services are closely related to Emergency communications which according to ENISA report named "Emergency Communications Stocktaking"[2] are a set of systems and processes that allow the Emergency Services to manage response to incidents, to disasters and crisis. The report also identifies the critical elements that are crucial whenever an incident happens and will be mentioned in the section below.

6.10.2 Critical elements identified

According to the previous subsector segmentation provided in the 5 categories there is a list of elements to protect and of high importance for each one of them. So in a per subsector basis the following critical elements have been identified[3]:

- Law Enforcement:
  - Loss of communication lines can result in a degradation of the response of the emergency service.
  - Additionally, inaccurate information from public alerting and warning systems can result in wasting resources and creating public confusion and panic.
- Fire and Emergency Services:
  - Possible cyber-attack in the emergency communication lines can cause inability of the general public to access the service and inability for the department to effectively react.
- Emergency Medical Services:
  - Lack of availability of sector database causes disruption of mission capability which may result in inability to access subject matter affecting emergency response procedures.
  - Compromised sector database causes corruption of critical information which may result in slower overall response time and inability of internal staff to trust the integrity of the data they handle.

[1] http://www.preventionweb.net/english/professional/terminology/v.php?id=7821

[2] https://www.enisa.europa.eu/publications/emergency-communications-stocktaking

[3] https://www.dhs.gov/sites/default/files/publications/Emergency-Services-Sector-Cyber-Risk-Assessment-508.pdf

- Emergency Management:
  - Public alerting and warning systems malfunction,
  - loss of communications lines and
  - overloading in the communications network can cause false alarms, wasting of resources, loss of services and ineffectiveness of operations
- Public Works: compromised sector database, loss of communications lines and blocked monitoring systems could potentially cause panic and harm citizens.

Per subsector the following critical cyber infrastructure is used and should be protected against cyber threats and attacks:

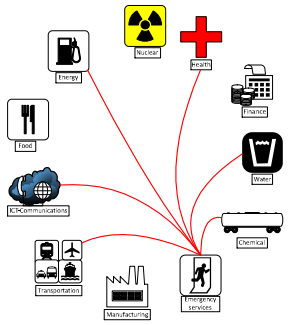
Tools & Elements used per subsector	Law Enforcement	Fire and Emergency Services	Emergency Medical Services	Emergency Management	Public Works
Security and Surveilance Systems	X				
Warning Systems	X			X	X
Computer Aided Dispatch	X	X	X		
Geospatial Tools and Systems	X	X		X	X
Criminal Justice Networks and Systems	X				
Internet	X	X	X	X	X
Telecommunication Systems	X	X	X	X	X
Radio Infrastructure	X	X	X	X	X
Fire and Medical Alarm Systems		X	X		
Personal Alert Safety Systems		X			
Modeling and Simulation Tools		X	X	X	

The previous table and the elements reported is a superset of those identified in the ENISA document which include:

- Broadcast: including radio and television signals for proper and the reception of crucial information to the public
- Telephony: including voice systems for proper communication channels between citizens and the emergency services
- Internet: including the electronic communications using email or voice over IP
- Data networking: usually private IP networks that are used for electronic exchange of information.
- Emergency radio: including private highly available radio facilities and infrastructure operated by the emergency services, mostly used for management purposes in case of crisis and various emergency incidents.

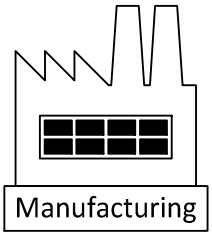
6.10.3 Sector dependencies

The following critical dependencies are identified for this sector:



- **Chemical Industry**: personnel of this sector can be used together with emergency services personnel in joint exercises to enhance response efforts
- **ICT – Communications**: public alerting and warning systems. Internal communication networks and emergency lines, computer-aided dispatch services
- **Energy**: rely on energy supplies to maintain critical operations during natural and manmade disasters and to fuel its service vehicle fleet
- **Health**: in responding to emergencies, first responders coordinate with the health sector
- **Transportation**: depends on resilient transportation networks to respond effectively to emergencies
- **Water**: water supply in order to provide emergency services, such as in firefighting and public works

6.11 Manufacturing



6.11.1 Overview and what is included

The manufacturing sector mainly includes automotive, pharmaceutical, chemical and electronics companies. According to IBM[1], 30% of the total attacks against the manufacturing sector in 2015 targeted automotive manufacturers. Chemical industries ranked second in the same survey. Attackers target at stealing potentially valuable intellectual property or sensitive information[2].

In the manufacturing sector there is a lack of adoption of key information security practices, resulting in vulnerabilities to older attacks, such as Shellshock, SQL injections and Heartbleed. The Heartbleed[3] bug is a serious vulnerability found in the OpenSSL cryptographic that allows attackers to eavesdrop on communications, steal data directly from the services and users, and to impersonate services and users.

In the "2015 Critical Manufacturing Sector-Specific Plan"[4], it is referred that manufacturing processes are typically operated by Industrial Control Systems that increasingly use open platforms and common operating systems, rather than proprietary system designs. Cyber intruders may aim to seize control of the systems to disrupt processes, corrupt information sent to facility operators, damage equipment, or steal proprietary information. Intellectual property theft through cyber-attacks can threaten competitiveness, affect business reputation, and subject customers to risk from counterfeit products. Intellectual property shared with business partners outside the company also becomes subject to the security risk of partners' systems.

6.11.2 Critical elements identified

The variety of communication protocols in ICS networks which are used in the manufacturing sector often lack of basic security controls such as authentication and encryption. Modbus and DNP3[5], standard data plane protocols, used by HMI/SCADA/DCS applications to communicate physical measurements and process parameters such as real time temperature, pressure and valve status[6]. Control plane protocols — which are used to configure automation controllers, update their logic, make code changes, download firmware — are proprietary and vendor-specific. Each vendor uses its own implementation of the IEC-61131[7] Standard for Programmable Controllers. These implementations are rarely documented, making it very difficult to monitor critical activities.

Since the goal of most ICS cyber-attacks is to cause operational disruptions or physical damage, an attacker will try to change the way the process executes. While a predefined set of process parameters can be changed through HMI/SCADA applications, the logic maintained on the controller defines the process flow and its safety settings. Therefore, changing the controller logic is both the easiest and most successful way to cause such disruptions. Once inside the network, an attacker can easily download control logic to an industrial controller or change its configuration. Since these actions are executed using proprietary vendor-specific protocols, there is no standard way to monitor these control plane activities. As a result, changes made by an attacker can go unnoticed until damage starts to occur.

The connectivity between the Internet and the manufacturing network exposes the latter to cyber-attacks. Attackers can easily gain access to the internal network in order to initiate their attacks.

---

[1] http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03133USEN&attachment=SEW03133USEN.PDF

[2] http://www.darkreading.com/vulnerabilities---threats/manufacturers-suffer-increase-in-cyberattacks/d/d-id/1325209

[3] http://heartbleed.com/

[4] https://www.dhs.gov/sites/default/files/publications/nipp-ssp-critical-manufacturing-2015-508.pdf

[5] https://scadahacker.com/library/Documents/ICS_Protocols/Triangle%20Microworks%20-%20Modbus-DNP3%20Comparison.pdf

[6] http://www.industryweek.com/information-technology/cyberthreats-targeting-factory-floor

[7] http://www.plcopen.org/pages/tc1_standards/

Cyber-attacks (targeting manufacturing)

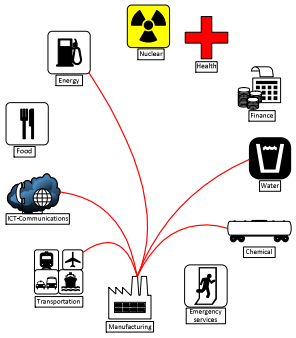
Apart from attacks targeting the ICS systems of the industry, personal computers and devices used by employees inside the network could be used by attackers to compromise the system. According to this article[1] and Chris Weber, co-founder of Casaba Security[2], a cyber-security consultant firm for the industrial, financial, technology and government sectors, there are four major types of cyber-attacks targeting manufacturers and depending on the use of personal devices:

- Drive by Downloads: Malware is installed on an employee's computer as soon as they visit a compromised website
- Cross-Site scripting: XSS attacks take advantage of legitimate websites to conceal the attack. By using this attack, hackers can gain access to key online accounts, network control and access, machinery system access, client and vendor portals and bank accounts.
- Watering hole attack: Attackers find a website regularly visited by employees of that company or industry and inject malicious code into it. Once employees of the targeted company visit the website, they are infected either through a drive-by download attack or 'malvertising,' which is when malware is delivered through a third-party advertising network on a website.
- Wrappers: are used by attackers to bypass antivirus and Intrusion Detection Systems. The malware code is changed in a way that a signature based detection will fail and the tool would identify the virus file as a legitimate one - like a PDF, Word document, a computer game or utility tool.

6.11.3 Sector dependencies

The following critical dependencies are identified for this sector:

- **Chemical Industry**: requirements of chemicals for the production of goods (e.g., chemicals used in the production of metals from ore deposits, and various plastics used in vehicle manufacturing).
- **ICT – Communications**: owners and operators rely on this sector for telecommunications access for operations and logistics.
- **Energy**: require large amounts of uninterrupted power for operations.
- **Transportation**: movement of raw materials, feed stocks, and products
- **Water**: is some cases continuous water sources are essential for manufacturing processes.



[1] http://www.automationworld.com/4-types-cyber-attacks-targeting-manufacturers

[2] https://www.casaba.com/

6.12 Other CI domains

In this section we refer to CI domains that are reported by some countries and their respective NCSS documents but there was no Cybersecurity related information found according to the needs of the deliverable. We think that the needs of those CIs are fully covered by the needs of the CIs analyzed in the relevant section with the eleven different CI domains. Below are some of those CIs domains and we list them for completeness purposes.

Those CIs include: **Dams** sector (which may be thought as subcategory of Water sector), **Commercial Facilities** (which is only reported as CI by the US), **Government Services and Facilities** (which is also reported by US and mainly refers to large infrastructures and buildings), **Public/Civil administration** (which are covered to some extent by the Emergency services and already analyzed). Another CI domain that was mentioned by some countries is **Space** (France and Spain) and **Defense/Armed forces** but there were no reports found including information addressing the Cybersecurity aspects. This does not mean that the findings of the report does not fit those domains as well. As a general remark we could say that most of the findings can be thought as common to most of the CIs but each report studied focuses on the most important for each specific case. That way we managed to provide the following matrices and graphs that present the diversity of needs for the various CIs.

7 Matrices

7.1 Matrix of CI domains

According to D1.2 the CIPSEC consortium has identified twenty (20) security requirements based on the input provided by the three (3) pilots. Many of them are also reported in the documents related to other CI domains as well. The 20 common security requirements of D1.2 are:

1. Strong network security management mechanism
2. Strong identification and authentication/authorization mechanism
3. Firm security policy
4. Data confidentiality (through encryption)
5. Forensics Analysis
6. Strong separation between internal and external IT network (design and retain a DMZ, introduce network protection structures (eg.. Firewalls))
7. OT Infrastructure protection
8. OT network protection
9. Secure communication channel
10. Cascading effect protection, threat Interdependencies protection
11. Anomaly behavior detection mechanism
12. High network traffic detection mechanism (for DOS/DDOS attacks)
13. Strong Identification mechanism beyond Type I identification (username-password) for example using security tokens (HSMs)
14. Strong Authentication mechanism
15. A commercial CIS oriented Security Information and Event Management (SIEM) solution
16. A sophisticated network protection mechanism (including firewalls, Intrusion Detection Systems)
17. An antimalware protection mechanism beyond antivirus protection offering wide range of malware resistance
18. Forensics analysis toolset working in association with SIEM system
19. Data privacy
20. A strong cryptography toolbox for data confidentiality and integrity (encryption, digital signatures, security protocol primitives etc.)

Below is the list with the 22 Cybersecurity related elements/features that were pointed by the documents studied regarding the eleven (11) CI domains:

1. Insider threat
2. WAN
3. LAN
4. Operating systems
5. Databases
6. SCADA
7. PLC
8. ICS

9. DCS
10. Authentication
11. Authorization
12. Strong password usage
13. Secure communications
14. Smart grid technologies
15. Mobile banking
16. Lack of expertise
17. Data confidentiality
18. Data integrity
19. Sensors
20. Interlocking systems
21. COTS products
22. Radio infrastructure

It is obvious that there are many common entries between those two lists despite the different names used. For some CI domains like Finance it is explicitly stated that the Mobile banking is important. It is not mentioned in other CIs with the same name but it could easily go under the category of secure communications. We decided to not perform any aggregation to provide a better view of the naming used and what is important per CI domain.

Below is the matrix (Figure 9) that we have compiled based on the documents and reports studied. The matrix presents those 22 features/characteristics and elements which are of high importance for the CI domains studied.

What is important per CI	Chemical	ICT Communication	Energy	Finance	Food	Health	Transportation	Water	Emergency Services	Manufacturing	Nuclear
Insider threat	X		X	X	X	X				X	
WAN	X	X	X	X	X		X		X		X
LAN	X	X	X	X	X	X	X		X		X
Operating systems	X	X			X						X
Databases	X	X				X	X		X		
SCADA	X		X		X		X	X		X	
PLC	X		X					X		X	
ICS	X				X					X	X
DCS	X							X			
Authentication	X	X	X	X		X		X		X	X
Authorization	X	X	X	X	X	X		X		X	X
Strong password usage		X			X						
Secure communications		X		X		X	X	X	X		X
Smart grid technologies			X								
Mobile banking				X							
Lack of expertise				X							
Data confidentiality		X		X					X		X
Data integrity		X			X						
Sensors						X	X	X		X	X
Interlocking systems							X				
COTS products							X				
Radio infrastructure						X	X		X		

Figure 9 What is important per CI domain matrix

Below we have also compiled a graph presenting the percentage of the CIs that share common cybersecurity related concerns. The graph is based again in the 22 elements identified from our study. Figure 10 shows that most of the CI domains analyzed are interested in securing their network and how to enforce better authentication and authorization processes.

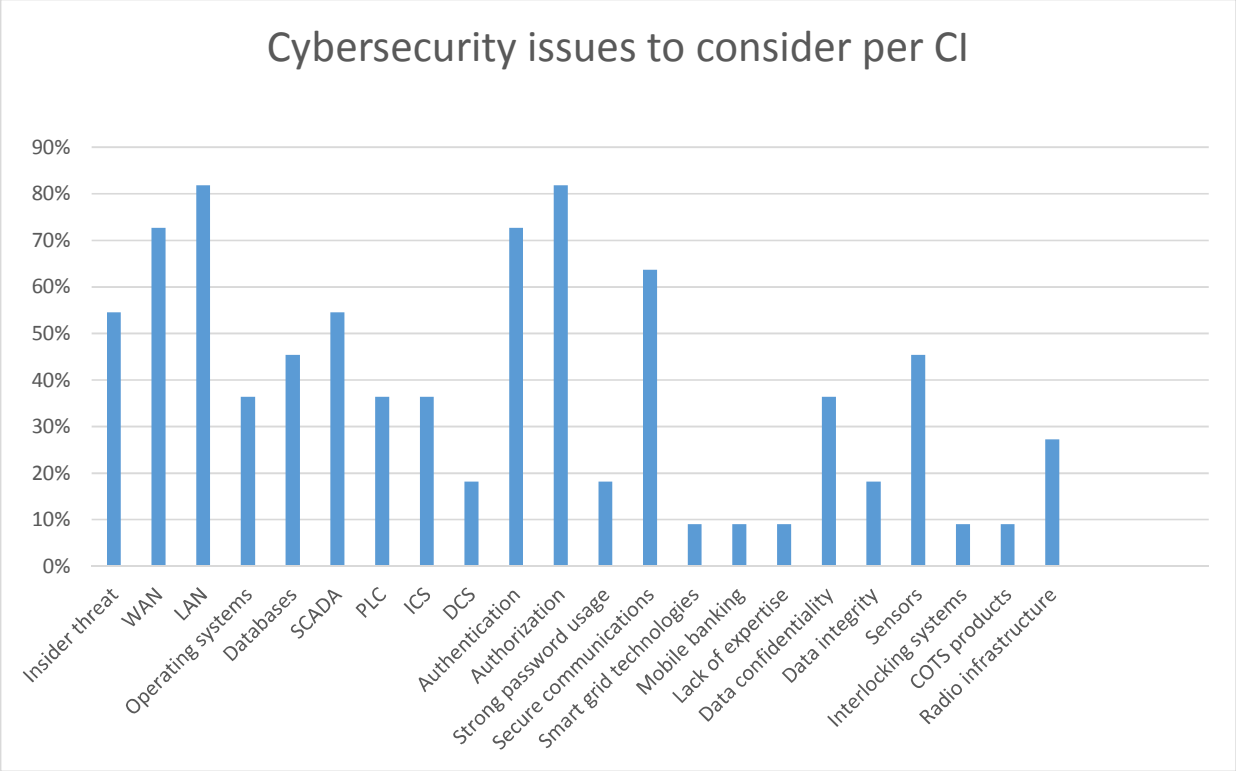


Figure 10 Common cybersecurity concerns/interests between the CIs analyzed.

For every CI domain that was analyzed in Section 5 we have included a section related to the dependencies of each one CI with all the others. A visual representation of how all these CIs are related is presented in Figure 11. The figure also presents the need for addressing the Cybersecurity aspects as a whole by all CI domains in order for all them to work as expected. The lines that connect the CIs in Figure 11 represent that CI domain A is either dependent on CI domain B or B is dependent on A, or both depend each other.

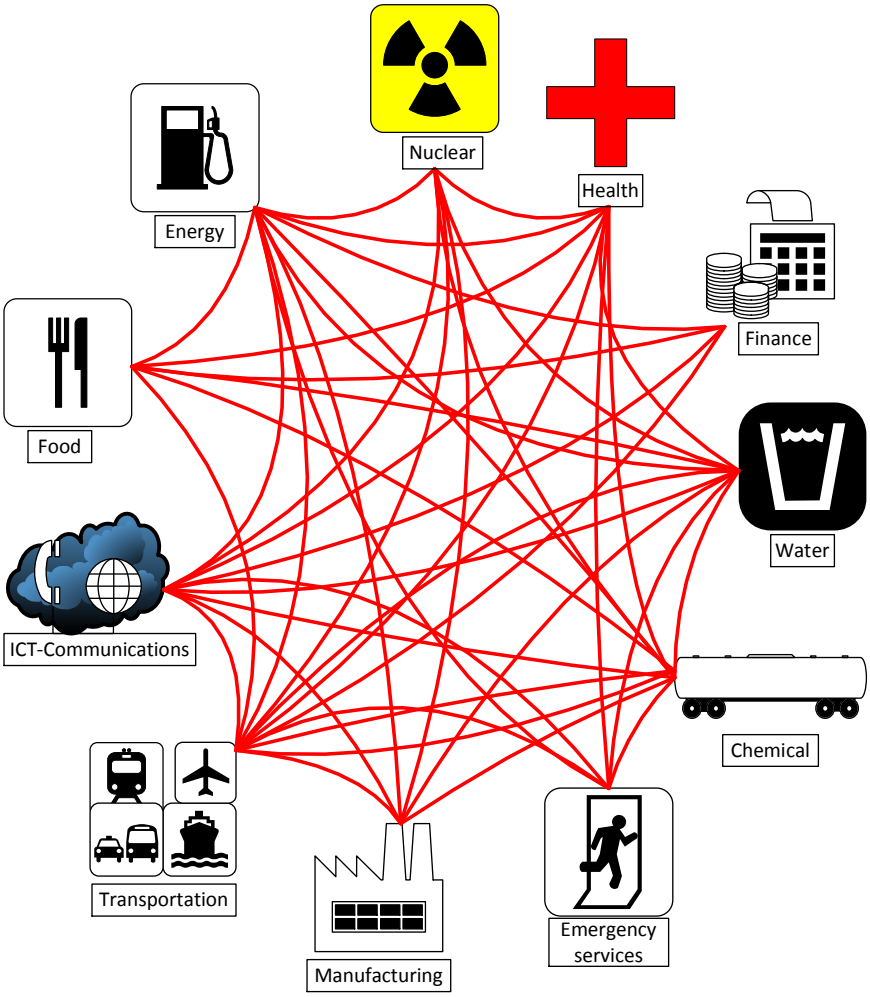


Figure 11 A visual representation of the dependencies between the various CI domain.

7.2 Matrix of pilot domains

CIPSEC consortium has three (3) pilots. None of the documents studied reported explicitly the Environment CI but we think that it could be part of the Water CI which is a common domain for many countries. Similar to Figure 9, Figure 12 presents similar information for the three CI domains that are related to the CI domain where the three CIPSEC pilots belong to. We can see that there is some overlap and complementarity as well.

We believe to some extent this is due to the naming used by each of the domain. Another reason could be the fragmentation (amount) of the features identified. Some of them could be grouped and produce a table with more overlap. E.g. SCADA PLC ISC and DCS systems are referring to control systems of each CI domain and might grouped as one. Nevertheless we wanted to also provide the diversity in the naming between those CIs.

Moreover features like “mobile banking” is not present in any of the three CIs in this figure and “Data confidentiality and integrity” may be hidden under the “Secure communications” category. Strong password authentication is not visible to any of these CIs but these CIs rely on ICT which states clearly that it is crucial for the ICT domain. So if we take under consideration the interdependences between those CIs then most of the identified security requirements should be addressed for almost all CIs.

What is important per CI	Health	Transportation	Water
Insider threat	X		
WAN		X	
LAN	X	X	
Operating systems			
Databases	X	X	
SCADA		X	X
PLC			X
ICS			
DCS			X
Authentication	X		X
Authorization	X		X
Strong password usage			
Secure communications	X	X	X
Smart grid technologies			
Mobile banking			
Lack of expertise			
Data confidentiality			
Data integrity			
Sensors	X	X	X
Interlocking systems		X	
COTS products		X	
Radio infrastructure	X	X	

Figure 12 What is important per the three CI domains which are related to CIPSEC pilots

8 Conclusions

This deliverable (D1.3) describes a taxonomy of different CI environments according to their needs and what should be protected against Cyber-attacks and threats. The reports identify common concerns in different CI domains. This is an initial step to realize common needs of those CIs. This means that security solutions that will be provided to the three pilots may be directly (with no major modifications needed) applied to a set of CI domains with the same concerns and interests. Moreover, the analysis provides directives to the CIPSEC security solutions in order to cover and secure other CI domains as well. Thus, the current report will be used in order to properly tailor the CIPSEC design to the set of target CIs.

It has been clear that many CIs are suffering from many external and internal threats. Almost all the CIs are currently relied upon new ICT technologies to improve efficiency and increase productivity. This has increased the potential attack surface for malicious users.

The CI interdependence has also been increased so it is urgent that every CI should properly address the Cybersecurity aspects so any cooperation between various CI domains remains secure, safe and uninterrupted.

As a general remark we could mention that most of the findings (the security concerns of each CI) are more or less common to the most of the CIs. For example, the “strong password usage” requirement which is visible to some of the CIs it does not mean that is not important to the rest of the CIs as well. The fact is that each report (for each one of the analyzed CIs) studied highlighted the most important requirements. By gathering all those different requirements from the various reports we were able to produce the matrices and graphs of Section 7 which are indeed presenting the diversity of the security requirements and concerns for each CI domain.