TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technology

Diana Carolina Burbano Valencia – 194243IVCM

EU Cybersecurity Certification: Case Study Analysis For Implementation in the transportation sector in the EU

Master's thesis

Supervisor: Andrew J. Roberts
MSc
MCyberSecOps

Cybersecurity
master's degree

Tallinn 2021

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Diana Carolina Burbano Valencia – 194243IVCM

EL-i küberturvalisuse sertifitseerimine: Juhtumiuuringute analüüs rakendamise kohta EL-i transpordisektoris

Magistritöö

Juhendaja: Andrew J. Roberts
MSc McyberSecOps

Küberjulgeoleku magistrikraad

Tallinn 2021

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Diana Carolina Burbano Valencia

14.12.2021

Abstract

The EU has developed a regulatory framework, the EU Cybersecurity Act, and updates to the Network and Information Security (NIS) Directive to strengthen the resilience against cyber threats in the EU. Within these regulations, an EU cybersecurity certification framework is proposed for key sectors such as transportation. This thesis investigates how can a certification scheme, as envisaged by the EU Cybersecurity Act and NIS Directive, be implemented for the transportation sector in Europe.

An action research methodology is utilized to explore the implementation of the EU Cybersecurity certification in the transportation sector using existing sources of information from formal studies or cybersecurity agencies, standards, or bodies such as the European Union Agency for Cybersecurity (ENISA). First, the thesis research shows very few studies into certification schemes for cybersecurity in the EU market and a scarcity of work focused on the transportation sector. Second, the thesis analyses the implementation of the cybersecurity certification on two case study scenarios in the transportation sector. Outcomes of these exercises demonstrate that cybersecurity certification is a complex process to implement; the existent studies and available work concerning cybersecurity certification are not sufficient for the transportation sector.

These results suggest that transport organizations need more support to understand and implement a cybersecurity certification. The thesis concludes by providing general recommendations to transportation organizations to define a policy for cybersecurity certification implementation. Primarily, the thesis emphasizes the need for active collaboration and cooperation between the transportation organizations and ENISA to overcome the different challenges derived from the implementation of the cybersecurity certification. This open communication will be a key starting point to facilitate the implementation process within the sector based on their needs and realistic expectations.

This thesis is written in English and is 71 pages long, including 7 chapters, 6 figures and 15 tables.

Annotatsioon

EL on välja töötanud reguleeriva raamistiku, ELi küberturvalisuse seaduse, ning ajakohastanud võrgu- ja infoturbe direktiivi, et tugevdada ELi vastupanuvõimet küberohtude vastu. Nende määruste raames tekivad transpordisektori jaoks uued väljakutsed, näiteks toodete küberturvalisuse sertifitseerimine ja märgistamine. Käesolevas väitekirjas uuritakse, kuidas saab ELi küberturvalisuse seaduses ja võrgu- ja infoturbe direktiivis kavandatud sertifitseerimissüsteemi rakendada Euroopa transpordisektoris.

ELi küberturvalisuse sertifitseerimise rakendamise uurimiseks transpordisektoris kasutatakse tegevusuuringu metoodikat, kasutades olemasolevaid teabeallikaid, mis pärinevad ametlikest uuringutest või küberturvalisuse ametitest, standarditest või asutustest, nagu ENISA. Esiteks näitab lõputöö uuring, et ELi turul on väga vähe uuringuid küberturvalisuse sertifitseerimissüsteemide kohta ning transpordisektorile keskendunud tööde vähesus. Teiseks analüüsitakse doktoritöös küberturvalisuse sertifitseerimise rakendamist transpordisektori kahe juhtumiuuringu stsenaariumi põhjal. Nende tööde tulemused näitavad, et küberturvalisuse sertifitseerimine on keeruline protsess, olemasolevad uuringud ja olemasolevad tööd küberturvalisuse sertifitseerimise kohta ei ole transpordisektori jaoks piisavad.

Need tulemused viitavad sellele, et transpordiorganisatsioonid vajavad küberturvalisuse sertifitseerimise mõistmiseks ja rakendamiseks rohkem tuge. Lõputöö lõpetab üldised soovitused transpordiorganisatsioonidele küberturvalisuse sertifitseerimise rakendamise poliitika määratlemiseks. Eelkõige rõhutatakse lõputöös vajadust aktiivse koostöö ja koostöö järele transpordiorganisatsioonide ja ENISA vahel, et ületada küberturvalisuse sertifitseerimise rakendamisest tulenevaid erinevaid probleeme. Selline avatud suhtlus on peamine lähtepunkt, et hõlbustada sektori siseselt rakendusprotsessi, mis põhineb nende vajadustel ja realistlikel ootustel.

Magistritöö on kirjutatud inglise keeles, on 71 lehekülge pikk, koosneb 7 peatükist, sisaldab 6 joonist ning 15 tabelit.

List of abbreviations and terms

3GPP	3rd Generation Partnership Project
AHWG	Ad Hoc Working Group
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information (National Security Agency of Information Systems)
AV	Autonomous Vehicle
BIMCO	Baltic and International Maritime Council
BSI	Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Security)
CAL	Cybersecurity Assurance Level
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CER	Critical Entities Resilience
CPA	Commercial Product Assurance
CSA	Cybersecurity Act
CSPN	Certification de Sécurité de Premier Niveau
DDoS	Distributed Denial of Service
DoS	Denial of Service
ECCG	European Cybersecurity Certification Group
ECU	Electronic Control Unit
ENISA	European Union Agency for Cybersecurity
ERTMS	European Rail Traffic Management System
ETCS	European Train Control System
ETSI	European Telecommunications Standards Institute
ETSI TR	ETSI Technical Report
ETSI TS	ETSI Technical Specification
EU	European Union
EUCC	European Union Common Criteria
EUCS	EU Cloud Services Candidate Scheme
EVC	European Vital Computer
FW	Firmware
GDPR	General Data Protection Regulation
GPS	Global Positioning System
GSM	Global System for Mobile communications

GSMA	Global System for Mobile Communications Association
GUI	Graphical User Interface
HW	Hardware
IACS	Industrial Automation & Control Systems
ICS	Industrial Control System
ICSA	International Computer Security Association
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IMU	Inertial Measurement Unit
IoT	Internet of Things
ISA	International Society of Automation
ISO	International Organization for Standardization
IT	Information Technology
ITS	Intelligent Transportation Systems
JRC	Joint Research Centre
LiDAR	Light Detection and Ranging
MIFARE	MIkron FARE Collection System
MW	Middleware
NCAP	New Car Assessment Programme
NCSC	National Computer Security Center
NERC	North American Electric Reliability Corporation
NIS	Network and Information Security
NITES	National IT Evaluation Scheme
NW	Network
NXP	Trademark of a series of integrated circuit
OES	Operators of Essential Services
OWASP	Open Web Application Security Project
RTCA	Radio Technical Commission for Aeronautics
SAE	Society of Automotive Engineers
SCSA	Methodology for sectoral cybersecurity assessment
SIG	Software Improvement Group
SLAM	Simultaneous Localization and Mapping
SOG-IS	Senior Officials Group Information Systems Security
SOG-IS MRA	SOG-IS Mutual Recognition Agreement
SW	Software
UL	Underwriters' Laboratories
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (German: Independent Centre for Privacy Protection Schleswig-Holstein)

VDA	Verband der Automobilindustrie (Association of the Automotive Industry)
VDA-QMC	VDA Quality Management Center
VLAN	Virtual Local Area Networks

Table of contents

List of figures

List of tables

1 Introduction

The transportation sector plays a crucial role in the economic development of the European Union (EU) by enabling the transportation of goods and passengers within countries and across borders. [1]. This digitalisation process opens new opportunities and creates challenges to the transportation sector [2] by increasing dependency on information technologies and systems vulnerable to cyberattacks.

Over the last decade, there has been an increase of cyberattacks against the transportation sector at a global level [3]. Most known cyberattacks and cyber incidents affecting EU countries within the last five years include examples such as:

- **2015, Poland:** A DoS attack was carried out on the polish airline ’LOT’, which disrupted the operation of the IT system that LOT uses for issuing flights plans. The airline was not allowed to depart [4] until the issue was fixed (receive valid flight plans).

- **2016, Netherlands:** The Port of Rotterdam was a victim of a ransomware attack that affected the customs systems disrupting the operation for hours [5].

- **2017, Germany:** The German rail operator ’Deutsche Bahn’ was a victim of the ’WannaCry’ ransomware attack. Although this attack did not disrupt the train operation, the video surveillance, ticket vending machines and electronic departure boards at stations were affected [6].

- **2017, Ukraine:** The Danish shipping company ’Maersk’ reported damage of 300 million dollars by the malware infection ‘NotPetya’, which paralyzed their operations [7].

- **2017, Sweden:** DDoS attacks on two days brought down several IT systems employed by Sweden’s transport agencies, causing train delays and managing operations manually. The first attack occurred in the Sweden Transport Administration (Trafikverket), affecting the IT system that monitors trains’ locations,

the email system, website and road traffic maps. The second attack impacted the website of the government Transport Agency (Transportstyrelsen) and public transport operator (Västtrafik), who provides train, bus, ferry, and tram transport for parts of Western Sweden [8].

- **2018, Denmark:** Danish railway company ´DSB´ suffered a DDoS attack that impacted the ticketing system. Around 15.000 danish travellers could not purchase tickets from the mobile application, website, ticket machines and certain station kiosks. The passengers could buy tickets from staff on trains [9].

- **2019, United Kingdom:** Transport for London was forced to temporarily close down the online facility for its Oyster card system due to a data breach that compromised around 1.200 customer accounts [10].

- **2020, United Kingdom:** Railway station Wi-Fi provider 'C3UKA' exposed traveller data of about 10.000 people who used the free Wi-Fi in the UK railway stations. The database compromised contained 146 million records, including personal contact details, dates of birth, and it was not password protected [11].

- **2020, Switzerland:** The Swiss rail vehicle manufacturer 'Stadler' was infected by malware that allowed attackers to steal and leak sensitive business data on its locations. To continue the production of new trains and their services, Stadler had to reboot all affected systems [12] [13].

- **2020, Spain:** Adif, a public company that manages railway infrastructures in Spain, was a victim of a ransomware attack, which compromised 800 gigabytes of personal and business data (e.g., contracts, invoices, private correspondence, telephone numbers, customer data, certificates, files, tariffs and internal reports). However, the attack was controlled by its internal security services without making the payment required by the criminals [14].

These real-world examples demonstrate the challenges transportation operators face against cyber threat actors. In part, these challenges have been recognised, and the EU has developed a regulatory response, the EU Cybersecurity Act and updates to the NIS Directive. Within these regulations, a new challenge arises for the transportation sector: the certification and labelling of products for cybersecurity. Currently, there are very few

studies into certification schemes for cybersecurity in the EU market, and even little work has focused on individual market sectors. Transportation is a high-priority sector, and therefore certification and labelling of transportation technologies for cybersecurity are of predominant importance.

2 Research Problem

In the last decade, numerous countries have been affected by cyberattacks [15]. Appropriate measures to prepare and respond against cyberattacks are ongoing challenges, especially when the threat landscape continuously changes, making cyber risks difficult to assess and mitigate. Therefore, effective and comprehensive EU cybersecurity policies are necessary for society at all levels (e.g. governments, critical infrastructures, private sector and individuals) to deal with the evolving cyber threats [16].

One example of fast-evolving cyberattacks was Stuxnet, which compromised in 2010 over 15 Iranian nuclear facilities [17], and other countries around the globe, such as Indonesia, India, Azerbaijan and United States. In particular, the damage to Iran was significantly severe; over 1.000 machines were physically degraded. The Stuxnet worm gained access to the industrial program logic controllers of the nuclear plants and caused physical damage to the centrifuges until tearing the machines apart [18]. This cyber-attack demonstrated to be a real ´threat´ becoming the main driver to raise cybersecurity awareness and development of new cybersecurity strategies for critical infrastructures around the world [19].

Since 2013, the European Commission has developed a cybersecurity strategy to enhance the cooperation in cyberspace to respond against cyberattacks, reduce cybercrime and achieve a high common level of cybersecurity across Europe. An outcome of this strategy commitment was the EU NIS Directive, known as the first piece of EU-wide cybersecurity legislation [20]. In particular, the NIS Directive sets out that each EU Member state shall ensure that Operators of Essentials Services (OES) such as energy, transportation, water, banking, healthcare and digital infrastructure, have taken

appropriate and proportionate technical and organisational measures to manage the security risks of the networks and information systems used in their operations [21] [22].

As a result, every EU member state has started to adopt national legislation to follow or 'transpose' the NIS Directive [23] within their legislation. The current progress focuses overall on the protection of critical infrastructure. Whereas the energy sector, part of the critical infrastructure, was the predominant focus of regulatory responses, including guidelines for risk management, minimum security requirements, minimum protection level for energy system operators, cybersecurity maturity framework and supply chain risk management [24]. However, other critical infrastructure sectors such as transportation have not received the same focus or level of activity.

In addition, the transportation sector faces a complex regulatory system that requires a deep understanding of the dense layers of system-of-systems and diverse service providers which characterise the real-time system operations used in transportation. In particular, the sector must find a balance between operational, business and cybersecurity requirements while the continuous digital transformation increases the need for cybersecurity. Furthermore, the industry depends on suppliers with disparate technical standards and cybersecurity capabilities, making it difficult to adhere the operational technology to the security policies required [25].

Considering this situation, the European Commission proposed in 2019 a cybersecurity certification scheme for Information and Communications Technology (ICT) products within the scope of the Cybersecurity Act. However, a detailed policy implementation plan to implement the EU requirements in the transportation sector is not available yet, making it difficult to the stakeholders to take action into this new regulation [26].

There is a lack of understanding of how cybersecurity certification can be implemented in the transportation sector and how transportation stakeholders would operate within the certification framework. That´s why it is crucial to develop recommendations to assist transportation organizations in understanding how cybersecurity certification and labelling could be implemented.

2.1 Research Questions

This thesis investigates the main research question: How can a certification scheme, as envisaged by the EU Cybersecurity Act and NIS Directive, be implemented for the transportation sector in Europe?

To appropriately answer this research question, it is necessary to break down the components of the research topic and develop sub-research questions. The sub-research questions which assist in answering the main research question have been identified as:

- **SRQ1:** What are the main challenges faced by the transportation sector in meeting the requirements of the EU Cybersecurity Act concerning certification?
- **SRQ2:** What are the transportation sector's foremost safety and security priorities? How does this align with the certification scheme proposed in the EU Cybersecurity Act?
- **SRQ3:** What improvements can be made to the EU Cybersecurity Act to implement cybersecurity certification and labelling of products for the transportation sector?

2.2 Purpose

The purpose of this thesis is to provide guidance and recommendations in understanding how the cybersecurity certification framework and labelling of ICT products could be implemented under the EU Cybersecurity Act. This initiative will help the transportation sector to reach maturity in managing and handling cybersecurity risks and threats.

In addition, this thesis research will provide recommendations that will assist the policy implementation of a cybersecurity certification scheme in the transportation sector.

2.3 Objectives

The objectives of this thesis are:

- Provide state-of-the-art cybersecurity standards, guidelines, regulations and policy implementation studies for the transportation sector. Identify gaps in existing knowledge that can assist transportation operators in having a better understanding of

the features, benefits and implementation of the cybersecurity framework and labelling of ICT products proposed by the EU cybersecurity act.

- Identify the main challenges faced by the transportation sector in meeting the requirements of the Cybersecurity Act in regards to cybersecurity labelling and certification.

- Develop recommendations for policy implementation of certification and labelling of the transportation sector under the light of the EU Cybersecurity Act.

2.4 Novelty and contribution

The EU Cybersecurity Act and the NIS Directive provided a high-level common approach for critical infrastructure cybersecurity. However, an ENISA report found that the main cybersecurity gaps in the transportation sector were the lack of detailed policy, standardization and benchmarks for measuring policy implementation effectiveness [27].

The policy for maritime cybersecurity needs to be adaptable to support today, and in the near future, the dynamic threat environment faced. There is a lack of state-of-the-art understanding for a policy of cybersecurity and transportation [28].

In addition, the increase in research of the public governance challenges of smart cities and autonomous and connected systems have emphasized the need for research into cybersecurity policy and protection of transportation critical infrastructure [29].

The transportation sector as a critical operator has not been the subject of research of previous studies in the cybersecurity policy and certification context. The new Cybersecurity strategy for EU countries that was recently released in December 2020 and the ongoing public consultation to prepare a candidate certification scheme for ICT products provide a general overview of the certification process for the products regardless of the sector. There is a lack of formal study and understanding on how cybersecurity product certification and labelling can be implemented within transport operators. Therefore, this thesis will be the first known detailed research study of cybersecurity certification policy implementation in the transportation sector within the EU.

2.5 Scope

This thesis aims to develop recommendations for policy implementation of cybersecurity certification and labelling of the transportation sector based on the EU Cybersecurity Act and NIS Directive. The following activities are in the scope of this thesis:

- State-of-the-art cybersecurity research, standards, guidelines, regulations for the transportation sector.
- Analysis of existing qualitative data of EU cybersecurity transportation stakeholders and data generated from interviews.
- Recommendations for policy implementation of cybersecurity certification and labelling in the EU.

The following items are out-of-the-scope of this research:

- This thesis will not develop a cybersecurity policy for the transportation sector and sub-sectors across the EU or specific countries.
- The thesis might include literature about certification and labelling from non-EU sources; however, the policy implementation recommendations will focus specifically on the EU.
- Sectors co-related with the transportation sector, such as banking and energy, have not been included in the study.
- The focus of this thesis is the EU Cybersecurity Act due to its predominant importance as pan-European legislation for cybersecurity. Other regulations such as General Data Protection Regulation (GDPR) are not the central focus of this thesis.

2.6 Research Methodology

The thesis research aims to identify the main challenges in the cybersecurity certification process under the light of the EU Cybersecurity Act and provide recommendations to facilitate the implementation process in the transportation sector. For achieving this, qualitative research will be conducted and, as a such, utilizes the action research methodology.

Action research is a methodology based on action, evaluation and critical analysis of situations based on collected data to introduce improvements. Because of this, action research is commonly used to bring together theory and practice in pursuit of practical solutions to issues [30], which in the thesis context is the implementation of the cybersecurity certification proposed by the EU Cybersecurity Act in the transportation sector.

To provide practical solutions to 'real-world' scenarios, the methodology develops the research in four main phases:

1. Plan

2. Act

3. Observe

4. Reflect

As depicted in Figure 1, this methodology combines research with action. A cyclic process is triggered by planning the thesis research, continued by actioning solutions to the problem identified, observing and evaluating the solution implemented and reflecting on the results in the light of the data collected [31]. The last phase will lead to the argument and contribution of the thesis research.

Figure 1 - Action Research methodology [32]

This iterative process aims to understand better what is happening around a particular situation by alternating between research, action, and critical reflection. In the context of the thesis research, the stages are developed as follows:

Plan – Diagnosing the problem

Comprises the identification of a problem, research the problem and its probable causes. Overall, this stage comprehends a review of existing information resources surrounding the cybersecurity certification framework implementation proposed by the EU Cybersecurity Act within the transportation sector.

The actual evidence is grouped in the following areas:

- **Current status of existing academic and policy research related to the implementation of the Cybersecurity Act in the critical infrastructure sector:** The study will start with the review of existent formal investigations on the cybersecurity certification framework and EU Cybersecurity Act, which will help to provide a state-of-the-art of existing academic and policy research for the implementation of the cybersecurity certification framework in the critical infrastructure sector, including transportation.

- **State of the art of cybersecurity laws and regulations for the transportation sector in the EU:** This review recognises applicable laws and regulations available for the transportation sector in the EU, also considering the different approaches followed by the countries to adopt these requirements into their national regulations.

- **The current state of the art for cybersecurity standards in the transportation sector:** With this review, the research will provide a state-of-the-art of existing cybersecurity standards from the industry as the central bodies involved in the standardization and harmonization of cybersecurity processes, products and services.

- **Analysis of expert opinions on cybersecurity of the transportation sector:** This area aims to interview transportation sector experts within the EU and provide a qualitative review of the different surveys and consultations conducted. This analysis will support the research to give a current status of the cybersecurity challenges,

priorities and improvements needed for the sector regarding cybersecurity and the complex regulatory framework required to face.

- **Cybersecurity implementation guidelines for implementing the EU Cybersecurity Act**: This review will focus on the existent guidelines developed by ENISA to implement and improve the cybersecurity certification process in the transportation sector according to what is stipulated in the Cybersecurity Act.

Act and observe - Develop a response to the problem, implement and evaluate the solution

Within this stage, observation and action coincide as the research utilizes case studies to collect more information about the implementation process for a cybersecurity certification in the transportation sector. Two real scenarios of the transportation sector are used as case studies to understand better the transportation sector's cybersecurity landscape and how a cybersecurity certification could be implemented. Learning from the experience of implementing the cybersecurity certification in these two scenarios will bring the opportunity to identify the main challenges faced during the process and propose a practical solution for these issues. Implementing the solution will help obtain a greater overall understanding of the cybersecurity certification process. From this continuous learning experience, the researcher will observe the effects and results of the solution with enhanced knowledge. In this direction, the action research will generate knowledge based on the inquiries carried out within the act and observation phases.

Reflect on the results

This stage aims to make a self and critical reflection on the results obtained in the previous phase. The outcomes of the solution implemented will allow to generate recommendations for the implementation of the cybersecurity certification policy in the transportation sector and discuss possible directions for future research.

2.7 Limitations

The enforcement of the EU Cybersecurity Act is mostly a recent topic for the transportation sector. Therefore, we might have limited data from the stakeholders' engagement due to a lack of literacy and awareness of these specific cybersecurity requirements.

Understanding the main challenges for implementing the cybersecurity certification includes expert opinions, which might be considered subjective. In addition, the following external and internal events might also limit the research:

- **External:** the representation of the cybersecurity threat landscape used in the research could change drastically, altering the environment of the transportation sector.
- **Internal:** Legal changes to the definition of the transportation sector as a critical infrastructure could also happen.

2.8 Ethics

The scope of the research only considers public documents and cybersecurity frameworks; no restricted or commercially sensitive information is included in the thesis. Approval for public disclosure of information was gained from all interview participants.

2.9 Thesis Organisation

The thesis has the structure of the action research methodology cycle. There are 7 chapters. Chapter 1 introduces the transportation sector cyber threat landscape and incidents within the last 5 years. Chapter 2 includes the research problem, objectives, scope, research methodology, and the research's motivation. Chapter 3 provides background information about the NIS Directive and EU Cybersecurity Act to give a context to the reader. Chapter 4 synthesises the existing evidence by reviewing the literature, standards, regulations, and guidelines in cybersecurity in the transportation sector. In addition, it presents the outcomes identified within the literature review and analysis of the interviews. Chapter 5 contains the case studies of the transportation scenarios used to identify challenges or problems derived from the cybersecurity certification implementation in practice. Chapter 6 reflects on the results obtained with

the lessons learned and findings drawn from this research, while chapter 7 presents the study's conclusions and the direction for future research.

3 Background

According to the cybersecurity factsheet of the European Commission released in 2017, the cyber incidents and attacks are on the rise, awareness and knowledge of cybersecurity issues is still insufficient, whereas 86 % of Europeans believe that the risk of becoming a victim of cybercrime is increasing [33]. These facts demonstrate that cybersecurity policy is of predominant importance. To deal with ever-changing cyber threats, it is required to provide clear guidance at all levels (e.g., governments, critical infrastructures, private sector and individuals) [16].

In response to this, the European Commission proposed in 2017 an update to the EU Cybersecurity strategy to build strong cybersecurity in the EU [34]. For this purpose, the European Commission emphasizes the reinforcement of the EU's cyber resilience, deterrence and response to cyberattacks through a set of measures such as [34]:

- The establishment of the European Union Cybersecurity Agency (ENISA) as the EU Cybersecurity Agency to permanent assist the EU Member States in dealing with cyberattacks [34].
- A Blueprint to respond quickly, operationally and in unison to cyberattacks [34].
- A new directive to combat fraud and counterfeiting of non-cash means of payment [33].
- An EU certification framework to ensure that products and services are cybersecure [34].
- A network of competence centres to help develop and roll out the tools and technology needed [34].
- Strengthen international cooperation on cybersecurity [34].

The first outcome of this initiative was to enforce in 2018 the NIS Directive, as the first legislative framework on the security of Network and Information Systems, establishing security requirements and obligations for OES [35]. Overall, this Directive aims to ensure preparedness to respond to cyberattacks, enhance the cooperation among the EU member states against cyber security incidents and set appropriate security measures for critical infrastructure operators.

One year later, the European Commission introduced the EU Cybersecurity Act to complement the NIS Directive, which came into force in 2019 [36]. Briefly, this legislation establishes an EU cybersecurity certification framework for products, services, and processes. It designates ENISA as the EU agency for cybersecurity to coordinate across the EU the implementation of the NIS Directive and the certification framework.

While in 2020, a new cybersecurity strategy was released, which proposes a reform of the NIS Directive (NIS 2.0) with a new Critical Entities Resilience (CER) directive to increase the level of cyber resilience, sovereignty and leadership of critical public and private sectors such as transportation [37].

The reform of the NIS Directive will expand the scope and depth of the existing EU rules on critical infrastructure released in 2008 that was mainly focused on energy and the transportation sector [38]. With the new proposal, ten industries will be covered: energy, transport, banking, financial market infrastructures, health, drinking water, wastewater, digital infrastructure, public administration and space. Furthermore, stricter security and notification obligations will be introduced. Now, each EU member state will be able to impose sanctions such as administrative fines up to € 10 million or 2% of total worldwide annual turnover on companies [39], including those in the transportation sector, that are not adhering to the directive accordingly.

The EU Cybersecurity Act established the first EU-wide cybersecurity certification framework to ensure a common cybersecurity approach in products, services and processes [36]. This framework aims to improve cybersecurity protection within the EU market by issuing certificates to the manufacturers with a determined cybersecurity level based on the requirements met. Therefore, the EU market security conditions will improve by increasing trust and security level in the products, leading to positive results in the services and processes that rely on the certified products [40].

ENISA, as the supervisory entity for cybersecurity matters in the EU, opened a public consultation to support the preparation of the EU cybersecurity certification candidate scheme (EUCC) for ICT products [41]. The EUCC scheme has been proposed based on the Common Criteria (CC) standard, which is prominently used for Information Technology Security Evaluation. Overall, the EUCC scheme aims to address the requirements included in articles 46 to 65 of the EU Cybersecurity Act, mainly focused on providing citizens transparency on the security characteristics of products acquired [42]. Then, vendors and providers will have the opportunity to certify that their products meet EU cybersecurity standards, ensuring a critical competitive advantage to satisfy the growing need for more secure digital solutions [43].

4 Plan – Diagnosing the problem

The literature review will provide a state of the art of existing evidence for the main challenges faced by the transportation sector in meeting the requirements of the NIS 2.0 directive and EU Cybersecurity Act for cybersecurity certification. In addition, as part of the literature review, the opinion of cybersecurity experts on the transportation sector will be collected, reviewed, and analysed to identify the sector's main touchpoints and priorities. With this in mind, the literature review will also give an overview of how these priorities are in line with the cybersecurity certification scheme proposed by the EU Cybersecurity Act. Then, the examination of existing guidance of the EU cybersecurity certification scheme will support the expert opinion on the improvements that could be made on the EU Cybersecurity Act to implement cybersecurity certification and labelling of products in the transportation sector. Therefore, to provide the answers to the research questions, the literature review is structured in the following sections:

1. Current status of existing academic and policy research about implementing the EU Cybersecurity Act in the critical infrastructure sector.

2. State of the art of cybersecurity laws and regulations for the transportation sector in the EU and national regulations in EU countries.

3. The current state of the art for cybersecurity standards in the transportation sector.

4. Analysis of expert opinions on cybersecurity of transportation sector.

5. Cybersecurity implementation guidelines for the cybersecurity certification.

4.1 Current status of existing academic and policy research related to the implementation of cyber security certification in the critical infrastructure sector

The literature review shows the existence of very few studies related to cybersecurity certification in the critical infrastructure, and as such other studies focused on the implementation of cybersecurity certification in different contexts were considered.

In addition, this review demonstrates that cybersecurity certification has not been explored specifically for the transportation sector as a whole. The formal studies analyzed are fragmented in different areas that also concerns the transportation sector:

Cybersecurity certification in autonomous vehicles

Cheah and Oka focus the research on the cybersecurity methods to measure the Cybersecurity Level of Assurance (CAL) of vehicles, which is essential for consumers who need to know that the products they buy are safe and secure. The authors propose cybersecurity as a measure of product quality and expose the need for an organization to perform related activities to achieve the CAL defined. In addition, the thesis emphasizes that there is a lack of understanding of what level of cybersecurity is needed between the different suppliers and manufacturers. Moreover, the research also outlines the need for the automotive sector to have a common approach of cybersecurity metrics and guidance on how to determine the metrics for each level of assurance required. This research concludes that safety aspects need to be appropriately considered and implemented between relevant parties to ensure that drivers, passengers and pedestrians are protected from physical injuries related to cybersecurity issues [44].

Another research was identified within the context of cybersecurity certification in autonomous vehicles. Burzio, Cordella, Colajanni, Marchetti and Stabili, in their research, develop an analysis of the autonomous vehicles landscape and expose the ongoing activities of public bodies and regulatory authorities related to cybersecurity certification in the automotive domain. The research highlights the relevance of the

security standard SAE J3061 and the efforts from the EU for the automotive sector. Within this research, the authors propose a ranking based approach to assess the cybersecurity level of autonomous vehicles. Safety aspects of vehicles (i.e., protection of the adult occupants, protection of children, pedestrians, and accident prevention) proposed by the Euro New Car Assessment Programme (NCAP) are included. Overall, this approach provides assistance to the transportation sector to assess the CAL. However, it suits the automotive industry since it is specifically designed for Electronic Control Units (ECUs) that support driver assistance systems and autonomous driving solutions [45]. The Transportation organization still lack reliable and repeatable methods to assess the cybersecurity level as this research proposes.

Cybersecurity certification in software

Hernández-Ramos, Matheu and Skarmeta expose the challenges of implementing the cybersecurity certification proposed in the Cybersecurity Act for the software [46]. The research points out that software providers consider cybersecurity certification to be a costly and complex process that could cause delays in the launch of new systems generating a significant economic impact. Furthermore, the authors emphasize that a certification process requires a joint effort of certification bodies, manufacturers, and software providers to certify a system. The authors explain that a system is composed of different components, subsystems and software modules. Therefore, the overall cybersecurity certification of the system also requires the evaluation of each of its subsystems, components and modules. Thus, the research highlights that the following activities around the certification process are not transparent yet and make software providers more reluctant to implement certifications [46]:

- Standardise the approach to measure the fulfilment of a certain assurance level. There is a lack of standardized and widely used methods to carry out these processes [46, p.99-100].

- Harmonize the different assurance levels provided by existing certification schemes. End users could find it challenging to compare the cybersecurity level of various systems certified with various schemes or based on different standards [46, p.100].

- Reuse of previous certifications. The same component might be deployed in systems that are certified under different assurance levels and contexts; it is not clear if the same software component must be certified again [46, p.100].

- How to determine if a component must be certified after a system update. Depending on the type of software update, a cybersecurity re-certification of the system and component could be required. However, there are no clear guidelines to address this situation to encourage the software providers to re-certify their updated systems [46, p.100-101].

- Define a vulnerability disclosure process to give manufacturers and software providers a period to prepare patches and notify users quickly and accurately before a vulnerability is disclosed. However, it is unclear how the software providers will share this information with manufacturers and end-users, considering the impact this might cause on their reputation. The above situation encourages software providers not willing to share information about their components' vulnerabilities [46, p.101].

Even though the challenges exposed in this research are related to the certification process in software, it also affects the transportation sector also makes use of software within their products, processes or services.

Cybersecurity certification in IoT

Matheu-García, Hernández-Ramos, Skarmeta and Baldini [47] propose in their research a security certification methodology for assessing the fulfilment of several security properties of the IoT devices through a security risk assessment and security testing. In addition, the authors analyse the main challenges associated with the creation and implementation of this certification framework and the efforts required [47, p.65-69]. Overall, the authors expose that there is no common approach to compare and assess the security levels of the different IoT devices deployed. The variety of technologies makes it difficult to understand the requirements to achieve a certain level of security in each context or technology [47, p.65]. The authors expose the need to define a cybersecurity framework for IoT devices, ensuring that key challenges derived from this process must be addressed:

- The different stages of an IoT device's life cycle, including the identification of new potential vulnerabilities and the re-certification process due to an update in the device's security level [47, p.67].

- The security levels of the different components of any IoT device, as an IoT device may have several components with different security levels. Therefore, there is a need to define a consistent way to measure security (e.g., likelihood, impact, vulnerability exposure) at each component and layer [47, p.67].

Even though this research focuses on IoT devices, the challenges outlined are also applicable to transportation systems, which are commonly composed of several components of different technologies that also require life cycle maintenance processes to ensure successful upgrades, and consequently, successful re-certification processes.

Cybersecurity certification in consumer products

Banasinski and Rojszczak focus on protecting consumer products by implementing ICT certification programmes, which is now a concern with the increasing number of smart connected products and the expansion of the Internet of Things (IoT) products. The research revises the existing regulations in the EU for the consumer product safety market, discuss whether they are adequate for cybersecurity purposes and the next steps required to effectively integrate the new EU cybersecurity regulations (including the cybersecurity certification framework) with existing consumer product safety laws. The research concludes that existing regulations in the EU for the consumer product safety market are not adequate for cybersecurity purposes, as the safety concept is oriented to health protection, excluding from scope the risks coming from the exploitation of vulnerabilities in commonly used consumer products [48]. It is needed that relevant parties (e.g., legislators, manufacturers, cybersecurity experts) work together to align the sector's foremost safety and security priorities with the new EU cybersecurity regulations. The current state of the art for the transportation sector is developed in section 4.3.

The formal literature review shows that cybersecurity certification is a challenging process to implement that requires attention from the sector and other relevant parties. In response to this, ENISA released in 2021 the report 'Methodology for sectoral cybersecurity assessments' [49] as a guideline to assess the cybersecurity assurance level of a certification scheme. This methodology was used as one of the information sources

to explore the implementation of the cybersecurity certification in two transportation scenarios. Discussion and outcomes of this exercise are developed with more details in section 5.

4.2 State of the art of cybersecurity laws and regulations for the transportation sector in the EU

The EU Directive 2010/40/EU [50] with its Decision (EU) 2017/2380 [51] established a framework to coordinate, deploy and use Intelligent Transport Systems (ITS) within the EU [52]. In particular, this directive defines priority areas, specifications (e.g., functional, technical, organisational) and measures to implement to ensure compatibility, interoperability and continuity of the transportation services [53], but it does not fully consider requirements in regards to cybersecurity matters.

In the past years, the European Commission has established directives and regulations related to cybersecurity. Table No. 1 lists the main EU directives and regulations applicable to the transportation sector within the scope of cybersecurity:

Year	Name	Description
2013	EU Cybersecurity Strategy - First version	First EU Cybersecurity Strategy sets out strategic objectives and concrete actions to achieve cyber resilience, reduce cybercrime, develop cyber defence policy, develop industrial and technological resources, and establish a coherent international cyberspace policy for the EU [54].
2016	Regulation (EU) 2016/67978	General Data Protection Regulation (GDPR) defines requirements for the protection of personal data processed in all sectors, including transport [55].
2016	Directive 2016/1148	Network and Information Security (NIS) Directive that sets cybersecurity requirements to be adopted in critical sectors such as transportation in conjunction with cross-border collaboration across the EU [20].
2017	Regulation (EU) 526/2013	Regulation to establish the EU Cybersecurity Agency (ENISA) to supervise cybersecurity capabilities in EU countries [56].
2017	EU Cybersecurity Strategy - Second version	This version of the EU Cybersecurity Strategy emphasized the need for measures to build a greater EU resilience to cyberattacks, facilitate detection of cyberattacks and strengthen international cooperation on cybersecurity [33]
2019	EU Cybersecurity Act	This act strengthens the position of ENISA for cybersecurity matters in the EU member states and defines an EU-wide cybersecurity certification framework for ICT products, services, and processes in order to attest their trustworthiness based on EU requirements [36]

Year	Name	Description
2020	EU Cybersecurity Strategy - Third version	This is the most recent version of the EU Cybersecurity Strategy and is focused on improving resilience, technological sovereignty, and leadership of critical infrastructure, strengthening the operational capacity of EU members to prevent, deter and respond to cyberattacks and enhance the international cooperation to advance towards global and open cyberspace [37].

Table 1 - EU Strategy, directives and regulations for the transportation sector

The transportation sector as critical infrastructure is aware that cybersecurity within their products, processes and services can be improved by implementing the cybersecurity certification framework proposed by the EU Cybersecurity Act and NIS Directive. However, this process requires also support from the national regulations of each country and best practices given by the industry.

Each EU member state has adopted national legislation on their own to accomplish the cybersecurity goals enforced in the EU Cybersecurity Act and NIS Directive. The table below provides an overview of the cybersecurity regulations currently in force by France, Estonia and Germany:

Country	Code	Regulation/Law
Estonia	RTI, 22.05.2018, 1	Cybersecurity Act, which provides requirements for the maintenance of network and information systems essential for the functioning of society and state and local authorities, and bases for the prevention and resolution of cyber incidents [57].
Estonia	RTI,10.07.2018, 6	Requirements for risk analysis of network and information systems and description of security measures [58]
France	Laws No. 2013-1168 and No. 2015-917	The “Loi de Programmation Militaire” (the LPM or ‘Military Planning Law’) enabled national public and private sector operators of vital importance (OIV) to protect themselves better and provides the adoption of measures to step up the security.
France	Decree No. 2015-351	Security of information systems for vital operators [59].
France	Laws No. 2018-133	Provides general direction for transposing NIS Directive [60].
France	Law No. 2018- 384	Provides details for the application of the NIS, lists the sectors, types of operators and critical infrastructures concerned [61].
Germany	IT Security Act 2.0 (IT Sicherheits-gesetz)	Provides the minimum level of IT security that operators of critical facilities/infrastructures in the transportation sector must comply with and report to the Federal Office for Information Security (BSI) significant IT disruptions [62].

Table 2 - Cybersecurity laws and regulations in EU countries

As shown in the table above, Estonia, France and Germany have established their own laws and regulations to provide general direction to implement the NIS Directive and cybersecurity act into their nations. Overall, these laws and regulations focus on the following areas:

- Protection requirements of critical operators
- Risk management of critical operators
- Prevention and resolution of cyber incidents

The existence of these regulations implicitly says that these countries are committed to cybersecurity and the NIS Directive mandates.

4.3 The current state of the art for Cybersecurity Standards in the Transportation sector

The ETSI Technical Committee Intelligent Transportation System (ITS) has published numerous specifications and standards on the topic of ITS. Specifically, in the area of security, there are 7 technical specification documents:

Standard Code	Standard
ETSI TS 102 731	Security Services and Architecture [63]
TR 102 893	Security, Threat, Vulnerability and Risk Analysis [64]
TS 102 940	Communications security architecture and security management [65]
TS 102 941	Trust and Privacy Management [66]
TS 102 942	Access control [67]
TS 102 943	Confidentiality services [68]
TS 103 097	Security header and certificate formats [69]

Table 3 - ETSI Security technical specifications for ITS

Within these documents, ETSI provides technical requirements for Intelligent transportation systems in the areas of architecture, communication, access control, confidentiality, trust and privacy. However, these documents do not provide sufficient information on how to implement a secure transportation system.

Currently, cybersecurity Standards for the transportation sector is limited; there are a major number of national and international cybersecurity standards applicable to different sectors such as critical infrastructure, energy or automotive sectors. The table below collects all the standards that might be relevant and applicable to the transportation sector, even though they are not specifically oriented to this sector:

Sector	Country	Body	Standard
Automotive	International	ISO/SAE	DIS 21434: Road vehicles Cybersecurity engineering [70]
Automotive	International	ISO	PAS 21448:2019: Road vehicles — Safety of the intended functionality [71]
Automotive	International	ISO	26262: Road vehicles - Functional safety [72]
Automotive	International	SAE	J3061: Cybersecurity Guidebook for Cyber-physical Vehicle Systems [73]
Automotive	International	SAE	J3101: Requirements for Hardware Protected Security for Ground Vehicle Application [74]
Automotive	Germany	VDA- QMC	AK ACSMS: Automotive Cybersecurity Management System Audit [75]
Automotive	United Kingdom	BSI	PAS 1885:2018: The fundamental principles of automotive cybersecurity [76]
Automotive	United Kingdom	BSI	PAS 11281:2018: Connected automotive ecosystems. Impact of security on safety. Code of practice [77]
Aviation	International	RTCA	RTCA DO-326A (Airworthiness Security Process Specification) [78]
Energy	United States	NERC	CIP-002-5.1a to CIP-014-2: Set of standards and requirements designed to secure the assets required for operating North America's bulk electric system [79]
Critical infrastructure	Germany	BSI	200-1, 200-2, 200-3: Standards of the Federal Office for Information Security (BSI) [80]
Critical infrastructure	International	ETSI	TR 103 303: Protection measures for ICT in the context of Critical Infrastructure [81]
Shipping	International	BIMCO	The Guidelines on Cyber Security Onboard Ships
Shipping	International	BIMCO	Cyber Security Workbook for On Board Ship Use [82]
Shipping	International	BIMCO	Industry Standard Software Maintenance of Shipboard Equipment [83]
All	International	ISO/IEC	15408: Common Criteria for Information Technology Security Evaluation [84]
All	International	ISO/IEC	27001 and 27002: Information security management requirements and security controls [85] [86]

Table 4 - Cybersecurity standards for the transportation sector

By analysing these standards, cybersecurity in the transportation sector is mainly focused on three areas:

- Safety management.
- Secure design, testing and patch management of the suppliers and manufacturers.
- Cybersecurity risk management.

Overall, these cybersecurity standards provide guidance on security requirements that must be implemented to increase the cybersecurity resilience against cyber threats and cyberattacks that could negatively impact the safety and security of the transportation sector. The industry (i.e., road, rail, air, sea) often makes practical adaptations of the different standards based on their needs and risk appetite to limit any damage that could affect them.

Based on study research done by ENISA in 2015 [87], the transport organizations are not open to collaborate and exchange information about cybersecurity among them [87], as there is a lack of awareness for information sharing and collaboration related to cybersecurity matters. This finding limits the optimization of cybersecurity processes through knowledge sharing of best practices and learning experiences from other transportation organizations.

The transportation sector is well known for the complexity of their own systems and infrastructure, for which the active participation and collaboration of the transportation organizations is a key factor to building a cybersecurity resilience network within the sector as they have the details and in-deep knowledge of the different products, systems and technologies used. From this perspective, the transport organizations are the most suitable actors to provide more details and guidelines to ensure that products and services are safe, reliable, and of good quality. Partnering with Cybersecurity Institutions such as ENISA, ANSSI, BSI, among others, will allow addressing the challenges faced to implement cybersecurity controls and measures, leverage lessons learned and ensure optimal solutions for the implementation of the cybersecurity requirements.

4.4 Analysis of experts opinion on cybersecurity of the transportation sector

The thesis research focuses on the implementation of the cybersecurity framework in Europe under the light oCybersecurityerseurity Act. The target sector for this thesis research is the transportation sector. The main purpose is to provide recommendations for the implementation of cybersecurity certification in the transportation sector.

For that purpose, the study research includes the conduction of interviews with three subject matter experts in the cybersecurity area, which profiles and experience are related to cybersecurity or the transportation sector. The interviews involved a total of 3 participants drawn from different stakeholder groups. The size of the interviewers is limited; nevertheless, they provide a good starting point for understanding the position of the different stakeholder groups in regard to cybersecurity certification. The interviews were conducted with the following stakeholders:

Stakeholder group	Institution	Role/department
Public transport	City Transportation Department	Expert in Smart City Transportation
Maritime sector	Ministry of Defence	Expert in cybersecurity strategy and policy
Government	Ministry of Economics and Communications	Expert National Cybersecurity Policy

Table 5 - List of interviewees categorized by stakeholder group

The interviews do not focus on a specific architecture or transportation system but rather to get a comprehensive understanding of the challenges, priorities and improvements needed for the sector regarding the implementation of cybersecurity certification.

The design of the questions in the interview are based on the outcomes of the previous sections and desktop research conducted for the EU Cybersecurity Act and cybersecurity certification framework. Sources such as cybersecurity news feeds, guidelines, reports, surveys, interviews, and other types of information were considered to gather data regarding the current key policies, legislation, standards, initiatives, projects, among other

existent documentation that discusses the implementation of a cybersecurity certification within the transportation sector.

Based on the results of the desktop research, 15 questions were elaborated. A qualitative review of the different answers was performed to identify the key challenges for the implementation of cybersecurity certification. It is important to mention that the challenges identified are based on criticisms and answers of the stakeholders during the interviews. The output of this analysis supports the research to give an overview of the position of the different stakeholders regarding the cybersecurity certification framework and its challenges:

Lack of awareness of EU cybersecurity certification framework and related guidelines

The interview indicates that transport organizations in Estonia do not have sufficient information and clarity about the cybersecurity certification framework proposed in the EU Cybersecurity Act and the impact this new regulation might generate on their processes. Departments such as procurement do not have proper knowledge and skills to address the cybersecurity requirements derived from this regulation, most likely because transport organizations have low awareness of existent guidelines released by leading authorities, bodies or institutions in the cybersecurity topic for the transportation sector (e.g., ENISA). Therefore, available guidelines are not commonly known by transportation organizations and are not usually used as a reference within their processes.

Resistance to collaborate and share information on cybersecurity

A key finding from the interviews is that transportation organizations are not open to share information about cybersecurity issues with external parties, most likely because of the reputational costs and indirect losses derived from cybersecurity incidents (e.g., monetary fines for personal data breaches). However, a need to have any kind of cybersecurity network to collaborate and share information related to cybersecurity matters within the sector is perceived positively.

Limited resources to invest in cybersecurity and resistance to adopt the cybersecurity certifications

Transport organizations still do not give the proper relevance to cybersecurity. This results in minimal effort and limited investments for improving cybersecurity in transportation organizations. In the context of cybersecurity certification, this matter will become a priority for the transportation organizations once the regulation becomes mandatory, which highlights the resistance of transportation organizations to improve cybersecurity proactively within their process unless they are told to do it.

Difficulties to implement the cybersecurity certification into the transportation sector

The cybersecurity certification framework proposed by the EU cybersecurity act is considered as not easy to implement as it comes with costs and administrative burdens that EU countries must be willing to invest. In the context of the transportation sector, there are different factors that difficult this implementation, such as:

- Variety and complexity of the infrastructure, systems and solutions implemented within the transportation organizations. Each organization and EU country have their own flavours and level of sophistication, which makes it hard to define which type of certification is required.

- To what extent a cybersecurity certification must be implemented as any incompliance with the requirements defined could delay the operation of new solutions and technologies, resulting in an obstacle for the digital transformation of the sector by the complexity of bringing up new technologies into the environment.

- How to comply and regulate countries outside the EU when the transportation organizations are doing business with these countries. It´s not easy to impose regulations on non-EU countries such as US and China.

4.5 Cybersecurity guidelines released by ENISA for the implementation of the EU Cybersecurity Act

ENISA, the lead agency for cybersecurity matters in the EU, is actively involved in the development of new guidelines to support the organizations towards the implementation of the cybersecurity certification proposed by the EU Cybersecurity Act. The most relevant publications done by ENISA around this topic are illustrated below:

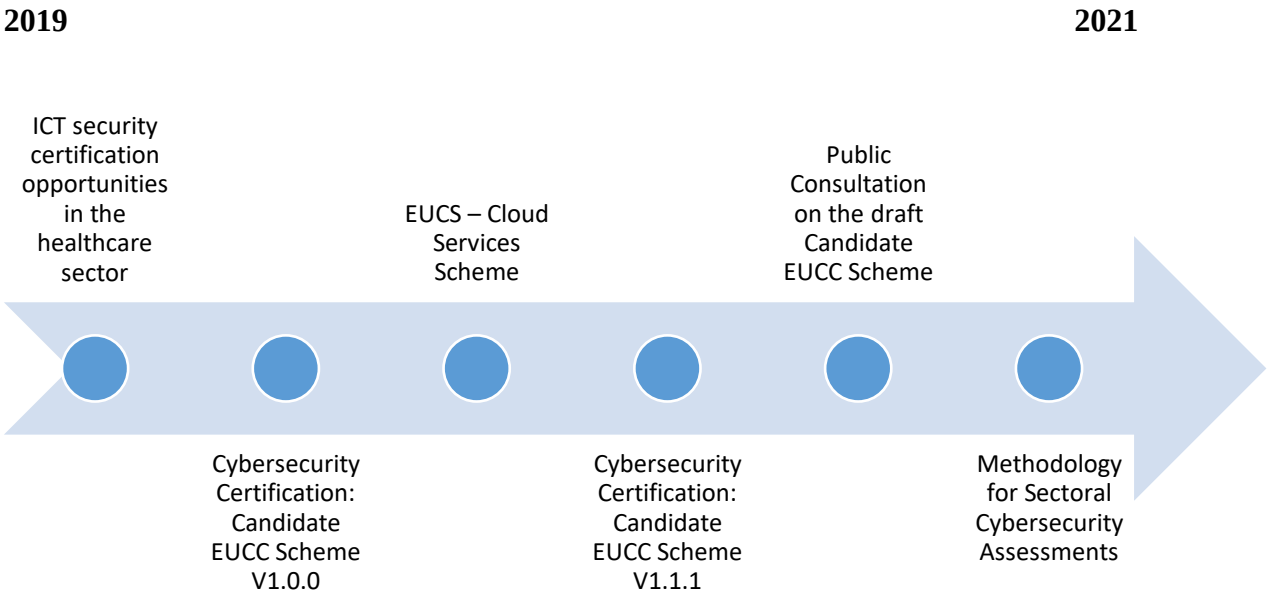

Figure 2 - ENISA publications related to cybersecurity certification [88]

ICT security certification opportunities in the healthcare sector

This report was released in January 2019 and covered functional requirements for a potential ICT security certification scheme in the context of the healthcare sector [89]. Distinct components fall under the scope of this report:

- Semiconductors – chips used in the medical equipment [89].
- Medical devices – all medical equipment, from glucose meters and insulin pumps to sophisticated hospital equipment, interconnected by the Internet of Medical Things [89].

- Electronic services – using traditional IT systems and cloud technology [89].

Overall, ENISA provides a high-level overview of the network and information security of the sector, the ICT components of products and services with their security requirements, the possible opportunities for certification of the components identified and functional requirements. The most relevant outcome of this publication is that ENISA recognizes that it is impossible to certify the healthcare sector as a whole as there are different requirements for semiconductors used in medical devices, devices themselves, the Internet of Medical Things and medical records on the cloud [89]. To overcome this situation, ENISA started to work in a segregated scheme that is able to provide a common assurance level and reuse other schemes to reduce the number of certification approaches.

Cybersecurity Certification: Candidate EUCC Scheme V1.0.0

Following the mandates of the Cybersecurity Act, ENISA set up an Ad Hoc Working Group to support the preparation of a candidate EU cybersecurity certification scheme as a successor to the existing schemes operating under the SOG-IS MRA [42].

In July 2020, ENISA released the first version of the candidate scheme named EUCC scheme (Common Criteria based European candidate cybersecurity certification scheme), which looks into the certification of ICT products cybersecurity, based on the Common Criteria, the Common Methodology for Information Technology Security Evaluation, and corresponding standards, respectively, ISO/IEC 15408 and ISO/IEC 18045 [90]. ENISA opened a public consultation on this draft version to all interested parties to collaborate with the project and share comments that may be useful for the improvement of the scheme that will be reviewed in a later version.

In general, the EUCC candidate scheme comprises 28 chapters that provide answers to the requirements stated in the EU CSA, followed by annexes that define in greater detail the content of the scheme [90]. However, this candidate scheme supports only two assurance levels in the EU CSA: ‘substantial’ and ‘high’. Other schemes may be more appropriate to support the certification of ICT products that are less demanding in terms of levels of assurance.

EUCS – Cloud Services Scheme

In December 2020, ENISA released a draft version of the EUCS candidate scheme (European Cybersecurity Certification Scheme for Cloud Services) for the cybersecurity certification of cloud services. For the preparation of this candidate scheme, ENISA has set up an Ad Hoc Working Group (AHWG) on cloud services as required in the European Cybersecurity Certification Framework [91].

This candidate scheme is based on the ISO/IEC 17065 standard in terms of applicable conformity requirements for the Certification Bodies Accreditation (CAB) performing the certification. While for the assessment of the cybersecurity of cloud services, the scheme utilizes the standards based on the ISO 27000 and International Auditing Standards. The assessment approach proposed is compatible with both certification approaches, allowing cloud service providers to easily integrate the scheme into their current certification and assurance strategy [91].

EUCS also supports the three assurance levels in the EU CSA: 'basic', 'substantial' and 'high'. The requirements at level 'high' are more demanding, whereas the requirements at level 'basic' define a minimum acceptable baseline for cloud cybersecurity, covering all major aspects of cloud security. The 'substantial' level will serve to protect businesses offering a level of choice in between 'basic' and 'high' [91].

The EUCS scheme is part of the European cybersecurity certification framework. It is very different from the EUCC candidate scheme, which focuses on ICT products, while this EUCS candidate scheme is focused on cloud services, an ICT service. This candidate scheme follows the same general presentation as EUCC, with 22 chapters that provide answers to the requirements stated in the EU CSA, followed by annexes that define in greater detail the content of the scheme. In addition, this draft version was also open to the public (all interested parties) to provide feedback on the EUCS candidate cybersecurity certification scheme [91].

Cybersecurity Certification: Candidate EUCC Scheme V1.1.1

In May 2021, ENISA released the second version of the EUCC candidate scheme. Based on the feedback obtained in the external consultation opened for the first version and the ECCG comments, this second version now comprises 26 chapters that still provide

answers to the requirements stated in the EU CSA, followed by annexes that define in greater detail the content of the scheme. Substantial changes are not done in this second version, just cosmetic changes and updates of annex 10 [42]. Essentially, the scope, requirements and certification process remain the same as in the first version.

This EUCC version is still based on Common Criteria (ISO/IEC 15408 and ISO/IEC 18045) and can be considered a horizontal scheme, as it can be used in several sectors [92]. In the long term, this EUCC scheme will replace the current national certification schemes also based on Common Criteria to reduce the number of existing certification schemes.

As shown in figure 3, this version of the candidate scheme will be used by the European Commission for drafting and implementing an Act to adopt the cybersecurity certification scheme, and as such, the scheme will become part of the European legislation [93].

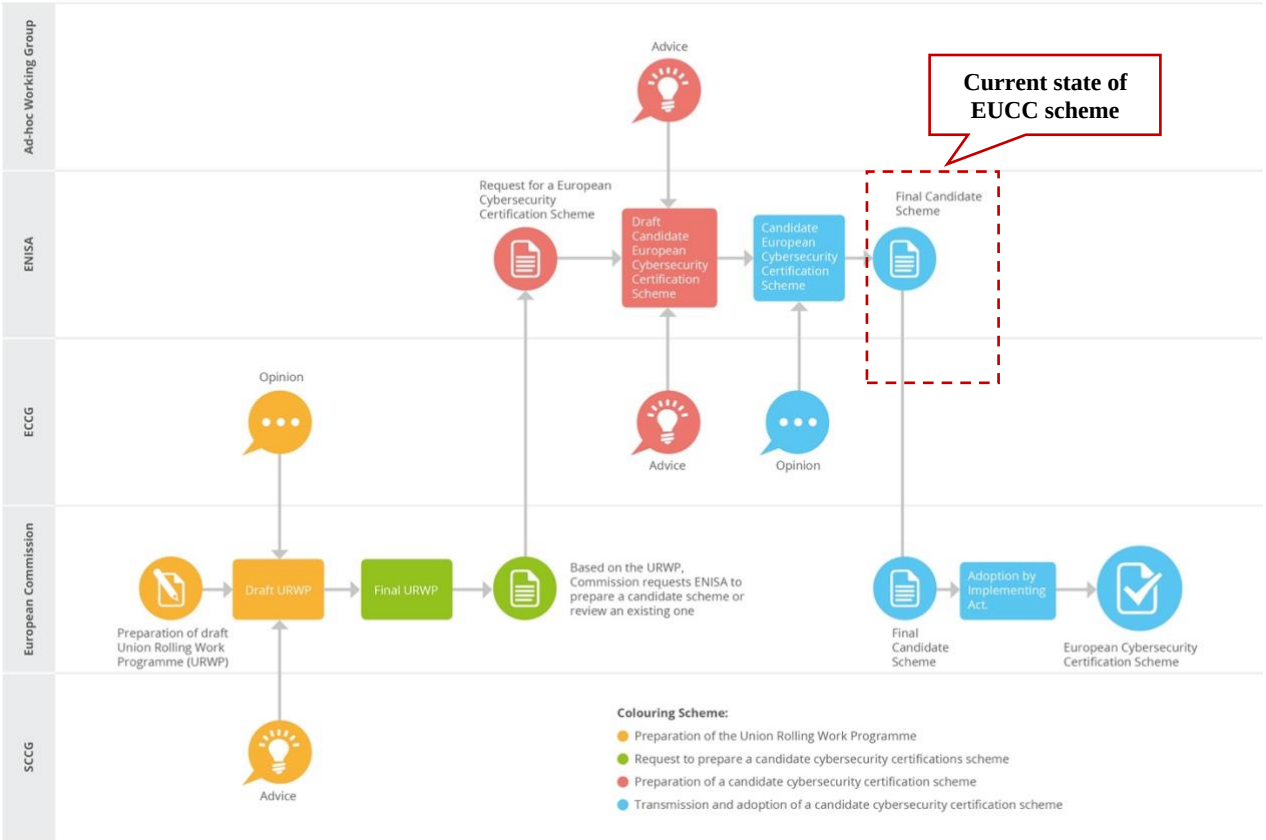

Figure 3 - Diagram flow for the definition of the EU Cybersecurity certification scheme by ENISA [93]

Once it is approved, the main challenges expected to come with the implementation and adaptation of previous schemes into the EUCC scheme are:

- All existing schemes (e.g. common criteria, SOG-IS MRA) cease at the same date [92].
- There is zero parallel emission of EUCC and SOG-IS MRA certificates for the same ICT products during the transition period [92].

The scheme foresees some possible reuse conditions to ease the transition (e.g., reuse of certification activities or reuse of peer assessment results) [92]. In addition, ENISA is working in the following key activities, for which the transportation sector must follow closely:

- Define a transition period to terminate current certification projects under the existing schemes or their easy conversion into the EUCC scheme [92].
- Create transition guides to allow manufacturers to adapt to the new conditions [92].

Public Consultation on the draft Candidate EUCC Scheme V.1.0.0

This report was released simultaneously with the EUCC scheme V.1.1.1 and presented the outcome of the public consultation performed for the first draft of the cybersecurity certification candidate EUCC scheme. Once the EUCC scheme is approved, it would serve as a successor to the existing ICT products certification schemes operating under the SOG-IS MRA (Senior Officials Group Information Systems Security Mutual Recognition Agreement) [94].

Methodology for sectoral cybersecurity assessments (SCSA)

This methodology was released on September 2021 and comprised 9 chapters that provide answers to the identification of security and assurance requirements of the ICT sector using a risk-based approach, followed by annexes that define in greater detail the content of the methodology [49].

This methodology looks into security for sectoral multi-stakeholder systems and drafting sectoral cybersecurity certification schemes. By applying the SCSA Methodology, the sector will have information about the sectoral system and relationships between the stakeholders involved, providing transparency concerning related risks and the potential to optimize the implementation of security for the sectoral system.

All these publications from ENISA show that the cybersecurity certification scheme adoption is an ongoing process and will probably require new discussions and guidelines in the European Commission to facilitate the transition and use of the new scheme, but at some point, it will become a reality throughout Europe for which the transportation sector must adapt and prepare as soon as possible by identifying which ICT products, ICT services and ICT processes such as procurement might be impacted by this new regulation and defining an action plan on how to adapt it internally.

Overall, the literature review developed in chapter 4 provides evidence that a cybersecurity certification process is not an easy topic to implement. In the context of the transportation sector, which is commonly known for the complex infrastructure and variety of ICT products interacting with each other with ICT services, ICT systems, this initiative seems a little bit ‘unrealistic’ to implement. However, all these impressions are given by the theory and different documentation available and collected. This is the reason why in the next chapter, the research will explore how to implement in reality a cybersecurity certification in the transportation sector.

5 Act and observe – Analysis of case studies in the transportation sector

For research purposes, two transport scenarios will be developed and will focus on the interaction of the driver and passenger with the transportation systems, supporting IT assets and external actors (e.g., pedestrians). The scenarios to assess are critical as they present real-life situations and are likely to impact people´s safety negatively, which is of interest to the sector.

The transportation types included in the scenarios are:

- Bus and Autonomous vehicle
- Railway

The purpose of these scenarios is to provide use cases that will help to identify systems, assets and ICT products that will require to have a cybersecurity certification. This information will be used to present to transportation stakeholders the benefits and challenges of the certification process with guidance on how to get required products certified.

5.1 Scenario 1 - Vulnerable Road user warning

This scenario focuses on the safety of the pedestrians, which combines the complexity of speed control and traffic management. The parties involved in this scenario are buses, autonomous vehicles, city surveillance, road safety unit, traffic management system, satellite communications, GPS, smart traffic lights and pedestrians.

As figure 3 shows, the autonomous vehicles will be in motion in the designated road and approach an intersection with traffic lights and surveillance cameras. The road safety units provide warnings to vehicles of the presence of vulnerable road users (e.g., pedestrian or cyclist) in case of a dangerous situation to prevent an unfortunate accident. The vulnerable road users communicate their position and speed to the road safety Units close to the intersection, which will send this data to the Traffic Management System, which will be responsible for notifying other vehicles about approaching in the same direction.

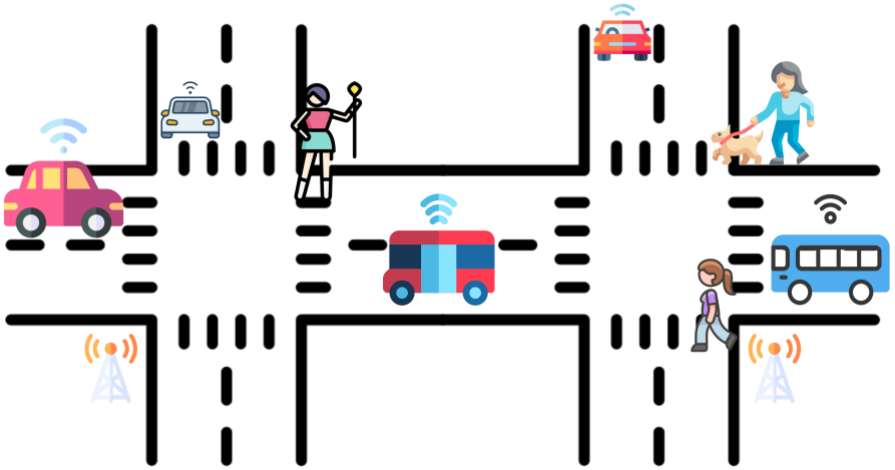

Figure 4 - Scenario 1 - Vulnerable road user warning

Table 6 provides a detailed description of the transportation scenario with a brief overview of the infrastructure elements, systems, and other components:

Context	Vulnerable road user warning
Description	The road safety units provide warnings to vehicles of the presence of vulnerable road users (e.g., pedestrian or cyclist) in case of a dangerous situation to prevent an unfortunate accident. The vulnerable road users communicate their position and speed to the road safety units close to the intersection, and the Traffic Management System will use this information to notify other vehicles approaching in the same direction.
Actors/stakeholders	1- Automated vehicles and their passengers. 2- Road Users (e.g., pedestrians, cyclists). 3- Traffic Management System and responsible operator. 4- Road safe unit and responsible operator (e.g., police).
Infrastructure, system, and components	1. Autonomous vehicles can communicate with road safe units. 2. Road Users wear smart devices to communicate with Traffic Management System. 3. Traffic Management System can communicate with road safe units via the internet. 4. Road safe units can communicate with Traffic Management Systemvia the internet. 5. Road safe units can communicate with autonomous vehicles and smart devices of the road users.
Assumptions	1. The road users are capable of sending their position to the Traffic Management System smart devices. 2. The Road safe units are able to send traffic video and data to the Traffic Management System.

Table 6 - Scenario 1 - Vulnerable road user warning: Details

Table 7 describes the purpose and role played of the different actors involved in the transportation scenario:

Actor	Role	Description
Bus Driver	User	Responsible for driving the buses in the smart cities
Autonomous vehicle	User	Self-driving vehicle. It is designed by cars manufacturers, and it is operated by civilians. The manufacturer's responsibilities include car design, system engineering, modifications and upgrades to the vehicle, as well as the correct operation of the vehicle.
Smart device	User	The road users are capable of sending their position to the Traffic Management System via smart devices.
Remote Operator	Stakeholder	Responsible for actively monitoring the journey of the autonomous vehicle and taking manual driving actions in case of a dangerous situation. The operator must be a licenced driver.
Traffic Control Management Operator	Stakeholder	Responsible for the administration of the traffic management system involving manual activities such as monitoring traffic flows and programming and re-programming traffic lights.
Transport Authority	Stakeholder	Authority responsible for the city Transportation
Telecommunications operator	Stakeholder	The third-party supplier that provides telecommunication services (4G/5G) for the autonomous vehicles and the road safe units located in the smart cities

Table 7 - Scenario 1 - Vulnerable road user warning: Actors and roles

In table 8, the common technology elements are summarized and mapped to ICT products and ICT Services that according to the EU Cybersecurity Act, require cybersecurity certification. In particular, ENISA in the Sectoral Cybersecurity Assessment methodology (SCSA Methodology) introduces the concepts of ICT system and ICT Infrastructure [49] as relevant elements of the cybersecurity certification process; therefore, these categories were also considered. Overall, the assets are categorized as software (SW), hardware (HW), network (NW), middleware (MW), and firmware (FW) to facilitate the identification of the different asset types:

Transport element	Component	Asset Type	Purpose	ICT Category	Responsible for the certification
Network	Mobile Network (4G/5G)	NW	Network infrastructure that enables the communication between remote operators,	ICT Infrastructure	Telecoms operator

Transport element	Component	Asset Type	Purpose	ICT Category	Responsible for the certification
			autonomous vehicles, buses and road users		
	Satellite communications	NW	Network communication between vehicles and roadside units through the internet	ICT Infrastructure	Telecoms operator
Traffic management system	Traffic management system	HW, MW, SW	Provides real-time traffic data to the drivers and road users (e.g. pedestrians)	ICT System	Transportation sector
Buses	Journey Planning and Timetable	SW	Allow transport users to plan journeys, track journeys, plan timetable times, see departures etc.	ICT Service	Transportation sector
	Internal Driver Display Screen	HW, MW, SW	Driver interface (GUI) for displaying real-time route, stop, destination and vehicle position on a map.	ICT Product	Vendor
	Communication Module	HW, MW, SW	Establishes the internet connection.	ICT Product	Vendor
	Internal Passenger Display Screen	HW, MW, SW	It is controlled by the onboard computer. Displays next stop, real-time information about departures from next stops transport zone and media playlists (video/picture) for passengers.	ICT Product	Vendor
Road safety unit	Road safety unit	HW, MW, SW	Device located on the roadside that provides connectivity and information support to passing vehicles, including safety warnings and traffic information through a wireless network.	ICT Product	Vendor
Road users smart devices	Smart device	HW, FW, SW	Road users wear smart devices to communicate with Traffic Management System to send their position.	ICT Product	Vendor
	Mobile application for real-time traffic	SW	Displays the information on the traffic	ICT Service	Transportation sector
Video surveillance system	Video surveillance system	HW, MW, SW	Vehicle cameras	ICT System	Transportation sector
AV vehicle	Vehicle on-board Computer	HW, FW	The vehicle computer.	ICT Product	Vendor
	Camera Sensors	HW, FW	The vehicle onboard cameras.	ICT Product	Vendor
	Geolocation	HW, FW	The vehicle system used for geolocation	ICT System	Vendor
	IMU	HW, FW	Vehicle IMU for capturing of measurement data of AV (acceleration, orientation, heading).	ICT Product	Vendor
	Ultrasonic Sensors	HW, FW	Used for short-range object detection.	ICT Product	Vendor

Transport element	Component	Asset Type	Purpose	ICT Category	Responsible for the certification
	Lidar	HW, FW	LiDAR is used for 3D point cloud mapping to build dynamic maps for SLAM.	ICT Product	Vendor
	Communication modem	HW, FW, SW	The modem ensures communication with other vehicles and infrastructure.	ICT Product	Vendor
	Switch	HW, FW, SW	A switch that connects the onboard unit, sensors and router. Manages access to the network and segments network in VLANs).	ICT Product	Vendor
	Self-driving application	SW	Software application for self-driving vehicles.	ICT Service	Vendor
	Journey Planning	SW	Uses the geolocation data to present a web interface to track the autonomous vehicle.	ICT Service	Vendor
	Actuators	HW, FW, SW	Actuators	ICT Product	Vendor

Table 8 - Scenario 1 - Vulnerable road user warning: IT assets

5.2 Scenario 2 – Railway collision warning

This scenario focuses on the safety of the railway passengers, which combines the complexity of speed control, traffic and route management. The parties involved in this scenario are city surveillance, road safety unit, traffic management system, GSM radio communication, GPS and railway driver.

As figure 4 shows, the train will be in motion in the designated road and approach an intersection with traffic lights and surveillance cameras. The road safety units provide warnings to trains of the presence of a rail intersection in case of a dangerous situation to prevent an unfortunate accident. The trains communicate their position and speed to the road safety Units close to the intersection, which will send this data to the Traffic Management System, which will be responsible for notifying other trains approaching in the same direction.

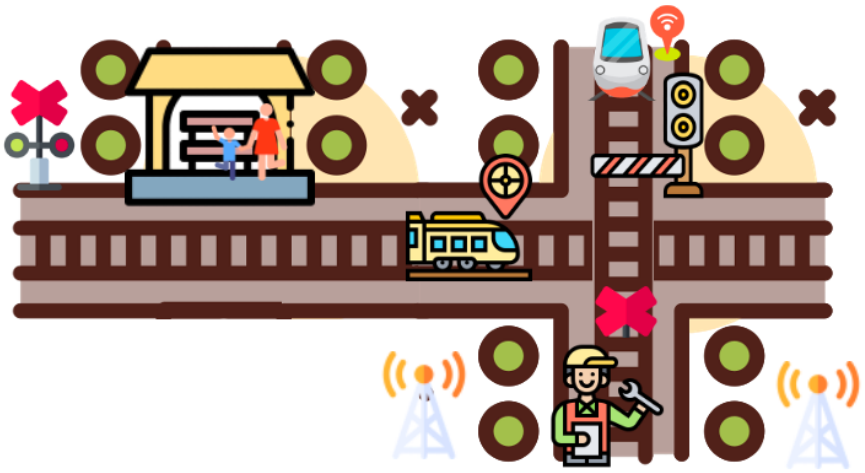

Figure 5 - Scenario 2 - Railway collision warning

Table 9 provides a detailed description of the transportation scenario with a brief overview of the infrastructure elements, systems, and other components:

Context	Railway collision warning
Description	The road safety units provide warnings to trains of the presence ofa railway intersection in case of a dangerous situation to prevent an unfortunate accident. The trains communicate their position and speed to the road safety units close to the intersection, and the Traffic Management System will use this information to notify other trains approaching in the same direction.
Actors/stakeholders	1. Trains, drivers, and passengers. 2. Traffic Management System and responsible operator. 3. Road safe unit and responsible operator (e.g., police).
Infrastructure, system, and components	1. Railways can communicate with the road safe units. 2. Railways have GPS to communicate with Traffic Management System. 3. Traffic Management System can communicate with road safe units via the internet. 4. Road safe units can communicate with Traffic Management System via the internet 5. Road safe units can communicate with railways.
Assumptions	1. The railways are capable of sending their position to the Traffic Management System. 2. The Road safe units are able to send traffic video and data to the Traffic Management System.

Table 9 - Scenario 2 - Railway collision warning: Details

Table 10 describes the purpose and roles played of the different actors involved in the transportation scenario:

Actor	Role	Description
Railway Driver	User	Responsible for driving the railways in the smart cities
Railways	User	It is designed by railway manufacturers, and it is operated by railway drivers. The manufacturer's responsibilities include design, system engineering, modifications, and upgrades to the train, as well as the correct operation of the train.
	User	The railways are capable of sending their position to the Traffic Management System via the GPS
Traffic control agent	Stakeholder	Responsible for actively monitoring the journey of the railways and taking manual driving actions in case of a dangerous situation. The operator must be a licensed driver.
Traffic Control Management Unit Administrator	Stakeholder	Responsible for the administration of the traffic management system involving manual activities such as monitoring traffic flows and programming and re-programming traffic lights.
Transport Authority	Stakeholder	Authority responsible for the City Transportation.
Telecommunications operator	Stakeholder	Provides telecommunication services (GSM radio communication) for the railways and the road safe units

Table 10 - Scenario 2 - Railway collision warning: Actors and roles

In table 11, the common technology elements are summarized and mapped to ICT products and ICT Services that according to the EU Cybersecurity Act, require cybersecurity certification. In particular, ENISA in the Sectoral Cybersecurity Assessment methodology (SCSA Methodology) introduces the concepts of ICT system and ICT Infrastructure [49] as relevant elements of the cybersecurity certification process; therefore, these categories were also considered. Overall, the assets are categorized as software (SW), hardware (HW), network (NW), middleware (MW), and firmware (FW) to facilitate the identification of the different asset types:

Transport element	Component	Asset Type	Purpose	ICT Category	Responsible for the certification
Telecommunications	**GSM radio communication**	NW	Network infrastructure that enables the communication between remote operators and railways	ICT Infrastructure	Telecoms operator
Rail Traffic Management system	**European Rail Traffic Management system (ERTMS)**	HW, MW, SW	Traffic management systems need knowledge on actual train position, train data (e.g. train length, train type) in combination with route settings, planned train	ICT System	Transportation sector

Transport element	Component	Asset Type	Purpose	ICT Category	Responsible for the certification
			path, traffic conflicts. On the other hand, they can provide information for shippers, interact with the energy system.		
European Train Control System (ETCS)	**European Train Control System (ETCS)**	SW	The ETCS is a system of systems for the signalling and control of the European Rail Traffic Management System (ERTMS) [95]. The core component of the onboard equipment is the European Vital Computer (EVC).	ICT System	Transportation sector
Real-time positioning	**GPS**	HW, FW	It allows other platforms/applications to access and share railway localisation data between them.	ICT Product	Vendor
	Rail map platform	SW	For precise and reliable data of the railway tracking (e.g. movement authorisation, speed profile, gradients). This 'rail map' could be interconnected with all other railway assets providing information (e.g. to feed in the localisation database or to provide information for good tracking).	ICT System	Transportation sector
Trains	**Driver assistance system**	SW	Software application that provides assistance to the driver	ICT System	Transportation sector
	Journey Planning and Timetable	SW	Allow transport users to plan journeys, track journeys, plan timetable times, see departures etc.	ICT Service	Transportation sector
	Internal Driver Display Screen	HW, MW, SW	Driver interface (GUI) for displaying real-time route, stop, destination and vehicle position on a map.	ICT Product	Vendor
	Internal Passenger Display Screen	HW, MW, SW	Controlled by the onboard computer. Displays next stops, real-time information about departures from next stops, transport zone and media playlists (video/picture) for passengers.	ICT Product	Vendor

Transport element	Component	Asset Type	Purpose	ICT Category	Responsible for the certification
	Passenger information system	SW	Systems that facilitate comfort and service to the passenger, such as Passenger Announcement Systems, Passenger Information Systems, off-boarding doors, stops, etc	ICT System	Transportation sector
	European Vital Computer (EVC)	HW, FW	Computer that hosts the train control functions, including vital functions such as the emergency braking function.	ICT Product	Vendor
	Communication modem	HW, FW, SW	The modem ensures communication with other railway vehicles and infrastructure.	ICT Product	Vendor
	Access point	HW, FW	Access point located inside the railways to provide internet service on board	ICT Product	Vendor
Railroad	**Sensors**	HW, FW	The sensors are used to sense the obstacles and cracks in the railway track when the train is moving	ICT Product	Vendor
	Road safety unit	HW, MW, SW	Device located on the roadside that provides connectivity and information support to passing railways, including safety warnings and traffic information through a wireless network.	ICT Product	Vendor
Video surveillance system	**Video surveillance cameras**	HW, MW, SW	Cameras located inside the railways, stations and the roads	ICT Product	Vendor

Table 11 - Scenario 2 - Railway collision warning: IT assets

5.3 Main challenges of the cybersecurity certification process in transportation scenarios 1 and 2

By analysing scenarios 1 and 2, we can observe that 22 and 16 products are in the scope of the cybersecurity certification framework proposed by the EU Cybersecurity Act, as they are considered as ICT products and ICT services [96] and ICT Systems [49]. It is important to highlight that the cybersecurity certification of the ICT products [42] and ICT Infrastructure [49] is the responsibility of the vendor (e.g., telecommunication

operators, manufacturers). Therefore, the transportation sector needs to face the following challenges:

- How to certify an ICT Service or ICT System. Currently, the candidate certification scheme proposed by ENISA [42] and the respective guidelines are focused on the certification process for ICT Products. The transportation sector does not have precise guidance on the best approach to certify these types of assets; it is uncertain if an ISO 27001 certification would be sufficient as the expectation from the EU is to have a cybersecurity certification of ICT products, ICT services and ICT processes [97].

- Due to the complexity of the transportation systems, several ICT products are identified in these scenarios (13 ICT Products). This means that the transportation sector would have to assign resources to manage the certificates of these products and related contracts/agreements established with the vendors as the main responsible for the certification of the products and the assurance level provided. Providing the certificate for the respective ICT Product is a good first step to improve the cybersecurity level of the transportation environment. However, it is important to monitor the vendor and the validity of the certificates to ensure that the security requirements and expectations by the sector are met.

- The reuse of existent certificates could be more complex than expected. Table 12 provides a list of relevant standards and specifications that can be used for assessing the overall cybersecurity posture of a product:

Product / component / Industry	Cybersecurity Standard/Certification Scheme	Body	Country
IT product	Certification de Sécurité de Premier Niveau (CSPN) [98]	ANSSI	France
IT product	Commercial Product Assurance (CPA) [99]	NCSC	UK
IT product	Common Criteria [100]	Signatories of the CCRA, Signatories of the SOG-IS	International
IT product	European Privacy Seal [101]	EuroPriSe	Europe
IT product	National IT Evaluation Scheme (NITES) [102]	Cybersecurity Agency of Singapore	Singapore
IT product	Software Improvement Group (SIG) Software Quality Model for Security [103]	SIG	Netherlands

Product / component / Industry	Cybersecurity Standard/Certification Scheme	Body	Country
IT product	UL Cybersecurity Assurance Program (UL 2900-1 / 2) [104]	UL	USA
IT product	ULD Datenschutz-Gütesiegel [105]	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein	Germany
Industry 4.0 and Industrial Control System (ICS)	ISA/IEC 62433 (Security for Industrial Automation and Control Systems) [106]	ISA/IEC	International
Industry 4.0 and Industrial Control System (ICS)	IACS Cybersecurity Certification Framework [107]	JRC	Europe
Telecommunications	GSMA Network Equipment Security Assurance Scheme [108]	GSMA and 3GPP	International
Web application	OWASP Application Security Verification Standard (including OWASP Top Ten) [109]	OWASP	International
Web application	OWASP Testing Guide [110]	OWASP	International
Internet of Things (IoT)	IoT Security Testing Framework [111]	ICSA Labs	USA / International
Internet of Things (IoT)	MIFARE Security Certification [112]	NXP	International MIFARE products
Internet of Things (IoT)	ISO/IEC 19792 (Security evaluation of biometrics) [113]	ISO/IEC	International Biometric systems

Table 12 - Cybersecurity standards / certification schemes available for ICT Products

These standards and certification schemes can have different approaches to evaluate the cybersecurity assurance level of a product. The EUCC candidate scheme is proposing a comprehensive way to reuse different certification schemes; however, ENISA, within their guidelines, does not provide sufficient information to the sectors which certification types/standards are comparable/acceptable/reusable under the proposed candidate scheme EUCC. Currently, the sectors do not have clear visibility if the current certificate of their ICT products could be reused by the EUCC to help them to take the decision to apply to this certification scheme.

- The Cybersecurity Act do not provide sufficient guidance on which assurance level (i.e., basic, substantial, high) should be associated to the potential impacts (e.g., business, operations, reputation, health, life). Furthermore, the transportation companies need guidance on how to decide which ICT products ‘must’ have a

certificate, and moreover, what level of assurance (i.e., basic, substantial, high) is adequate for the specific product. ENISA, within their guidelines, does not provide sufficient information as to what is expected or needed to have a certification in the transportation sector. In September 2021, ENISA released a methodology proposal (SCSA) [49] to identify the security and assurance requirements for ICT services, ICT processes or ICT products based on the risk associated with their intended use. This methodology intends to integrate the Standard 15408 (Common Criteria) and ISO 27001 (Information Security Management) to make the methodology applicable to ICT Products, ICT Processes and ICT Services, which implementation process isn´t easy, making it more difficult to understand the methodology proposed.

Therefore, as part of the thesis research, a solution is proposed to solve the complexity derived from the implementation of the EU cybersecurity certification. This solution consists of assessing the worth of the products, processes and services identified in scenarios 1 and 2, based on the impact and consequence of any damages that could generate to the transportation organization. This process will allow identifying the criticality of the IT assets for the transportation sector based on the impact on the people´s safety (e.g., life, health) when something goes wrong with the ICT Product, ICT Infrastructure, ICT system and ICT service. Based on the criticality assessed, the transportation sector will be able to identify the relevance of the ICT Products, ICT Infrastructures, ICT systems and ICT services and make a decision of the most appropriate level of assurance for the cybersecurity certification.

The impact assessment performed uses the criteria defined by ENISA in the SCSA [49]:

Impact area	Negligible	Minor	Moderate	Major	Catastrophic
Business operations and functionality	Limited impact on a single organization	Significant impact on a single organization	Limited impact on multiple entities in a sector or Significant impact on a few entities in a sector	Significant impact on multiple entities within a few sectors or Significant impact on a few entities within multiple sectors	Disruption of an entire sector and/or significant impact on the business, economy and society as a whole
Impact on citizens (e.g. failure to meet expected	Minor impact on daily activities of citizens	Minor impact on daily activities of citizens	Major impact on daily activities of citizens	Major impact on daily activities of citizens	Severe impact on daily activities of citizens

Impact area	Negligible	Minor	Moderate	Major	Catastrophic
availability of services)					
Type of data processed	Sectoral Intellectual Property	Personal data	Special categories of personal data	Data essential for critical infrastructures	Data affecting national security
Reputation and trust	Minor damage to the reputation of a few organizations	Minor damage to the reputation of many organizations and/or a sector	Major damage to the reputation of many organizations and/or a sector	Major damage to the reputation of the whole sector and/or damage to trust in specific technology or service(s)	Major damage to the reputation of more than one sector and/or loss of trust in specific technology or service(s)
Contractual requirements	Minor non-compliance with contractual requirements	Minor non-compliance with contractual requirements	Major non-compliance with contractual requirements	Major non-compliance with contractual requirements	Major non-compliance with contractual requirements
Health and life	N/A	N/A	Negative effects on health for people and/or environment that may not be recoverable	Life-changing health effects and/or environmental damage	Potential loss of life and/or environmental damage
Cybersecurity Assurance level Proposed	**Basic**	**Basic**	**Substantial**	**Substantial**	**High**

Table 13 - Cybersecurity assurance level proposed per impact level used by ENISA in the SCSA

Table 14 provides information on the proposed assurance level for the ICT products identified in scenario 1 of the transportation sector:

Component	ICT Category	Responsible for the certification	Impact	Assurance level
Mobile Network (4G/5G)	ICT Infrastructure	Telecoms operator	Moderate	Substantial
Satellite communications	ICT Infrastructure	Telecoms operator	Moderate	Substantial
Traffic management system	ICT System	Transportation sector	Major	Substantial
Journey Planning and Timetable	ICT Service	Transportation sector	Minor	Basic
Internal Driver Display Screen	ICT Product	Vendor	Minor	Basic

Component	ICT Category	Responsible for the certification	Impact	Assurance level
Communication Module	ICT Product	Vendor	Minor	Basic
Internal Passenger Display Screen	ICT Product	Vendor	Minor	Basic
Road safety unit	ICT Product	Vendor	Moderate	Substantial
Smart device	ICT Product	Vendor	Minor	Basic
Mobile application for real-time traffic	ICT Service	Transportation sector	Minor	Basic
Video surveillance system	ICT System	Transportation sector	Major	Substantial
Vehicle on-board Computer	ICT Product	Vendor	Major	Substantial
Camera Sensors	ICT Product	Vendor	Major	Substantial
Geolocation	ICT System	Vendor	Moderate	Substantial
IMU	ICT Product	Vendor	Moderate	Substantial
Ultrasonic Sensors	ICT Product	Vendor	Major	Substantial
Lidar	ICT Product	Vendor	Major	Substantial
Communication modem	ICT Product	Vendor	Moderate	Substantial
Switch	ICT Product	Vendor	Moderate	Substantial
Self-driving application	ICT Service	Vendor	Catastrophic	High
Journey Planning	ICT Service	Vendor	Minor	Basic
Actuators	ICT Product	Vendor	Major	Substantial

Table 14 - Scenario 1 - Vulnerable road user warning: Assurance levels proposed

While table 15 provides information on the proposed assurance level for the ICT products identified in scenario 1 of the transportation sector:

Component	ICT Category	Responsible for the certification	Impact	Assurance level
GSM radio communication	ICT Infrastructure	Telecoms operator	Moderate	Substantial
European Rail Traffic Management system (ERTMS)	ICT System	Transportation sector	Major	Substantial
European Train Control System (ETCS)	ICT System	Transportation sector	Major	Substantial
GPS	ICT Product	Vendor	Major	Substantial
Rail map platform	ICT System	Transportation sector	Major	Substantial
Driver assistance system	ICT System	Transportation sector	Major	Substantial
Journey Planning and Timetable	ICT Service	Transportation sector	Minor	Basic
Internal Driver Display Screen	ICT Product	Vendor	Minor	Basic

Component	ICT Category	Responsible for the certification	Impact	Assurance level
Internal Passenger Display Screen	ICT Product	Vendor	Minor	Basic
Passenger information system	ICT System	Transportation sector	Minor	Basic
European Vital Computer (EVC)	ICT Product	Vendor	Catastrophic	High
Communication modem	ICT Product	Vendor	Moderate	Substantial
Access point	ICT Product	Vendor	Minor	Basic
Sensors	ICT Product	Vendor	Major	Substantial
Road safety unit	ICT Product	Vendor	Major	Substantial
Video surveillance cameras	ICT Product	Vendor	Major	Substantial

Table 15 - Scenario 2 - Railway collision warning: Assurance levels proposed

By analysing scenarios 1 and 2 with the solution implemented, we can observe in figure 4 that approximately 70% of the IT assets identified in each scenario are considered relevant and require a cybersecurity certification of assurance level 'Substantial' or 'High'.

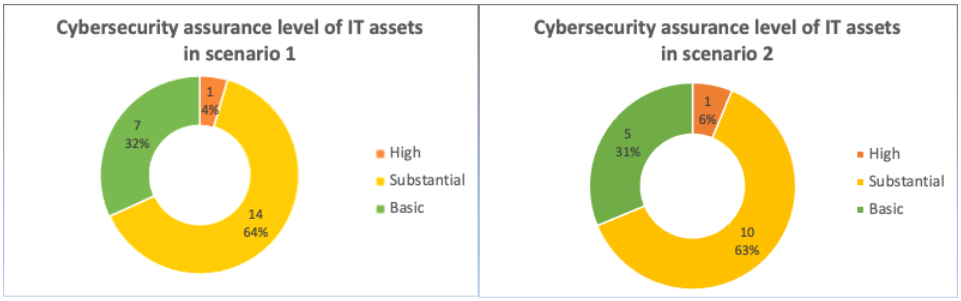

Figure 6 - Overview of cybersecurity assurance levels in scenarios 1 and 2

The transportation sector could use this approach to decide on the IT assets that must have a cybersecurity certification and the respective assurance level. For the ICT products with risk impact of level 'Minor', a cybersecurity certificate of assurance level 'basic' would be the most appropriate. Nevertheless, the transportation sector could consider the relevance of the IT assets to decide whether a cybersecurity certification is needed or not. Currently, the EUCC scheme covers any type of ICT product aiming to reach the assurance levels 'substantial' or 'high'. Therefore, it is up to the transportation sector to think about other standards or certification schemes that could be more appropriate to support the cybersecurity certification of ICT products that are less demanding in terms of levels of assurance.

In addition, it is important to consider that sometimes, an assurance level may be forced through regulations; for instance, a regulation that is applicable to a specific ICT product such as IoT or autonomous vehicles may enforce to obtain a cybersecurity certification of a higher level of assurance. However, defining precisely which assurance level is suitable to the overall transportation sector is beyond the scope of this thesis research.

6 Reflection on the results

Based on the exercise and results obtained in the previous chapter, 70% of the components identified in the transportation scenarios are still a candidate for the cybersecurity certification; this number still means a high effort that transportation organizations need to consider for their operations.

The implementation of the cybersecurity certification framework proposed in the EU Cybersecurity Act comes with costs, and the European Commission needs to make sure that countries can invest in it. The study research demonstrates that this regulation is a challenge that comes with a high administrative burden to the sectors. It is important to keep a balance between theory and practice, which means that transport organizations need more support to understand and implement a cybersecurity certification as the requirements imposed upon them seem difficult to achieve.

The following recommendations provide general guidance to transportation organizations in the definition of a policy for cybersecurity certification implementation based on the sector needs:

Establish working groups for cybersecurity certification and encourage Pan-European cybersecurity cooperation within the sector

Cybersecurity agencies, institutions and bodies have general knowledge of the transportation sector and related products, processes and systems, while transportation organizations do not have dedicated skills in cybersecurity. In order to have more realistic guidelines to implement the cybersecurity certification considering the cybersecurity risks and threats the sector faces, it is required active participation or support from the

transportation organizations to generate a cybersecurity policy implementation in the sector. For this purpose, a coordinated joint approach for the implementation of the cybersecurity certification between the transportation organizations must be strongly encouraged and supported by ENISA through the establishment of adequate joint working groups.

The transportation organizations must interact with each other and ENISA to overcome complexity and incompatibilities between the standards and certification schemes. This will make sure that all relevant challenges, experiences and good practices for cybersecurity certification and standardization requests will be shared and considered jointly. Consequently, this will assist the definition of policy implementation of cybersecurity certification in the transportation sector.

Furthermore, the joint working group will allow quick access to information related to cybersecurity certification and areas of concern for the transportation sector.

Define a cybersecurity certification policy

It's important to create a cyber security policy for the implementation of the EU cybersecurity certification framework. The policy helps employees to understand their role and responsibilities in implementing the cybersecurity certification of the products, processes and services they are accountable. The following areas must be covered at least:

- The type of cybersecurity certification schemes accepted within the organization.
- Criteria to determine the cybersecurity assurance levels required for the products, processes and services.
- Cybersecurity management of third-party suppliers/manufacturers.
- Monitor and review the cybersecurity certifications and their validity.

Define the cybersecurity certification schemes accepted within the organization

The proposed EU Cybersecurity certification framework helps to solve the present fragmentation challenge in the market to evaluate cybersecurity assurance levels in products, processes and services. A smooth transition should be available for the

transportation organizations, considering the compatibility between the existent certification schemes and the EUCC scheme proposed.

The existence of a central repository with the compatibility level of the current certification schemes helps transportation organizations to have visibility of the different certification schemes in use and efforts needed to adapt them to the EU cybersecurity certification framework. The most accepted cybersecurity certification schemes (those that can be re-used in the EUCC certification scheme) will be the baseline for the cybersecurity certification schemes accepted in the products and services of the transportation organizations.

At some point, this smooth transition from existent certification schemes to the most accepted certification schemes will encourage transportation organizations to implement the EU cybersecurity framework proposed by ENISA, reducing the existence of different certification schemes and converging into a common certification approach, which is the final goal of the European Commission.

Define a process to select the cybersecurity assurance level required

Transportation organizations must define a process to select the cybersecurity assurance level required for the specific product, process and service of concern. This process definition requires the involvement of relevant stakeholders such as procurement, cybersecurity and transport operations.

The first step is to have an inventory of ICT products, ICT processes and ICT services that will provide visibility of the different technologies in use and respective vendors. To facilitate the selection of the cybersecurity assurance level for a specific ICT product, ICT process or ICT service; the research proposed a simple method to assess their criticality based on the impact (e.g., operations and functionality, impact on citizens, type of data processed, reputation and trust, contractual requirements, health and life) that could generate to the transportation organization if something goes wrong with them.

However, the transportation organizations may consider integrating into the impact assessment of the IT assets other criteria relevant to the organization, such as security requirements in confidentiality, integrity and availability. This additional criterion will help the transportation sector to have a more accurate cybersecurity assessment during

the selection of the assurance level required for a specific product, process or service. The higher accuracy of defining the target of the cybersecurity certification, the more precise and detailed identification of cybersecurity requirements and respective assurance levels.

Integrate cybersecurity experts in the management of third-party suppliers and manufacturers

The implementation of cybersecurity certifications in the products, processes and services impacts the agreements between the transportation organization and the suppliers/manufacturers primarily. The transportation organizations need to remove dependency on the suppliers and ensure that new requirements are being answered by the most suitable vendor.

For this purpose, there is a need to integrate cybersecurity experts in the procurement process to manage the different requirements that third parties must provide. For instance, a dedicated unit (e.g., Centre of Excellence) for handling cybersecurity topics/requirements in procurement processes can provide the support needed during this process.

Define a process to review and monitor the cybersecurity certifications

A process to review and monitor the cybersecurity certifications of the transportation organization must be in place. It is important that the transportation organization reviews the validity of a cybersecurity certification in a periodic manner to request the re-certification to the respective vendors.

In addition, the process must also consider if/when/how a cybersecurity incident affecting the certified product, process or service should trigger a re-assessment. This process should also provide clear guidance on how to react when a cybersecurity incident affects a product, process or service certified to trigger any ex-post investigative review outside of their normal audit cycle to ensure that the cybersecurity assurance level is maintained.

7 Conclusion

The guidelines released by ENISA for the implementation of the EU cybersecurity certification framework is a good starting point towards the achievement of the EU Digital Single Market Strategy, but different opinions and needs exist in the different sectors such as transportation. This EU cybersecurity certification framework provides a common approach to assess the cybersecurity assurance level of a product, process and service and solves the fragmentation challenge in the market from the implementation of different certification schemes. The adoption of the new certification scheme and costs related are key topics that need to be considered by the transportation sector in more detail to balance business operations and cybersecurity needs.

The research shows that cybersecurity certification certainly is not an easy process to implement; it is needed the definition of a cybersecurity policy to facilitate the implementation within the sector. For this purpose, it is required an active collaboration between the transportation organizations and ENISA to overcome the different challenges the sector faces and define the policy based on the sector needs. Once this policy is defined, the transportation organizations will see the benefits of implementing cybersecurity certification within their process, as this requires a high effort from the sector. A cybersecurity certification does not guarantee that a product, process or service is secure; however, it gives a certain level of assurance that every product, process or service meets certain requirements to prevent the occurrence of cybersecurity incidents that might negatively impact the transportation organization, moreover, the safety of people.

A direction for future research is to evaluate if defining a cybersecurity assurance level is suitable to the overall transportation sector. This topic research could be of interest as a cybersecurity assurance level may be forced through new regulations, for instance, a regulation that is applicable to the critical infrastructure and the transportation sector as a such may enforce it to obtain a cybersecurity certification of a higher level of assurance expected.

References

[1] O. S. L. C. a. N. F. O. Nykyforuk, «System of digital transformation indicators in the transport sector,» *European Journal of Intelligent Transportation Systems*, vol. 1, pp. 3-12, 2019.

[2] E. Commission, «A digital single market strategy for Europe,» EUR-Lex Access to European Union law, 2015.

[3] E. C. O. (ECS), «Transportation sector report. cyber security for road, rail, air, and sea. WG3 I Sectoral Demand,» European Cybersecurity Organization (ECS), 2020.

[4] E. A. E. Szary, «Polish airline, hit by cyber attack, says all carriers are at risk,» Reuters, 2015.

[5] B. Gupta, «Computer and cyber security: Principles, algorithm, applications, and perspectives,» 2018.

[6] S. Netzwelt, «450 Computer der bahn von "wannacry"-virus betroffen,» 05 2017. [En línea]. [Último acceso: 2021].

[7] A. Greenberg, «The untold story of not Petya, the most devastating cyberattack in history,» Wired, 2018.

[8] C. Cimpanu, «DDoS attacks cause train delays across Sweden,» Bleepingcomputer, 2017.

[9] M. Hill, «Danish railway company dsb suffers DDoS attack,» Info security magazine, 2018.

[10] M. Burgess, «Tfl kills the oyster website as customers are hit by a dumb hack,» Wired, 2019.

[11] Z. Kleinman, «Rail station wi-fi provider exposed traveller data,» BBC, 2020.

[12] S. R. Group, «Cyberattack against stadler IT network,» Stadler Rail Group Media release, 2020.

[13] D. Burroughs, «Internal documents published after Stadler refuses us 6m ransom,» *International Railway Journal*, 2020.

[14] I. España, «Adif, hit by ransomware,» Incibe-cert, 2020.

[15] H. Hamdouni., «The digital destruction: A case study of Stuxnet within the theory of new and old wars,» Swedish Defense University, 2017.

[16] ENISA, «ENISA threat landscape report 2020,» ENISA, 2020.

[17] M. Holloway, «Stuxnet worm attack on Iranian nuclear facilities,» Stanford University, 2015.

[18] M. Solutions, «Sheep dip your removable storage devices to reduce the threat of cyber attacks,» M.A.C. Solutions, 2017.

[19] P. R. M. Baezner, «Hotspot analysis: Stuxnet. Center for Security Studies (CSS),» ETH Zürich, 2017.

[20] E. Commission, «Network and information security directive (NIS),» European Union Agency for Cybersecurity (ENISA), 2021.

[21] S. a. May, «https://prodstoragesam.blob.core.windows.net/highq/2535266/new-cyber-security-law-what-does-the-nis-directive-mean-for-your-business.pdf,» 10 02 2016. [En línea]. Available: https://prodstoragesam.blob.core.windows.net/highq/2535266/new-cyber-security-law-what-does-the-nis-directive-mean-for-your-business.pdf. [Último acceso: 2021].

[22] E. Commission, «Concerning measures for a high common level of security of network and information systems across the union,» EEUR-Lex Access to European Union law, 2016.

[23] L. Kovács, «Cyber security policy and strategy in the european union (EU) and NATO,» *Land Forces Academy Review*, vol. I, pp. 16-24, 2018.

[24] J. O. G. Erbach, «Cybersecurity of critical energy infrastructure,» EPRS | European Parliamentary Research Service, 2019.

[25] ENISA, «Railway cybersecurity, security measures in the railway transport sector,» ENISA, 2020.

[26] M. E. D. (. D. C. LÉVY-BENCHETON, «Cyber security and resilience of intelligent public transport: Good practices and recommendations,» ENISA, 2015.

[27] B. H. N. Fazel Anjomshoa Burak Kantarci Tolga Soyata Hadi Habibzadeh, «A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities,» *Sustainable Cities and Society,* Vols. %1 de %2ISSN 2210- 6707, 2019.

[28] K. T. Kevin D. Jones, «Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping,» *Journal of Cyber Policy, Taylor Francis Journals*, vol. 3, pp. 147-164, 2018.

[29] W. S. a. M. A. Quamar Niyaz Farha Jahan, «Security modeling of autonomous systems: A survey.,» ACM Comput. Surv, 2019.

[30] P. a. B. H. Reason, «Handbook of Action Research,» Sage, London, p. 1, London, 2001.

[31] S. publishing, «What is Action Research?,» 03 09 2010. [En línea]. Available: https://www.sagepub.com/sites/default/files/upm-binaries/36584_01_Koshy_et_al_Ch_01.pdf. [Último acceso: 2021].

[32] B. R. Methodology, «Action Research,» [En línea]. Available: https://research-methodology.net/research-methods/action-research/. [Último acceso: 2021].

[33] E. Commission, «Resilience, deterrence and defence: Building strong cyber- security in europe,» EU Digital Single Market, 2017.

[34] E. Commission, «State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks,» 2017. [En línea]. Available: https://ec.europa.eu/commission/presscorner/detail/en/IP_17_3193. [Último acceso: 2021].

[35] ENISA, «NIS Directive,» 2018. [En línea]. Available: https://www.enisa.europa.eu/topics/nis-directive. [Último acceso: 2021].

[36] E. Commission, «The EU Cybersecurity Act,» 2019. [En línea]. Available: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act. [Último acceso: 2021].

[37] E. Commission, «New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient,» 2020. [En línea]. Available: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391. [Último acceso: 2021].

[38] T. T. E. Parliament, «The NIS2 Directive: A high common level of cybersecurity in the EU,» 2021. [En línea]. Available: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333. [Último acceso: 2021].

[39] Reuters, «Companies may face 2% fine for breaching EU cybersecurity rules,» 16 December 2020. [En línea]. Available: https://www.reuters.com/article/eu-cybersecurity-idUSKBN28Q1NS. [Último acceso: 2021].

[40] E. Commission, «The EU cybersecurity certification framework,» 2021. [En línea]. Available: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework. [Último acceso: 2021].

[41] ENISA, «Public Consultation on the draft Candidate EUCC Scheme,» 26 May 2021. [En línea]. Available: https://www.enisa.europa.eu/publications/enisa-report-public_consultation-on-the-draft-candidate-eucc-scheme. [Último acceso: 2021].

[42] ENISA, «EUCC scheme (Common Criteria based European candidate cybersecurity certification scheme),» *Cybersecurity Certification,* vol. V.1.1.1, nº https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme, p. 288, 2021.

[43] E. Commission, «EU Cybersecurity Act: The latest eu's legislation to advance cybersecurity across europe,» Digital Single Market, 2019.

[44] M. C. a. D. Oka, «Cybersecurity metrics for automotive systems,» *SAE Technical Paper 2021-01-0138,* 2021.

[45] G. F. C. M. C. M. M. a. D. S. Gianfranco Burzio, «Cybersecurity of connected autonomous vehicles : A ranking based approach,» *IEEE,* p. 1–6, 2018.

[46] S. N. M. a. A. S. Jose L. Hernandez-Ramos, «The challenges of software cybersecurity certification [building security in],» *IEEE Security Privacy,* vol. 19(1):99–1O2, 2021.

[47] J. L. H.-R. A. F. S. a. G.-. m. B. Sara N. Matheu-García, «Risk-based automated assessment and testing for the cybersecurity certification and labelling of IoT devices,» *Computer Standards Interfaces*, vol. 62, p. 64–83, 2019.

[48] C. B. a. M. Rojszczak, «Cybersecurity of consumer products against the background of the EU model of cyberspace protection,» *Journal of Cybersecurity*, vol. 7 (1), nº tyabO11, 2021.

[49] ENISA, «Sectoral Cybersecurity Assessment methodology (SCSA Methodology),» ENISA, 2021.

[50] E. Parliament, «Directive 2010/40/EU of the European Parliament,» 2010. [En línea]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2010.207.01.0001.01.ENG. [Último acceso: 2021].

[51] E. Parliament, «Decision (EU) 2017/2380 of the European Parliament,» 2017. [En línea]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017D2380&qid=1639480181298. [Último acceso: 2021].

[52] E. S. Online, «Implementation of Directive 2010/40/EU on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport,» European Sources Online, 08 10 2019. [En línea]. Available: https://www.europeansources.info/record/implementation-of-directive-2010-40-eu-on-the-framework-for-the-deployment-of-intelligent-transport-systems-in-the-field-of-road-transport-and-for-interfaces-with-other-modes-of-transport-2/. [Último acceso: 2021].

[53] E. Commission, «EUR-Lex: REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Implementation of Directive 2010/40/EU o,» 8 10 2019. [En línea]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0464&from=EN. [Último acceso: 2021].

[54] E. Monitor, «Explanatory Memorandum to COM(2017)477 - ENISA, the "EU Cybersecurity Agency", and Information and Communication Technology cybersecurity certification ("Cybersecurity Act"),» EU Monitor, 13 09 2017. [En línea]. Available: https://www.eumonitor.eu/9353000/1/j4nvhdfdk3hydzq_j9vvik7m1c3gyxp/vkhlg25kz0yg. [Último acceso: 2021].

[55] E. Parliament, «Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da,» EUR-Lex, 27 04 2016. [En línea]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj. [Último acceso: 2021].

[56] E. Parliament, «Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004,» EUR-Lex, 21 05 2013. [En línea]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013R0526&qid=1639481169606. [Último acceso: 2021].

[57] R. Teataja, «Cybersecurity Act,» 09 05 2018. [En línea]. Available: https://www.riigiteataja.ee/en/eli/523052018003/consolide. [Último acceso: 2021].

[58] M. o. E. a. I. Technology, «Requirements for risk analysis of network and information systems and description of security measures,» 10 07 2018. [En línea]. Available: https://www.ria.ee/sites/default/files/content-editors/KIIK/requirements-for-risk-analysis.pdf. [Último acceso: 2021].

[59] Légifrance, «Décret n° 2015-351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale,» 29 03 2015. [En línea]. Available: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000030405967/. [Último acceso: 2021].

[60] Légifrance, «LOI n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité,» 27 02 2018. [En línea]. Available: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000036644772/. [Último acceso: 2021].

[61] Légifrance, «Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique,» 25 05 2018. [En línea]. Available: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000036939971/. [Último acceso: 2021].

[62] B. -. B. f. S. i. d. Informationstechnik, «Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0),» 23 04 2021. [En línea]. Available:

https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html. [Último acceso: 2021].

[63] ETSI, «Intelligent Transport Systems (ITS); Security; Security Services and Architecture.,» 09 2010. [En línea]. Available: https://www.etsi.org/deliver/etsi_ts/102700_102799/102731/01.01.01_60/ts_102731v010101p.pdf. [Último acceso: 2021].

[64] ETSI, «Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA),» 03 2010. [En línea]. Available: https://www.etsi.org/deliver/etsi_tr/102800_102899/102893/01.01.01_60/tr_102893v010101p.pdf.

[65] ETSI, «Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management; Release 2,» 07 2021. [En línea]. Available: https://www.etsi.org/deliver/etsi_ts/102900_102999/102940/02.01.01_60/ts_102940v020101p.pdf. [Último acceso: 2021].

[66] ETSI, «Intelligent Transport Systems (ITS); Security; Trust and Privacy Management,» 01 2021. [En línea]. Available: https://www.etsi.org/deliver/etsi_ts/102900_102999/102941/01.04.01_60/ts_102941v010401p.pdf. [Último acceso: 2021].

[67] ETSI, «Intelligent Transport Systems (ITS); Security; Access Control,» 06 2012. [En línea]. Available: https://www.etsi.org/deliver/etsi_ts/102900_102999/102942/01.01.01_60/ts_102942v010101p.pdf. [Último acceso: 2021].

[68] ETSI, «Intelligent Transport Systems (ITS); Security; Confidentiality services,» 06 2012. [En línea]. Available: https://www.etsi.org/deliver/etsi_ts/102900_102999/102943/01.01.01_60/ts_102943v010101p.pdf. [Último acceso: 2021].

[69] ETSI, «Intelligent Transport Systems (ITS); Security; Security header and certificate formats; Release 2,» 10 2021. [En línea]. Available: https://www.etsi.org/deliver/etsi_ts/103000_103099/103097/02.01.01_60/ts_103097v020101p.pdf. [Último acceso: 2021].

[70] I. 21434:2021, «Road vehicles — Cybersecurity engineering,» 08 2021. [En línea]. Available: https://www.iso.org/standard/70918.html. [Último acceso: 2021].

[71] I. 21448:2019, «Road vehicles - Safety of the intended functionality,» [En línea]. Available: https://www.iso.org/standard/70939. html. [Último acceso: 2021].

[72] I. 26262., «Road Vehicles - Functional Safety,» [En línea]. Available: https://www.iso.org/standard/68383.html. [Último acceso: 2021].

[73] S. J3061, «Hardware Protected Security for Ground Vehicles,» [En línea]. Available: https://www.sae.org/standards/content/j3061_ 201601/. [Último acceso: 2021].

[74] S. J3101, «Hardware Protected Security for Ground Vehicles,» 10 02 2020. [En línea]. Available: https://www.sae.org/standards/content/j3101_202002/. [Último acceso: 2021].

[75] V.-Q. A. ACSMS, «Automotive Cybersecurity Management System Audit,» [En línea]. Available: https://vda-qmc.de/fileadmin/ redakteur/Publikationen/Gelbdrucke/VDA_Yellow_Volume_ACSMS_EN_1_ edition_2020.pdf. [Último acceso: 2021].

[76] BSIPAS1885:2018, «Thefundamentalprinciplesofautomotivecybersecurity,» 31 12 2018. [En línea]. Available: https://shop.bsigroup.com/products/the-fundamental-principles-of-automotive-cyber-security-specification/standard.

[77] B. P. 11281:2018, «Connectedautomotiveecosystems.Impactofsecurityonsafety.Codeofpractice,» 31 12 2018. [En línea]. Available: https://shop.bsigroup.com/products/the-fundamental-principles-of-automotive-cyber-security-specification/standard. [Último acceso: 2021].

[78] R. DO-326, «Airworthiness Security Process Specification,» 06 08 2014. [En línea]. Available: https://standards.globalspec.com/std/9869201/RTCA%20DO-326. [Último acceso: 2021].

[79] NERC, «Critical Infrastructure Protection Standards,» [En línea]. Available: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx. [Último acceso: 2021].

[80] BSI, «BSI-Standards,» 10 2017. [En línea]. Available: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/bsi-standards_node.html. [Último acceso: 2021].

[81] ETSI, «CYBER; Protection measures for ICT in the context of Critical Infrastructure,» 04 2016. [En línea]. Available: https://www.etsi.org/deliver/etsi_tr/103300_103399/103303/01.01.01_60/tr_103303v010101p.pdf. [Último acceso: 2021].

[82] BIMCO, «Cyber Security Workbook for On Board Ship Use, Second Edition,» 11 2020. [En línea]. Available: https://www.ics-shipping.org/publication/cyber-security-workbook-second-edition/. [Último acceso: 2021].

[83] BIMCO, «Industry Standard Software Maintenance of Shipboard Equipment,» 12 2017. [En línea]. Available: https://www.bimco.org/about-us-and-our-members/publications/industry-standard-software-maintenance-of-shipboard-equipment. [Último acceso: 2021].

[84] I. 15408-1:2009, «Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model,» 12 2009. [En línea]. Available: https://www.iso.org/standard/50341.html. [Último acceso: 2021].

[85] I. 27001:2013, «Information technology — Security techniques — Information security management systems — Requirements,» 10 2013. [En línea]. Available: https://www.iso.org/isoiec-27001-information-security.html. [Último acceso: 2021].

[86] I. 27002:2013, «Information technology — Security techniques — Code of practice for information security controls,» 10 2013. [En línea]. Available: https://www.iso.org/standard/54533.html. [Último acceso: 2021].

[87] ENISA, «Cyber Security and Resilience of Intelligent Public Transport,» ENISA, 2016.

[88] ENISA, «EU Cybersecurity Certification Framework - Publications,» [En línea]. Available: https://www.enisa.europa.eu/topics/standards/certification?tab=publications. [Último acceso: 2021].

[89] ENISA, «ICT security certification opportunities in the healthcare sector,» 31 01 2019. [En línea]. Available: https://www.enisa.europa.eu/publications/healthcare-certification. [Último acceso: 2021].

[90] ENISA, «Cybersecurity Certification: Candidate EUCC Scheme,» 07 2020. [En línea]. Available: https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme. [Último acceso: 2021].

[91] ENISA, «EUCS – Cloud Services Scheme,» 12 2020. [En línea]. Available: https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme. [Último acceso: 2021].

[92] jtsec, «ENISA publishes EUCC 1.1.1 the first European cybersecurity scheme for ICT products.,» 26 05 2021. [En línea]. Available: https://www.jtsec.es/blog-entry/92/enisa-publishes-eucc-111-the-first-european-cybersecurity-scheme-for-ict-products. [Último acceso: 2021].

[93] ENISA, «EU Cybersecurity Certification Framework - Stakeholders' Interactions,» [En línea]. Available: https://www.enisa.europa.eu/topics/standards/certification. [Último acceso: 2021].

[94] ENISA, «Public Consultation on the draft Candidate EUCC Scheme,» 26 05 2021. [En línea]. Available: https://www.enisa.europa.eu/publications/enisa-report-public_consultation-on-the-draft-candidate-eucc-scheme. [Último acceso: 2021].

[95] D. B. F. C. C. M. Paolo Crisafulli, «Engineering Railway Systems with an Architecture-Centric Process Supported by AADL and ALISA: an Experience Report,» 01 2020. [En línea]. Available: https://hal.archives-ouvertes.fr/hal-02454258/document. [Último acceso: 2021].

[96] E. Commission, «ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act),» de *REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019*, EEUR-Lex Access to European Union law, 2019, pp. 55, Article 2, definition 12.

[97] E. Commission, «ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act),» *REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019*, pp. 55, Article 8, number 1, 2019.

[98] ANSSI, «Certification de Sécurité de Premier Niveau (CSPN),» [En línea]. Available: https://www.ssi.gouv.fr/administration/produits- certifies/cspn/les-procedures-formulaires-et-methodologies. [Último acceso: 2021].

[99] NCSC, «Commercial Product Assurance (CPA),» [En línea]. Available: https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa. [Último acceso: 2021].

[100] S. o. t. S.-I. Signatories of the CCRA, «Common Criteria,» [En línea]. Available: ¨https://www.commoncriteriaportal.org, ¨https://www.sogis.org". [Último acceso: 2021].

[101] EuroPriSe, «European Privacy Seal,» [En línea]. Available: https://www.european-privacy-seal.eu/EPS- en/Home. [Último acceso: 2021].

[102] C. Singapore, «National IT Evaluation Scheme (NITES),» [En línea]. Available: https://www.csa.gov.sg/. [Último acceso: 2021].

[103] S. I. Group, «Software Improvement Group (SIG) Software Quality Model for Security,» [En línea]. Available: https://www.sig.eu/insight/practical-model-rating- software-security. [Último acceso: 2021].

[104] UL, «UL Cybersecurity Assurance Program (UL 2900-1 / 2),» [En línea]. Available: http://www.ul.com/cybersecurity/. [Último acceso: 2021].

[105] U. L. f. D. Schleswig-Holstein, «ULD Datenschutz-Gütesiegel,» [En línea]. Available: https://www.datenschutzzentrum.de/guetesiegel/ (German only). [Último acceso: 2021].

[106] I. 62433, «Security for Industrial Automation and Control Systems,» [En línea]. Available: https://webstore.iec.ch/searchform&q=62443 http://www.isasecure.org/en-US/. [Último acceso: 2021].

[107] JRC, «IACS Cybersecurity Certification Framework,» [En línea]. Available: https://erncip-project.jrc.ec.europa.eu/networks/tgs/european-iacs. [Último acceso: 2021].

[108] G. a. 3GPP, «GSMA Network Equipment Security Assurance Scheme,» [En línea]. Available: http://www.3gpp.org/news-events/3gpp-news/1569-secam_for_3gpp_nodes. [Último acceso: 2021].

[109] OWASP, «OWASP Application Security Verification Standard (including OWASP Top Ten),» [En línea]. Available: https://www.owasp.org/index.php/Top_10_2013. [Último acceso: 2021].

[110] OWASP, «OWASP Testing Guide,» [En línea]. Available: https://www.owasp.org/index.php/Category:OWASP_Testing_Project. [Último acceso: 2021].

[111] I. Labs, «IoT Security Testing Framework,» [En línea]. Available: https://www.icsalabs.com/technology-program/iot-testing. [Último acceso: 2021].

[112] NXP, «MIFARE Security Certification,» [En línea]. Available: https://www.mifare.net/en/about-mifare/certification/. [Último acceso: 2021].

[113] I. 19792, «Security evaluation of biometrics,» [En línea]. Available: https://www.iso.org/standard/51521.html. [Último acceso: 2021].

[114] ENISA, «Consultation on the draft of the candidate Certification Scheme on Cloud Services (EUCS),» 07 02 2021. [En línea]. Available: https://www.enisa.europa.eu/topics/standards/certification/public-consultation-on-cybersecurity-schemes/draf-eucs. [Último acceso: 2021].

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I Diana Carolina Burbano Valencia

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis ´EU Cybersecurity Certification: Case Study Analysis For Implementation in the transportation sector in the EU´, supervised by Andrew J. Roberts
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

14.12.2021

1 The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.