Universidad Internacional de La Rioja
Escuela Superior de Ingeniería y Tecnología

Master's Degree in Cybersecurity

Protecting Onboard Industrial Control Systems: A Hybrid Cybersecurity Approach

Master's thesis presented by:	Francisco J. Daza Pastrana
Work type:	Research and Methodology
Director:	María Yoldi Sangüesa
Date:	July 9, 2024

Abstract

In the context of Onboard Industrial Control Systems (OICS) in the Transport sector, cybersecurity standards lack specificities for offline connectivity periods. This master thesis addresses these challenges highlighting the need for a hybrid design of centralized landside support security system (LSSS) for security and fleet management. Using the IEC 62443 framework, we identified factors impacting Security Level Target (SL-T) estimation, such as evolving threat actor landscapes and physical protection. We analyzed the mandatory and recommended IEC 62443 requirements for integrating LSSS functions and opened discussions for reducing the SL-C of critical OICS requirements and the role of nation-state backed threat actors. Our approach incorporates NIST SP 800-53 controls and other technological references, offering implementation guidance. The proposed hybrid design significantly reduced maintenance costs by 2.5 times while maintaining security robustness, enhancing both cybersecurity and maintainability for transportation sector fleets.

Keywords: Industrial Control Systems (ICS), Cybersecurity, Onboard, IEC 62443, Transportation

Resumen

En el contexto de “Sistemas de Control Industrial a Bordo” (OICS) en el sector del transporte, las normas de ciberseguridad carecen de especificidad para sus períodos sin conexión. Esta tesis aborda estos desafíos subrayando la necesidad de un diseño híbrido de Servicios de Soporte Compartido en Tierra (LSSS) para la gestión centralizada de la seguridad y flotas. Basados en el marco de la norma IEC 62443, identificamos factores que afectan la estimación del “Nivel Seguridad Objetivo” (SL-T), como la protección física. Analizamos los requisitos obligatorios y recomendados del IEC 62443 para integrar funciones LSSS y discutimos la reducción del SL-C de requisitos críticos, así como el rol de actores de amenazas apoyados por gobiernos. Nuestro enfoque incorpora controles de NIST SP 800-53 y otras referencias tecnológicas para su implementación. Este diseño híbrido, reduce en 2.5 veces los costos de mantenimiento, preservando la ciber resiliencia y facilitando la gestión del sector.

Palabras clave: Sistemas de Control Industrial (ICS), Ciberseguridad, a Bordo, IEC 62443, Transporte

Acknowledgments

I would like to thank my ALSTOM colleagues for providing me with useful information and mentoring me through all these years. Also, to my promoter for her support and keen guidance. Finally, this thesis could not have been possible without the full encouragement of my whole family.

Waterloo, Belgium. July 2024
Francisco José Daza Pastrana

Table of Contents

List of Figures

List of Tables

List of Acronyms and Abbreviations

CSIRT	Computer Security Incident Response Team(s)
COTS	Component Off The Shelf
DoS	Denial-of-Service
DPO	Data Protection Officer
ENISA	European Union Agency for Cybersecurity
ERA	European Railway Agency
EUROCAE	European Organization for Civil Aviation Equipment
GNSS	Global Navigation Satellite System
GoA3/4	Grade-of-Automation 3/4
GPS	Global Positioning System
HSE	Health, Safety and Environment
IACS	Industrial Automation and Control System(s) (IEC 62443 context)
IACS	International Association of Classification Societies (Maritime context)
IATA	International Air Transport Association
ICAO	International Civil Aviation Organization
ICS	Industrial Control System(s)
IEC	International Electrotechnical Commission
IIoT	Industrial Internet of Things
IMO	International Maritime Organization
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization
IT	Information Technology
ISA	International Society of Automation
LSSS	Landside Support Security System(s)

NHTSA	National Highway Traffic Safety Administration
NIST	National Institute of Standards and Technology
NTS	Network Time Security
OEM	Original Equipment Manufacturer
OICS	Onboard ICS(s)
OT	Operational Technology
PKI	Public-Key Infrastructure
RAMS	Reliability, Availability, Maintainability and Safety
RTCA	Radio Technical Commission for Aeronautics
SCADA	Supervisory Control And Data Acquisition
SIEM	Security Information and Event Management
SL	Security Level (from IEC 62443 standard)
SL-C	SL-Capability
SL-T	SL-Target
SOC	Security Operations Center
UAV	Unmanned Aerial Vehicle
UNECE	United Nations Economic Commission for Europe
UR	Unified Requirements
UTC	Coordinated Universal Time
UTO	Unattended Train Operation
WAN	Wide Area Network
ZTA	Zero-Trust Architecture

1. Introduction

1.1. Motivation

Warren Buffet said that cybersecurity is bigger threat to mankind than nuclear weapons, as "If [a nuclear attack] ever happens, there'll be more to worry about than the price of Berkshire"[1]. Indeed, the number of cybersecurity incidents continue growing year-to-year, and when speaking of Critical-Infrastructures and Industrial Control Systems (ICS), these reached values never expected years ago [2].

In the last two decades, industry sector associations have been developing and adapting specific ICS standards like IEC 62443 [3]. Governments and councils, such as the European Parliament, are also standardizing cybersecurity among EU manufacturers, suppliers, system integrators, and asset owners with the creation of the NIS2 Directive [4]. Additionally, the upcoming Cyber Resilience Act (CRA) is expected to impact any organization selling "[…] products with digital elements […]" by mandating a series of minimum requirements [5].

Most Critical Infrastructure sectors follow IEC 62443 as the reference ICS cybersecurity standard (refer to chapter 2.3). The integration of common communication protocols and COTS components into ICS is attracting threat actors due to the high benefit-to-effort ratio (refer to chapters 2.4 and 4.2.1) [2] . This has led to the widespread adoption of higher IEC 62443 Security Levels (SLs) as the new minimum to protect from attackers "[…] using sophisticated means with moderate resources, IACS specific skills, and moderate motivation" [7]. Additionally, these higher IEC 62443 SLs require the integration of services typically found on the Information Technology (IT) with the Operational Technology (OT) world to provide flexibility and cost reductions for centralized monitoring and management of OT assets. However, there is little discussion on the balance between cybersecurity and maintainability caused by unreachable or spoofed remote centralized support services during offline periods typical of the Onboard ICS (OICS) operational context.

Thus, there is a need to study this compromise within the framework of international cybersecurity standards. This study will define the basis for a hybrid and more cyber-resilient approach to OICS development when integrating Landside Support Security Systems (LSSS) for centralized and remote management of an entire fleet of OICS at the required SL.

1.2. Scope

This master thesis focuses on Onboard ICS from Transportation sector. While space vehicles, military drones and other “vehicles” may certainly fall in the definition of an “Onboard ICS”, the cybersecurity aspects considered in this work will focus on references from the transportation sector. Nonetheless, the outcomes observed may apply as well to the aforementioned ICS, but these deserve an independent work and certainly different security level and threat actor’s hypothesis.

It is not in the scope of this work the requirements to protect at network or host level the LSSS itself in the landside local network, as extended guidance exists on this matter. Instead, the focus is given to the design choices required to create a cyber-resilient integration between Landside Support Security Systems and Onboard ICS.

1.3. Problem statement

Unlike the Pharmaceutical, Food and Beverage, Nuclear, Wastewater, or Oil and Gas sectors, some Onboard ICS assets lack continuous connectivity, not facilitating event monitoring and up-to-date administration of security functions as required by certain requirements of IEC 62443. These assets may operate in a "degraded" mode for days or weeks (e.g., a train in the desert unable to update the authenticators database). Specific considerations are needed to preserve the required security level when no connection is available in a maintainable way. This master thesis aims to:

- Analyze the status of international standards addressing this issue.
- List recommended LSSS assets for a sector-agnostic architecture of Onboard ICS.
- Identify specific Onboard ICS threats from loss of connectivity or spoofing of air-gap data links (e.g., GNSS or SIEM) and their potential impact.
- Provide recommended cybersecurity requirements and mechanisms for a hybrid approach based, when possible, in a Zero-Trust Architecture (ZTA) to protect Onboard ICS assets during and after connectivity is lacking.
- Evaluate the potential benefits of applying a hybrid ICS cybersecurity design approach to current Onboard ICS organizations.

1.4.Structure of the thesis

This thesis is structured in five chapters.

- Chapter 1, *Introduction*: the current chapter presents the topic and its structure.
- Chapter 2, *State of the art*: introduces to the reader background information on ICS (OT) / IT cybersecurity and an overview of current applicative cybersecurity standards and normative in Transportation sector with special emphasis highlighting Onboard ICS considerations.
- Chapter 3, *Study Objectives*: presents the overall and the specific objectives of the proposed research work.
- Chapter 4, *Methodology*: outlines the steps to achieve cyber resilience, maintainable and centralized management of Onboard ICS by applying a hybrid system design approach. Also, evaluates the potential benefits of the proposed methodology.
- Chapter 5, *Conclusions and Future Work*: presents the conclusions of this master thesis research and suggests further directions for future work

2. State of the art

This chapter presents the differences between Information Technology (IT) and Operational Technology (OT), the uniqueness of Onboard ICS, and a survey of the latest applicable cybersecurity standards and guidelines for Transportation ICS systems by sector, along with related threats.

2.1.Cybersecurity of Industrial Control Systems

2.1.1. IT versus OT cybersecurity

The National Institute of Standard and Technology (NIST) defines OT as "Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment)". These systems or devices detect or cause a direct change through the monitoring or control of devices, processes, and events. […]"[9](p.22).

Curiously, and useful later in the context of chapter 2.1.3, the International Association of Classification Societies (IACS) defines "OT", in their onboard systems (sea vessel) cyber resilience guidelines context as "Devices, sensors, software and associated networking that monitor and control onboard systems. Operational technology systems may be thought of as focusing on the use of data to control or monitor physical processes." [31][32][33].

In Figure 1, some of the typical OT assets and operational workflow of most of ICS system is illustrated.

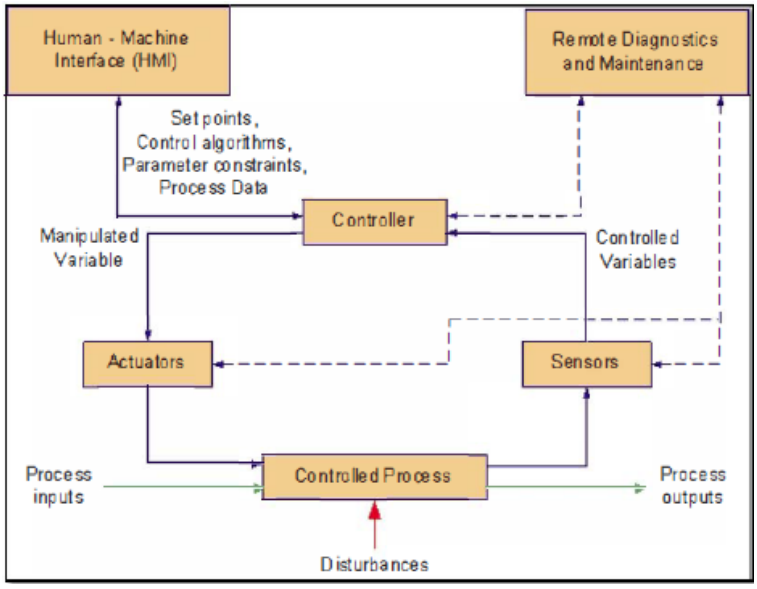

Figure 1 - Common ICS operation workflow. NIST [8] (p.6).

In particular with OT cybersecurity, it is also important to make the difference with traditional IT. Only considering the *CIA triad* (*Confidentiality*, *Integrity* and *Availability*) that since 1998 globally summarizes the principal cybersecurity attributes in digital assets [12], the priorities change greatly between IT and OT contexts. On the one hand, IT systems put most emphasis on protecting a loss on the *Confidentiality* related to the information system, which can lead to financial and data privacy consequences. On the other hand, OT interest is to ensure that both integrity and availability of cyber-physical devices operates in a safe manner to avoid a human-safety or environmental impact, thus considering confidentiality as a secondary issue (see Figure 2).

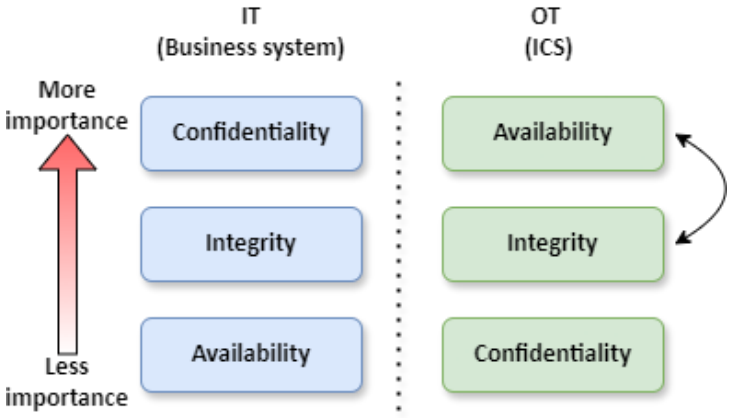

Figure 2 – Comparison of importance of Cybersecurity properties in IT and OT systems.

IT and OT differ much more than just in the “cyber-triad” (CIA). A good summary of these differences is given by the American Public Transportation Association (APTA) in Figure 3.

SECURITY TOPIC	INFORMATION TECHNOLOGY (IT)	CONTROL SYSTEMS (ICS)
Antivirus and Mobile Code	Very common; easily deployed and updated	Can be very difficult due to impact on ICS; legacy systems cannot be fixed
Patch Management	Easily defined; enterprise wide remote and automated	Very long runway to successful patch install; OEM specific; may impact performance
Technology Support Lifetime (Outsourcing)	2-3 years; multiple vendors; ubiquitous upgrades	10-20 years; same vendor
Cyber security Testing and Audit (Methods)	Use modern methods	Testing has to be tuned to system; modern methods inappropriate for ICS; fragile equipment breaks
Change Management	Regular and scheduled; aligned with minimum-use periods	Strategic scheduling; non trivial process due to impact
Asset Classification	Common practice and done annually; results drive cyber security expenditure	Only performed when obligated; critical asset protection associated with budget costs
Incident Response and Forensics	Easily developed and deployed; some regulatory requirements; embedded in technology	Uncommon beyond system resumption activities; no forensics beyond event re-creation
Physical and Environmental Security	Poor (office systems) to excellent (critical operations systems)	Excellent (operations centers; guards, gates, guns)
Secure Systems Development	Integral part of development process	Usually not an integral part of systems development
Security Compliance	Limited regulatory oversight	Specific regulatory guidance (some sectors)

Figure 3 - Comparison between Enterprise IT and OT (ICS) systems per cybersecurity topic. APTA [10] (p.15).

2.1.2. Safety is not Security

Safety and *Security* are two separate terms often misused since electronic computer and *networking* started to be digitally trespassed. While safety mechanisms and procedures protect from unintentional hazards (for example, hardware failures or human errors), the term *Security* went beyond of just "physical security" and covers the defense against intentional hazards (attacks) both originated by outsiders (external persons to an organization) and insiders. In addition, it can be often confused when speaking of secure (as synonym of *safe*) operations in OT environments, and this is can be worse in languages where the difference is less obvious (for example, in Spanish, both *safety* and *security* uses the same word: *seguridad*) [30].

If we look for a formal definition of Safety and (cyber)Security, the *de facto* standard for OT cybersecurity, IEC 62443, defines *Safety* as "The process to determine the required

protection factor for a safety system, while complex, is manageable since the probability of a component or system failure due to random hardware failures can be measured in quantitative terms. The overall risk can be calculated based on the consequences that those failures could potentially have on HSE [Human]" [7](p.67). Then, the standard compares it to *Security* as "Security systems are still meant to protect HSE, but they are also meant to protect the industrial process itself, company-proprietary information, public confidence and national security among other things in situations where random hardware failures may not be the root cause" [3](p.7).

2.1.3. IT and OT standards difference

Another important difference between IT and OT is regarding the standards and norms applicable to one another. While non ICS-specific standards like NIST CSF [14] or ISO/IEC 27001 [15] are largely used by organizations in both environments for generic cybersecurity implementation, OT actors and regulators have already identified IEC 62443 [3] (formerly ISA99) standard framework as the *de facto* ICS standard and a solid base for developing sector-specific standards on ICS / OT / Critical-infrastructure cybersecurity [6][10][11][13][20] (a more detailed survey on applicable ICS cybersecurity references per sector is given in chapter 2.3). Figure 4 shows the scope between IT and OT main cybersecurity standards.

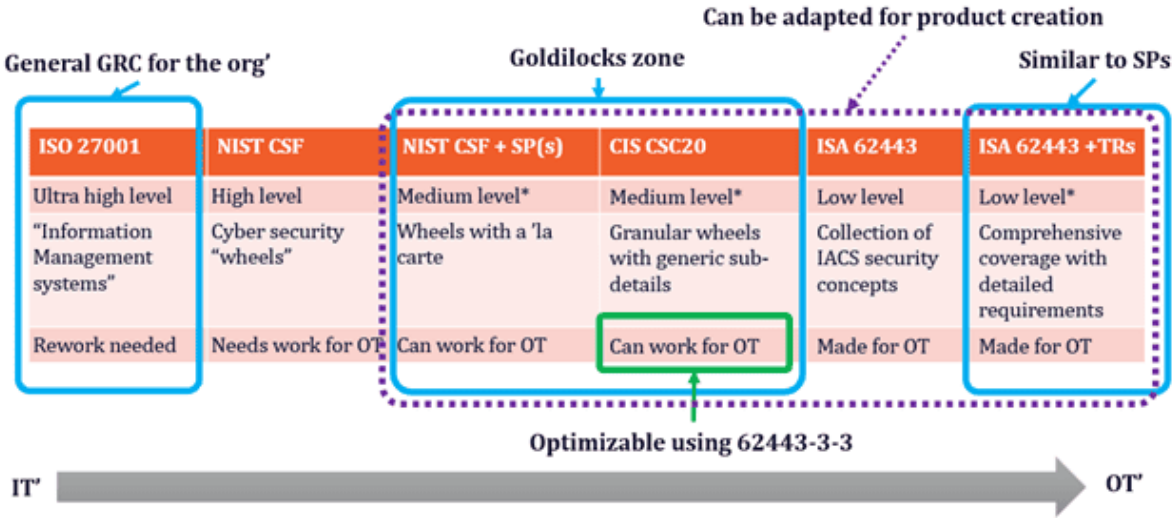

Figure 4 - Comparing main cybersecurity standards and guidance between IT and OT. Verve [13].

2.2. The Onboard ICS uniqueness in OT cybersecurity

2.2.1. Definition of Onboard ICS (OICS)

In this chapter, we will describe the concept of "Onboard ICS" (OICS) that will be used across this master thesis.

First, in a simple way, OICS could be defined as those industrial control systems installed and operated in autonomous (isolated) moving vehicles, vessels or planes. This is opposed to classical IT assets and "stationary ICS" found on Nuclear, Wastewater, Food, Chemical or Pharmaceutical ICS infrastructures. While stationary ICS are commonly located inside of the same geographical location in the form of "production plants" or in different locations that are interconnected thanks to fixed network infrastructure (WAN), most common examples of OICS are the ones included in road (bus, cars or trucks mainly), aviation (civil transport or cargo aircrafts), railway (passengers, freight or maintenance rolling stock) and maritime vessels (passenger, general cargo or fishing mainly). In other words, all those ICS included in vehicles commonly found in the Transportation sector, where many civilian lives depend on their safe operation. Please note that, as mentioned in chapter 1.2, aerospace (spacecrafts), military (aircrafts) or other non-common Transportation sector vehicles are not considered in this study).

Now, if we look for a formal definition of the concept of "Onboard industrial control systems" or "Onboard OT assets", the maritime International Association of Classification Societies (IACS) in their cyber resilience UR references mentions "Onboard ICS" and "Onboard OT" when defining "Computer Based System" (CBS) included in vessels (onboard vehicle). IACS considers a CBS as "[…] a combination of subsystems connected via network. […] connected directly or via public means of communications (e.g. Internet) to ashore CBSs, other vessels' CBS and/or other facilities." [31][32][33]. Particularly, it is worth noting that IACS UR E26 also defines "Operational Technology (OT) systems onboard ships, i.e. those CBSs using data to control or monitor physical processes that can be vulnerable to cyber incidents and, if compromised, could lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment" [32].

To simplify the reading during this work, please mind the fact that it will be used "OICS" to refer to all safety-critical assets onboard a same road vehicle, vessel, railway rolling stock

(as trains, metros or tramways) or civil aviation aircraft. For instance, when reading “fleet of OICS vehicles”, it refers to a fleet of road vehicles, vessels, railway or planes, except if specified otherwise.

2.2.2. OICS cybersecurity homologation

OICS integrates, in a same “vehicle” (road vehicle, vessel, train or plane), several safety-critical functions with the general exception of “trains” that can be attached several at the same time. Such safety functions need homologations to officially certify that a system reaches the requested safety (integrity) levels for commercial operation, providing insurance to transport people or dangerous goods, in a safe manner. As an example, at European level, there are regulations enforcing safety homologations per sector [35][36][37][38], but it is also common that countries and main industry-sector associations as NHTSA [44], IATA [39], ERA [40] or IMO[41] establish their own safety standards to be approved by certification bodies. Furthermore, needed certifications for safe operation have a great cost and efforts from manufacturers and thus are not done with frequency, making hard for them to adapt to the constant evolution of cybersecurity threats and vulnerabilities when speaking of Patch Management, as correctly reminds Hasratyan et al.: “While deploying a safety patch once every 5 years would seem exaggerated, deploying a security patch every 5 days is the minimal cyber hygiene.” [11](p. 36).

Regarding cybersecurity homologation of OICS, just one out of four Transportation sectors in our scope do not impose (yet) cybersecurity certification to operate when developing their products. The exception is Railways, which rather adds a new chapter (6.4) merely requesting to manage cybersecurity risks as part of the safety demonstration (Safety Case), but no real enforcement or guidance to comply with is given [87]. Aviation and Maritime sector, which needs to certify their products in compliancy with cybersecurity development. For example, In Maritime, IACS UR E26 and E27 [32][33] standards requires that new vessels from July 2024 have OICS like the propulsion, steering or anchoring and mooring functions developed at product level ensuring at least a “Security Profile 1” (corresponding to IEC 62443 SL1 [7]). In Aviation, the chapter 2.2 “Cyber Security Posture Upon Delivery” of the “Aviation Cyber Security Guidance Material – Part 2” (applicable to aircrafts) states that “Upon entry into service of a new e-connected aircraft, the airworthiness certificate should cover the cyber security elements which may impact safety. The latest version of the ED-202A/DO-326A

(Airworthiness Security Process Specification) [57][58] and ED-203A/DO-356A (Airworthiness Security Methods and Considerations) [59][60] cover these requirements for the OEMs/Suppliers and the DAHs [Design Approval Holders].” [56](p. 8).

Upcoming new regulations as CRA will impose requirements impacting the frequency in which assets need to be patched/updated and potentially homologated again. See 2.3.6.2.

2.2.3. OICS operational context

To differentiate OICS from classical stationary ICS, it is worth mention the description from NIST when describing that a Safety Instrumented System (SIS) “Historically […] was designed to be stand-alone, physically and logically separated, and airgapped from the rest of the control system.”. This description is interesting to contextualize the contrasting nature of OICS as, first, they do not depend on a fixed infrastructure, despite the fact that trains go along a rail or that road vehicles normally stay on a road infrastructure, and second, they need a wireless connection to have situational awareness respect to the ground and other OICS. In OICS architectures, there is not always a permanent and reliable network connection to support the management and monitoring of safety (or cyber) functions. In fact, it is common to have OICS going to geographical locations in which they can be isolated for several days or weeks for reasons like absence of wireless network to contact remote services, bad weather conditions affecting systems like GNSS, or intentional jamming of wireless signals.

Due to the high number of OICS to manage, is convenient to integrate them to a centralized system not just for greater security but also to ease its management (maintainability). In addition, offline periods impede OICS from reporting their security status like position, user database freshness, certificate expiration or intrusion alerts in a timely manner, resulting in degradation of the security capabilities of the OICS. Actually, an attacker may jam the communication to make the OICS fall to “offline/degraded mode”. Examples of issues in OICS implementing security mechanisms, without considering non-connected periods, would include (sample):

- A user login/password from a former employee that has not been removed allowing its access. This is particularly important in the operational context of a fleet, where access to onboard systems is allowed to multiple stakeholders (suppliers, contractors, and manufacturer) and they all have good knowledge of the system.

- Not buffering the security events and logs of a detected intrusion attempt to send it as soon as connectivity is back to the centralized log collector/SIEM in order to be analyzed by the SOC operator,
- A maintenance blockage due to time-dependent authentication mechanisms like an expired certificate because UTC time has been spoofed. [104].

These examples of threat events expose serious opportunity for threat actors targeting Critical Infrastructure / OT assets like Criminal Organizations (often backed by Nation-state actors; refer to chapter 4.2.1 and Annex A), corresponding to IEC 62443 SL 3 or SL 4 [7](pp. 72-73). In addition, v [28] (see Figure 5) is the case of any OT HSE impact, thus OICS can be classified as High-Value Asset as defined by NIST [9](p. 63), which falls in needing to protect from threat actors willing to harm to the nation [73] (p. H-2) like Criminal organizations backed by Nation organizations in certain countries.

Category	High Impact	Moderate Impact	Low Impact
Outage at multiple Sites	Significant disruption to operations at multiple sites with restoration expected to require one or more days	Operational disruptions at multiple sites with restoration expected to require more than one hour	Partially disrupted operations at multiple sites with restoration to full capability requiring less than one hour
National infrastructure and services	Impacts multiple sectors or disrupts community services in a major way	Potential to impact sector at a level beyond the company	Little to no impact to sectors beyond the individual company and little to no impact on community
Cost (% of revenue)	> 25 %	> 5 %	< 5 %
Legal	Felony criminal offense or compliance violation that affects the license to operate	Misdemeanor criminal offense or compliance violation that results in fines	None
Public confidence	Loss of brand image	Loss of customer confidence	None
People on-site	Fatality	Loss of workday or major injury	First aid or recordable injury
People off-site	Fatality or major community incident	Complaints or local community impact	No complaints
Environment	Citation by regional agency or long-term significant damage over large area	Citation by local agency	Small, contained release below reportable limits

Figure 5 - Possible definition of OT impact levels. NIST [28](p.49).

To conclude with this section, it is important to summarize the following key points:

- OICS are assets being part of a “moving critical infrastructure” fleet (normally hundreds of vehicles, boats and planes), owned and/or managed by a same organization.
- OICS are continuously spread through different geographical locations to turn a profit on the fleet.
- In most of OICS transport operations (exception to some particular operations like Urban rail) is common to have offline periods losing connectivity with centralized supporting systems during several days or weeks, meaning there is no real-time situational awareness or remote centralized maintenance and monitoring security functions.

Cybersecurity resilience, management and operation of an OICS fleet is directly impacted by the presented operational context and thus stands as a main pillar of this thesis.

2.2.3.1. Security versus Maintainability of OICS

As reviewed above, current cybersecurity standards like IEC 62443 and industry-specific guidelines are missing a systematic approach to manage the distributed OICS context (see above). While a simple solution could be done by imposing to fleet operators heavy maintenance procedures to frequently go to each OICS and thorough schedules to keep cybersecurity parameters updated, this increases largely the maintenance costs when speaking to maintain a fleet of hundreds or thousands of OICS (see Table 1 for an estimation of fleet size per organization in the transport sector).

Some examples related to Security and Maintainability dilemma could be the following:

- A system designed to be **locally managed** has an **obsolete authenticator database not granting a new trusted user** connection to the OICS to perform some mandatory maintenance. This also allows another **disgruntled** and currently **formerly trusted user** to access because its credentials are **still in the outdated authenticator database**. The authenticator database is updated only locally.
- A system designed to be **locally managed** has **outdated PKI-based authenticators** like Certificate Revocation List (CRL) in the system granting access to a **currently revoked** certificate **recognized as valid**. The PKI-based authenticators like CRL are updated only locally.

- A system designed to be **locally managed** detects a **security incident that is not reported** to the SOC and continues to **operate in a compromised condition** until a trusted user **retrieves the logs locally**. The retrieving of logs is performed locally as normal operation.
- A **system detects a security incident** while the attacker was **jamming** the **wireless** connection to the **MONITORING LSSS**. The system does **not buffer nor track** what **events** or logs have been received by the LSSS function and the s**ecurity incident is not reported** to the SOC, allowing to continue **operate in a compromised condition** until a trusted user retrieves the logs locally.

2.2.4. Landside Support Security Systems (LSSS)

As introduced in chapter 1.1, in this study it will be used the term “LSSS” to refer to systems in the ground supporting OICS cybersecurity functions used both to increase the security awareness and to ease the management of a fleet of OICS.

LSSS are typically situated in physically protected zones of the organization such as control centers or hub offices and operate at least as low as "Level 3" of the Purdue reference model [42] communicating with OICS via a wireless interface. In various industry sectors, this communication may occur over dedicated industry wireless networks, like GSM-R in railway infrastructures, or through public networks like in road vehicles context, but the latter increases the risk of attacks due to its increased exposition.

In Figure 5, Yu et al. [43](p. 8). illustrates the gap between Purdue Level 3 [42], corresponding to "Operation Management – ATS/CTC" (Automatic Train Supervision / Centralized Traffic Control), and the actual OICS at Purdue Level 0, corresponding to "Process Control – Train". While this example is specific to Communications-Based Train Control (CBTC) in the railway sector, a similar air gap between OICS and LSSS can be found in other transportation sectors.

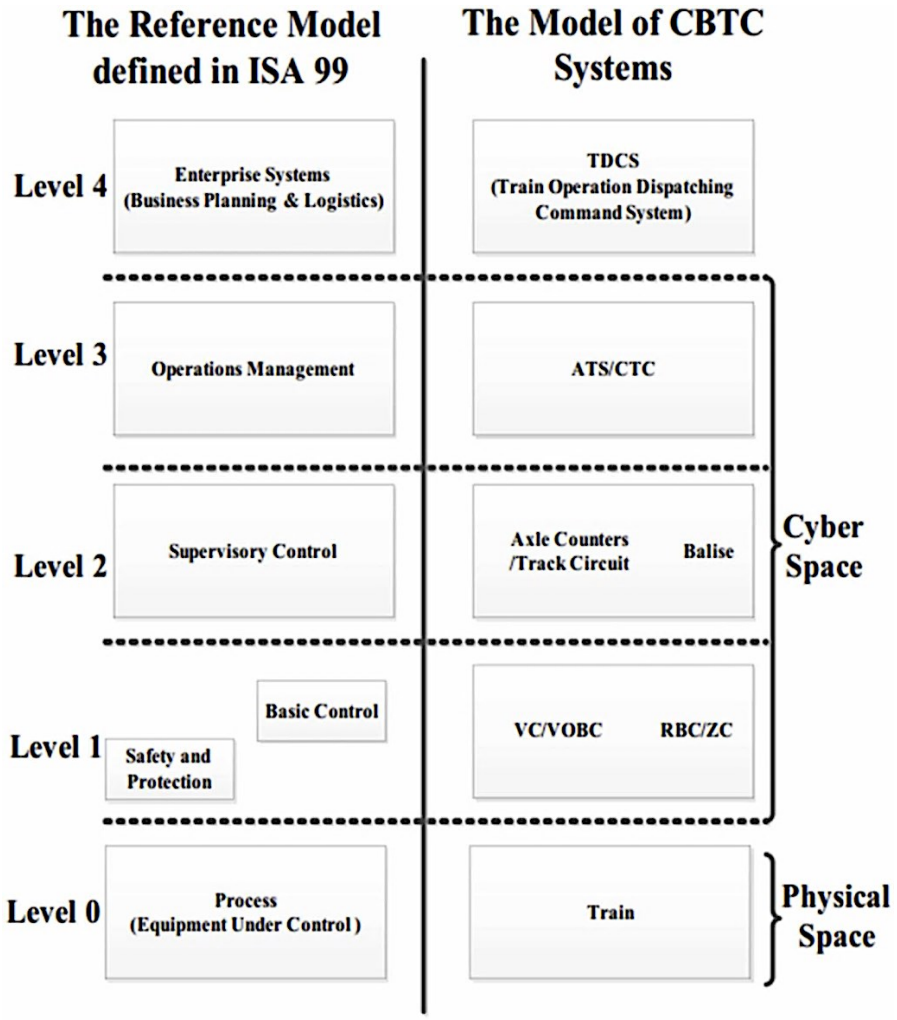

Figure 6 – Purdue reference model adaptation to Railway. Yu et al. [43](p. 8).

Applying this to an OICS cybersecurity architecture, an example of LSSS integration in OICS environment is given by EU project X2RAIL-3 [67], where a list of "Onboard Security Services" needed to support IEC 62443-3-3 [7]and 4-2 [70] required security functions are proposed. These services can be located with the *red arrows* in the railway generic cybersecurity architecture depicted in Figure 7. While X2RAIL-3 architecture shows "Onboard Security Services" as a separated zone, this could be part of the ICS itself (corresponding to the "Signalling Zone" in Figure 7).

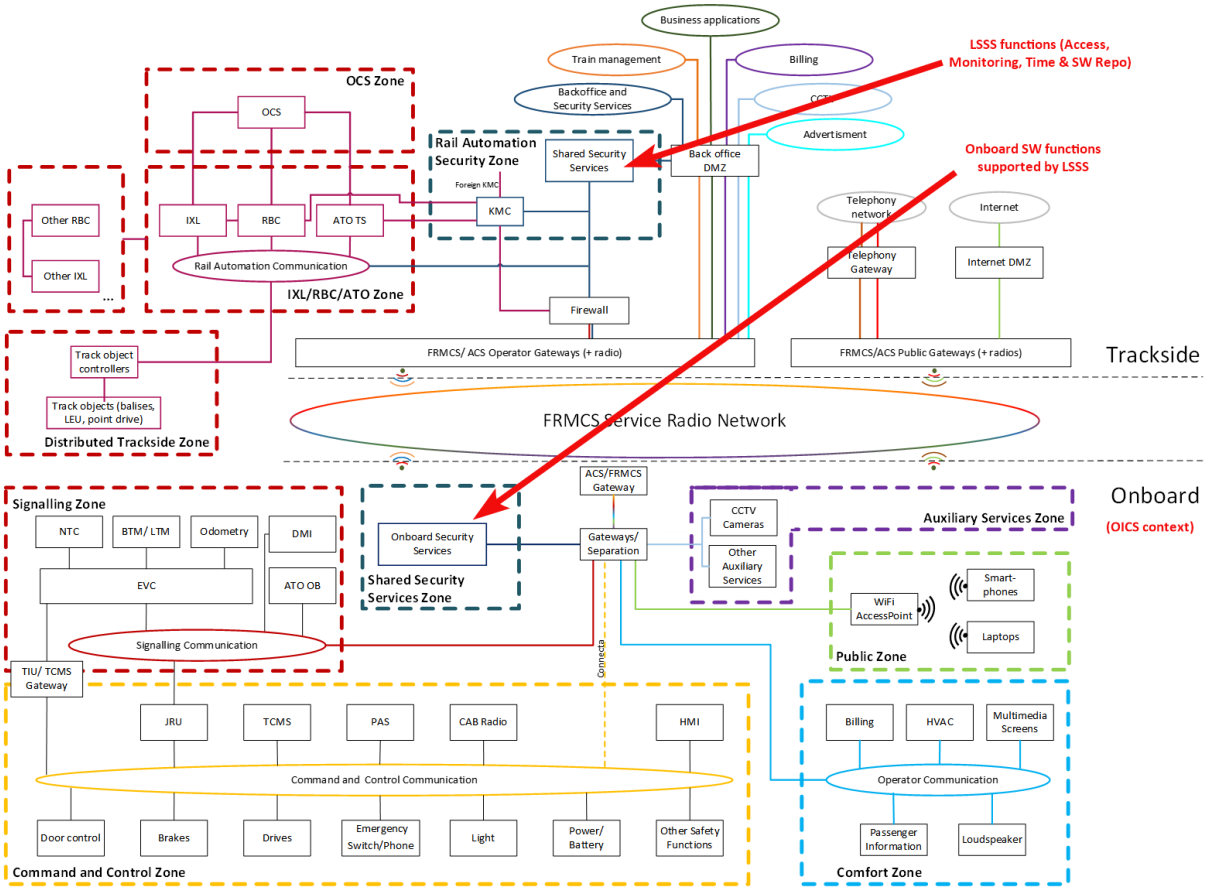

Figure 7 - Location of LSSS in a Railway generic cybersecurity architecture. X2RAIL-3. [67](p. 11).

While the list of supporting services composing a LSSS zone of any Transport system may vary between sectors, when organizations follow common international standards to implement basic security functions like those requested by IEC 62443-3-3 SL-C = 1 [7] or NIST 800-82/160 [28][9], the need for integrating LSSS in their solutions becomes evident not just for a cybersecurity purpose, but also when asset management is considered for a whole fleet of OT systems (see Figure 8).

N.B.: "SL-C" is defined by IEC 62443 as when "[…] a particular component or system is capable of meeting the target SLs natively without additional compensating countermeasures when properly configured and integrated" [7](p. 68).

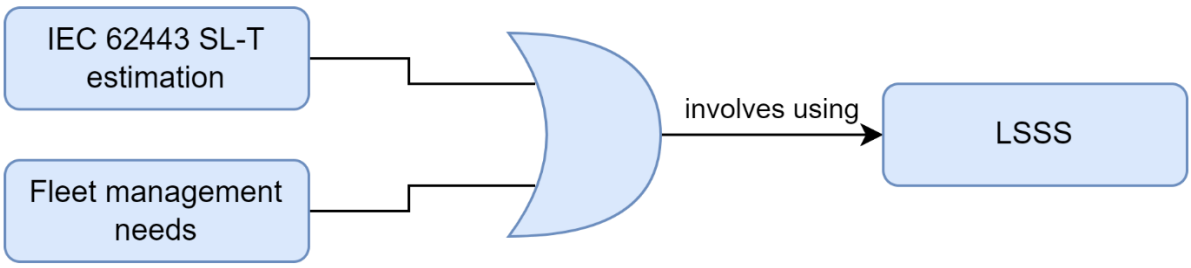

Figure 8 - Factors influencing the need of LSSS in OICS context.

Some advantages when incorporating LSSS to an OICS cybersecurity design are summarized as follows:

- Increased situational awareness of assets of a fleet via centralized monitoring of security events and alerts, if LSSS connection is available.
- Delayed-awareness and supervision of OICS after an offline period.
- Convenient centralized management of accounts (update of users / devices credentials and PKI-certificates / tokens lifecycle).
- Synchronized and reliable UTC time source when implementing a secure protocol as NTS [68] or used to cross-check with a local or GNSS UTC source.
- Timesaving deployment of SW updates to non-safety parts (not needing re-homologation) of the fleet assets.
- Centralized backup and restoration of fleet assets.

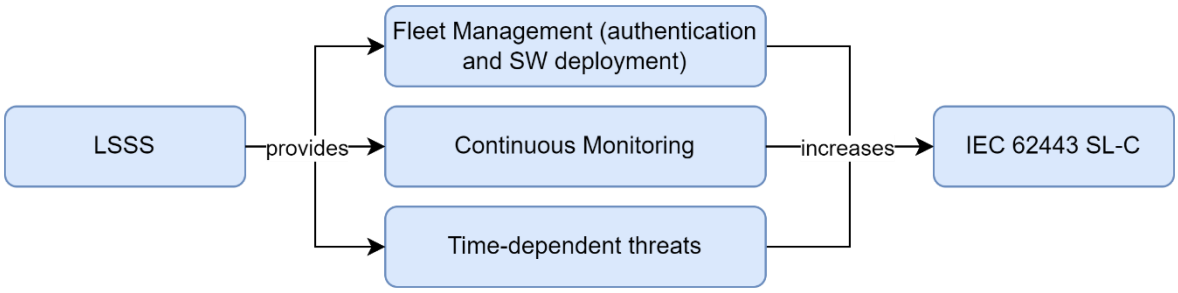

Figure 9 - Advantages of LSSS integration in OICS design.

IEC 62443-3-3 [7](p. 31) has specific requirements imposing the use of LSSS to support basic security functions starting from SL-C = 2 and SL-C = 3, but for security functions like *SR 1.3 – Account management* or *SR 1.5 – Authenticator management* but to name a few, is already recommended the use of LSSS to manage in a centralized way these functions when speaking of a fleet of hundreds or thousands of OICS, and this is with the minimum IEC 62443

SL-C = 1. In fact, most of these security functions without being managed in a centralized way, it heavily impacts both the cybersecurity status of OICS (as access accounts freshness or continuous monitoring) and helps to reduces the maintainability costs, as avoid needing to go to each OICS, locally, to retrieve security events or update local user accounts if a previously trusted employee operating the OICS quitted the company.

In this work it will be simplified the different LSSS services that are provided to an OICS to 4 categories, depending on the support need. This can be summarized as follows:

- **AUTH** – includes support security subsystems for functions like:
  - **Identification and Authentication Management (IAM)** system as for example an OT Active Directory for user and devices account management.
  - **PKI** (including key distribution and certificate creation for communication and device authentication).
- **MONITORING** – comprises services like:
  - **Centralized Log Collector Server** to ensure audit logs of the fleet are centralized for further log correlation and analysis.
  - **SIEM** is the service using the data collected by the Centralized Log Collector Server and is used "to identify patterns and anomalies that could indicate a security incident, facilitating rapid detection and response to potential threats" [88].
  - **SOC** is commonly the place where the SIEM is operated "[…] for identifying, investigating, and remediating threats." [88] and it implies continuous surveillance of assets. They are often connected to sector specific CSIRTs and ISACs to feed with latest vulnerabilities and threat intelligence data.
- **TIME** – involves a time server to synchronize with a system-wide time source common to all OICS.
- **SW REPOSITORY** – server to provide a centralized deployment system for SW updates in non-safety-homologated parts of OICS assets with the correct SW and HW architecture. (Providing safety-homologated SW updates in remote poses many challenges to be agreed also with regulation bodies).

These security features, while increasing the SL-C level, could be seen by fleet operators or engineers not *cyber-aware* as additional constraints, as they certainly complexify a

previously simpler operations by needing to be frequently updated to stay secure, but this is just a matter of cybersecurity awareness and lack of visibility on upcoming regulations.

Organizations may integrate several or more of these support services together. For example, it is common to see solutions for Centralized Log Collector together a SIEM and a SOC, or solutions comprising an OT IAM and the PKI for key management [96].

2.2.4.1. Threat scenarios on OICS per LSSS type

AUTH:

- If wireless connectivity is jammed, the OICS may fall to a degraded mode using local accounts where the authenticators database allowed to connect to the system could be obsolete, making it possible for an attacker to use a disabled local account or revoked certificate in a device to get unauthorized access to the OICS.
- If OICS is shut down for a long time, the authenticators database of users and devices allowed to connect to the system could be obsolete. If the design allows to login without first updating the database, an attacker could use an obsolete authenticator to get unauthorized access to the OICS.
- Other *TIME*-dependent threat scenarios (see below).

MONITORING:

- Wireless connectivity of OICS is being jammed as part of an attack on the and organization may miss alerts and events related to security breaches to react in a timely manner (for example, SW version has changed, UTC time changed, firewall detected an attack, brute-forcing of login interface, or an IDS alert).
- After an offline period, if the OICS did not buffer the alerts and events to send them to the SIEM once the connection is back, the organization may miss alerts and events related to a compromission happened during the offline period and continue operating a potentially compromised OICS without checking it first.

TIME (indirectly related to *AUTH* category):

- If an OICS has no means to authenticate and ensure the integrity of the UTC time (for example from NTP server or GPS), authentication mechanisms (and timestamps of events) could be spoofed to a convenient datetime, leading to the potential acceptance of an already expired authenticator (e.g., X.509 certificates or CRL lists) due

to poor design (soft-fail) or lack of alternative countermeasures like comparing several sources and the last recorded UTC time.

SW REPOSITORY:

- Without a centralized update deployment system, a new published vulnerability affecting all OICS of the fleet could be exploited in the time the organization needs to go in local to patch each OICS.
- **N.B.**: For the purpose of this study, it is assumed that the data hosted in this centralized service is authentic and pushed for deployment by a trusted user preserving its confidentiality, integrity and authenticity.

2.3. Transportation ICS main cybersecurity references

In subchapter 2.1.3 it was briefly introduced how IEC 62443 (previously ANSI/ISA99 series) founded the basis of ICS cybersecurity in a global manner. While in the last two decades there have been issued useful standards, regulations and guidelines for OT security and cyber resilience, a specific tailoring for OICS system design taking into account the particular OICS context of a fleet is still needed to withstand in a hybrid context (centralized/real-time management and isolated/degraded mode).

The following subchapters survey main standards and guidelines for each Transportation OT sector and if they address the OICS nature conveniently to the hybrid operational context presented in 2.2.3. As per this study, there have not been identified specific recommendations considering the mentioned hybrid nature of Onboard ICS, but rather applications and tailoring of IEC 62443 and NIST 800 series frameworks in a general way.

2.3.1. Railways

Railway cybersecurity has significantly evolved in the last years. In 2017 it was first agreed by European stakeholders via the Shift2Rail EU Joint-Undertaking R&D project the international standard IEC 62443 as cybersecurity reference for the Railway industry [20]. Then CENELEC published CLC/TS 50701 [22] merging the IEC 62443 [3], the mandatory European risk management process for the rail industry (CSM-RA [24]) and the RAMS aspects of the railway-

specific EN 50126 standard [23]. This work served as base for the first railway-specific international cybersecurity standard arriving in 2025, the IEC TC9/PT 63452 [25].

Thus, the railway sector correctly identified the need to further adapt a broad ICS standard like IEC 62443 to the specificities of railways (mixed onboard and landside distributed architecture), but while this has been identified as a necessary analysis in the future, no specific focus on Onboard vehicles has been made yet [11][21].

Figure 10 from Fouques et al. [21] summarizes the initiatives carried on at European level for the creation of a global Railway-specific cybersecurity framework.

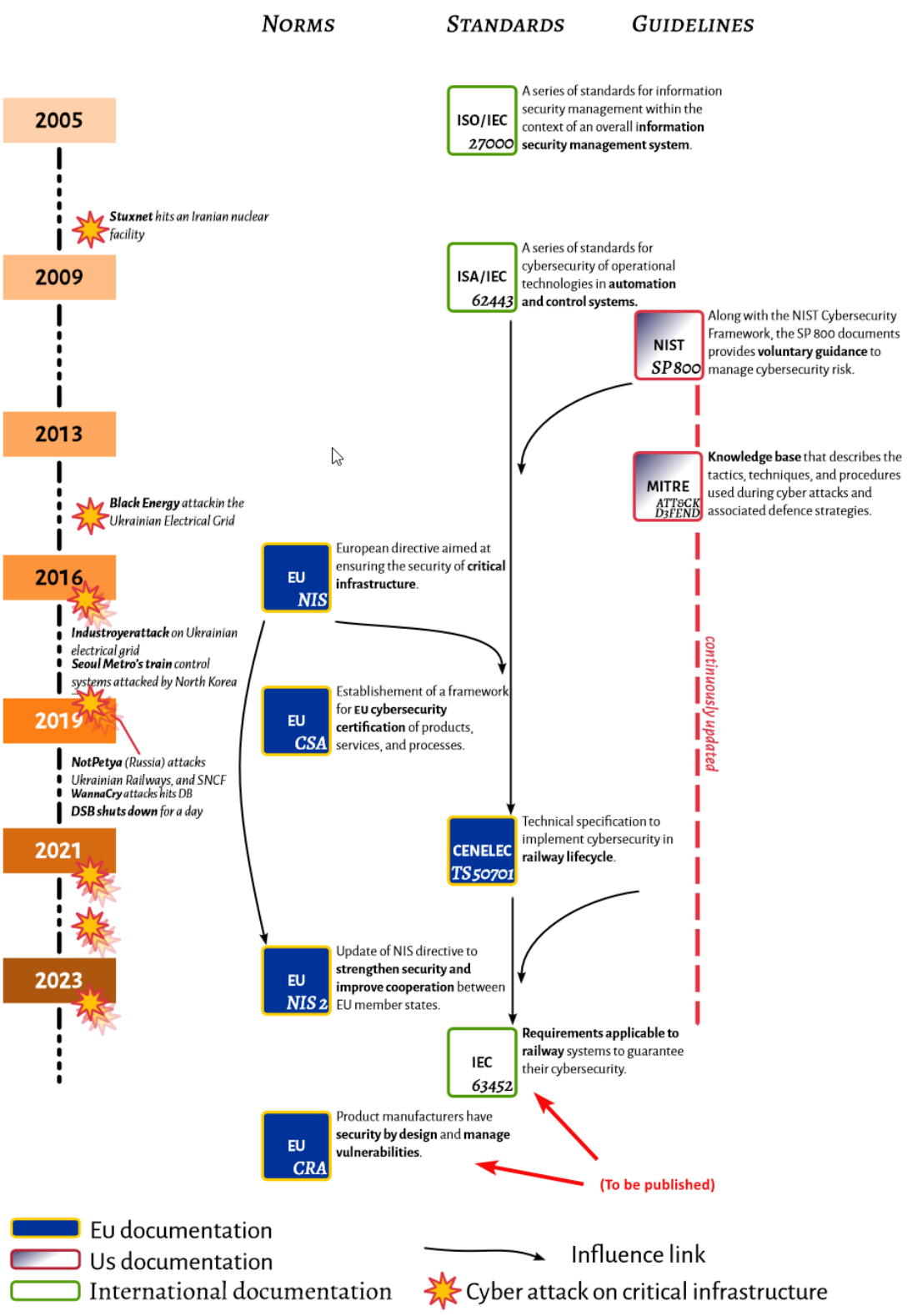

Figure 10 - Development of Cybersecurity in the railway industry in Europe. Alstom. [21](p.45)

When looking outside of Europe, USA associations like APTA also provide references helping to implement OT cybersecurity in the Transportation sector, for example, the "Cybersecurity Maturity Framework for OT" (CSM-OT) applies to "[…] bus, paratransit, light rail, commuter rail, subways, waterborne services, and intercity and high-speed passenger rail[…]" and defines the basis for a cybersecurity resilience model in operational technology systems through structured guidelines and maturity assessment [26].

More specific to railways, APTA provides white papers and recommended practices within their "Securing Control and Communications Systems in (Rail) Transit Environments" series. These references are based in concepts of former ANSI/ISA Standard 99 series (now IEC 62443 [3]) and use NIST 800-82 [28] and NIST 800-53 [29] as source for detailed guidance on cybersecurity controls and concepts as well. The list of documents of this series is the following:

- APTA-SS-CCS-RP-001-10 – *Securing Control and Communications Systems in Transit Environments Part I*, discusses the significance of control and communications security for transit agencies, surveys typical transit control and communication systems, outlines steps for establishing a successful program, and details the stages of conducting and managing risk assessments. The scope is for both Road (buses) and Railway public transport [47].
- APTA-SS-CCS-RP-002-13 – *Securing Control and Communications Systems in Rail Transit Environments Part II (Recommended Practice)*, introduces Defense-In-Depth for securing rail communications and control systems, defines security zone classifications, and recommends minimum security controls for the most critical classification: safety-critical. The scope is specific to railways [45].
- APTA-SS-CCS-WP-003-15 – *Securing Control and Communications Systems in Rail Transit Environments Part IIIa (White Paper),* outlines the APTA attack modeling for transit agencies, their systems integrators, and vendors, intended for use in procurement documents [46]. APTA recommends being used with Parts I [47] and II [45].
- APTA SS-CCS-RP-004-16 – *Securing Control and Communications Systems in Rail Transit Environments Part IIIb (Recommended Practice),* "provides control and

communications security systems designed to protect a transit agency's Operationally Critical Security Zone (OCSZ), including traction power and non-life-safety critical SCADA systems."[27].

- [Unknown] – *Part IIIc (future document),* will cover guidance to secure the zones OCSZ, Fire/Life-Safety Security Zone (FLSZ), and Safety-Critical Security Zone (SCSZ) for rail transit vehicles [27].

As observed, existing cybersecurity guidance for railways, though ample, overlooks the OICS operational context (refer to chapter 2.2.3). This makes it easy, if not carefully thought, to miss during the cybersecurity design of functions to consider security and fleet maintainability not only during a nominal (online) mode but also when OICS is offline for a long period.

2.3.2. Road vehicles

When looking for standardization of Road vehicles sector, there have been also important advances in the last years due in part to the resonance in the easiness to perform car vehicles attacks [105][107].

The automotive sector got in 2021 the first international standard ISO 21434:2021 providing guidelines for identifying and managing cybersecurity risks throughout the vehicle engineering lifecycle. However, the "United Nations Economic Commission for Europe (UNECE)", through its World Forum for Harmonization of Vehicle Regulations (WP.29), already published in June 2020 the first cybersecurity regulations called "UN Regulation No. 155 (UN R155)" cybersecurity framework for the automotive sector with a corrigendum in November 2021, to clarify OTA (Over-The-Air) software updates security requirements. Key constituents of UN R155 include:

- Recognizing and addressing cybersecurity threats in vehicle design.
- Ensuring that identified risks are effectively managed.
- Regularly updating risk assessments to reflect current conditions.
- Continuously monitoring for attacks and implementing response strategies.
- Evaluating both successful and attempted cyber-attacks.
- Reassessing cybersecurity measures to address emerging threats.

- Managing security throughout the vehicle's lifecycle, including development, production, and post-production phases.

The Road industry (and certainly most of the other sectors) are still coping with technology challenges when trying to secure external wireless communications like GNSS. In the "SAE proposals to UNECE WP.29 related to automotive cybersecurity" document in which SAE experts declare the impossibility for an international framework to require "carry out cryptographic authentication of received GNSS messages" at this time, as only EU's Galileo GNSS system would be able to properly cover this requirement, giving exclusivity of use to this only GNSS system and potentially.[116](p. 4).

In the USA, the National Highway Traffic Safety Administration (NHTSA) also launched several key initiatives to enhance cybersecurity since 2016 with its "Cybersecurity Best Practices for the Safety of Modern Vehicles" which received an update in 2022 [115]. And in the Transit sector, APTA adapted their initiatives in railway to the "Securing Control and Communications Systems in Transit Bus Vehicles and Supporting Infrastructure", which a security risk assessment in old and modern Bus Transits, providing a detailed description of OT assets, attack points and assessment in the needed capabilities to attack such vehices.[66]. APTA's scope of the aforementioned OT Cybersecurity Maturity Model Framework (OT-CMF) [10] also applies to Road vehicles sector.

In summary, Road vehicles cybersecurity is ramping up, and in our OICS regard, APTA provides a reference architecture identifying the LSSS in their operational context. However, there is no guidance to implement specific ICS standard requirements like those from IEC 62443 [7], NIST SP 800-82[28] or NIST SP 800-160 [9] to guarantee a secure, maintainable and centralized management of cybersecurity functions in OICS vehicles.

2.3.3. Maritime

Maritime sector has advanced significantly in the last decade. The sector has officially published through and defined a set of cybersecurity requirements and compliance level to the industry through several organizations like the cybersecurity working groups of the "International Association for Classification Societies (IACS) or industry guidelines by main actors like BIMCO, INTERCARGO, Maersk or the World Shipping Council but to name a few.

The IACS published international Unified Requirements addressing cybersecurity for maritime to reduce the likelihood and mitigate the consequences of cybersecurity incidents due to cyber-attacks. They are mandatory applications by the maritime industry. The IACS UR E22 "Computer based systems" [31] includes requirements for design, construction, commissioning and maintenance of computer-based systems where they depend on software for the proper achievement of their functions. Requirements in IACS UR E22 [31] focus on the functionality of the software and on the hardware supporting the software which provides control, alarm, monitoring, safety or internal communication functions subject to classification requirements, while IACS UR E26 [32] deals with requirements related to the cyber resilience of ships and IACS UR E27 with cyber resilience of on-board systems and equipment [33]. Finally, IACS Recommendation 166 on Cyber Resilience, while non-mandatory, it provides the recommended technical requirements that stakeholders may reference and apply to assist with the delivery of cyber resilient ships, whose resilience can be maintained throughout their service life. While the IACS recommendations apply to newbuild vessels and ships, it can also be applicable as guides for existing ships.

It is worth noting that maritime companies itself like *ClassNK* have been particularly proactive by providing interesting guidelines to the implementation of IACS Unified Requirements, like the ClassNK guideline [86] or guides like the DCSA's "Implementation Guide for Cyber Security on Vessels" [118] and "The guidelines on cyber security onboard ships" [117].

For further reading, a detailed analysis on specific cybersecurity Maritime regulation both at international organizations and country regulations has been given by Progolaukis et al. [51].

2.3.4. Aviation

Aviation, as per this master thesis research, has been the most prolific industry in creating a common framework for cybersecurity across all sector stakeholders. ICAO already make available a comprehensive "*Compilation of Cyber Security Regulations, Standards, and Guidance Applicable to Civil Aviation"* [61]. In this compilation, it is worth noting the already mentioned standards for secure product development *ED-202A/DO-326A* [57][58] *and ED-203/DO-356A* [59][60].

Particular consideration merits IATA's Aviation Cyber Security Guidance Material – Part 2 (Aircraft) which takes into account from a cybersecurity point of view, the OICS operational context when speaking about "Cyber Security Considerations Relative the Parked Aircraft" in chapter 2.4 as consequence of the COVID pandemic when aircrafts were grounded during months. In this chapter, IATA gives guidance on security checks to ensure cybersecurity, but specific details about ensuring the retrieval of an UTC time or sending logs to a SIEM are not considered, perhaps because aviation sector do not have as reference architecture the integration of LSSS to support cybersecurity functions like IAM, PKI or Audit logs collection in a centralized manner.[56](p. 11).

However, while ICAO in its compendium provides risk assessment methodologies and guidelines to stakeholders, unlike joint railway sector through Shift2Rail JU [65] or APTA for Road vehicles transit [66](p. 9-18), in Aviation there is limited public information related to OICS (aircraft) architecture, threat landscape and their associated risks. Yet, standards *ED-203A/DO-326A* [59][58] provide information related to threat assets conditions and identification and ED-204A/DO-355A [62][63] can be used to "[…] map Continued Airworthiness requirements against the CIA and mitigation strategy" [56]. In mentioned IATA's guidance [56], it is listed an asset inventory of OICS included in an aircraft and some example of generic threats are given in chapter 3.1 of [56], however, no official sector cybersecurity risk assessment or OICS threat landscape taking into account LSSS has been found.

2.3.5. International ICS cybersecurity standards

In this chapter, while there are multiple standards that can be applied to ICS like ISO 27001 [15] or NIST CSF [14], we will present the principal and internationally accepted standards for industrial control systems in which most of sector-specific standards, guidelines and regulations are based:

- IEC 62443 [3], and
- NIST SP 800-82r3 [28] together with NIST SP 800-160 Vol. 2 [9].

Specifically, we will introduce the seven Foundational Requirements and Security Level definition of IEC 62443, which will be used during our methodology in chapter 4.

2.3.5.1. IEC 62443

The IEC 62443 series, formerly an ANSI/ISA standard, is based in ISO 27000 series and rewritten to cover different aspects of IACS cybersecurity. It was organized in four primary categories with several parts each (see Figure 11):

- Part 1 – General concepts (including concepts, glossary and IACS lifecycle)
- Part 2 – Policies and procedures (providing guidance to establish and implement an IACS program and a Patch Management strategy in IACS)
- Part 3 – System requirements (introducing "Security Levels", risk assessment methodology, and system security requirements and technologies)
- Part 4 – Component requirements (defining a Secure-by-design lifecycle and technical security).

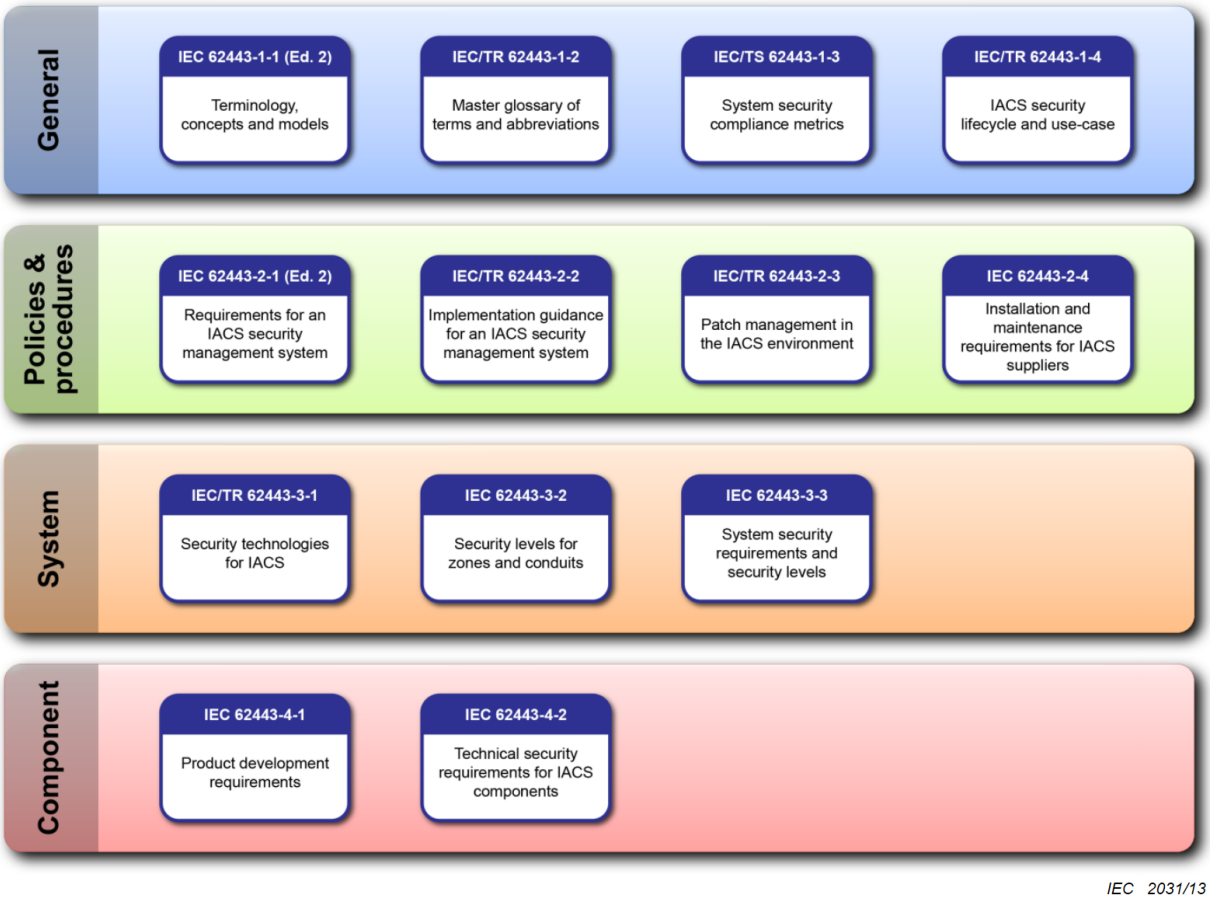

Figure 11 - IEC 62443 series of standards overview. IEC. [7](p. 13).

The main goals of IEC 62443 include guidance for establishing governance structures dedicated to ICS, forming dedicated OT cybersecurity teams, assessing risks, specifying

requirements for the organization but also during system and product development, evaluating risk mitigations, and maintaining asset security throughout their lifespan.

The technical requirements given to System (in part IEC 62443-3-3 [7]) and Product (IEC 62443-4-2 [70]) are divided in seven Foundational Requirements (FRs) classified in the following ICS capabilities:

- **Identification and Authentication Control (FR1)**: To implement robust mechanisms for ensuring users and devices are who they claim to be and controls to restrict access to authorized personnel or devices.
- **Use Control (FR2)**: To regulate how authorized users and devices interact with the ICS and prevent unauthorized actions enforcing access controls.
- **System Integrity (FR3)**: To safeguard the ICS from unauthorized modification, making sure the system operates as planned.
- **Data Confidentiality (FR4)**: To protect sensitive information within the ICS from unauthorized disclosure.
- **Restricted Data Flow (FR5)**: To manage how data transits within the ICS, preventing unauthorized lateral movement or access.
- **Timely Response to Events (FR6)**: To ensure prompt detection, reporting, and containment of security incidents to minimize the potential impact.
- **Resource Availability (FR7)**: To maintain critical ICS resources available and operational during normal and abnormal situations (for example, during a DoS attack). [3].

Each FR has four Security Levels, from SL1 to SL4 corresponding to the security requirements of each FR needed by the system (or product) to protect from threat actors with basic (SL1) or advanced (SL4) capabilities, motivation and resources. The formal definition for SL is provided by IEC as follows by taking the example of FR1 set of requirements needed to "Identify and authenticate all users (humans, software processes and devices), prior to allowing them access to the system or assets":

- **SL 1** – Identify and authenticate all users (humans, software processes and devices) by mechanisms that protect against casual or coincidental access by unauthenticated entities.

- **SL 2** – Identify and authenticate all users (humans, software processes and devices) by mechanisms that protect against intentional unauthenticated access by entities using simple means with low resources, generic skills and low motivation.
- **SL 3** – Identify and authenticate all users (humans, software processes and devices) by mechanisms that protect against intentional unauthenticated access by entities using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
- **SL 4** – Identify and authenticate all users (humans, software processes and devices) by mechanisms that protect against intentional unauthenticated access by entities using sophisticated means with extended resources, IACS specific skills and high motivation." [70](pp. 26).

(Considerations for Security Level estimation for OICS are given in chapter 4.2).

To conclude, arguably, IEC 62443 is known as THE industrial control system reference for cybersecurity, it provides a comprehensive framework for organizations willing to protect their OT environment through a wide range of challenges and design guidance to enhance the safety, reliability, and resilience of industrial systems against cyber threats. However, perhaps due to this broad extent, it does not consider or even mention onboard control systems, justifying the needed consideration in our study scope. Yet, it will be the reference base for our methodology, as most of the Transport sector references it at some point [10][11][20][21][22][25][33][61][65] [65][66][67]in their cybersecurity frameworks, guidance or research initiatives to protect ICS in the Transport sector.

2.3.5.2. NIST 800-82r3 and NIST 800-160.

Besides the aforementioned IEC 62443 [3], major countries like the USA have also provided in the last decades, via the National Institute of Standards and Technology (NIST), multiple cybersecurity resources considered "industry-accepted" and acknowledged by the cybersecurity community, despite some controversies with former recommended cryptographic standards [69]. Main resources from NIST, often referenced by sector-specific OT cybersecurity standards and guidelines, are the ICS series of NIST Special Publications (SP), standards and guidelines. Unfortunately, NIST publications are not specific to an industry

sector and, thus, does not consider Transport OICS specificities besides mentioning drones and UAVs.

In chapter 5.4.2 of NIST SP 800-82r3 “Guide to Industrial Control Systems (ICS) Security” [28](p. 86), it is proposed a “DCS - and PLC-Based OT with IIoT” architecture that could seem similar to a distributed architecture like OICS fleets, but does not really adapt to the OICS context. However, in chapter 5.3.7 it provides interesting “Additional Security considerations for IIoT”, which considers the “[…] increase connectivity and information exchanges with enterprise systems and cloud-based systems, which may require additional considerations for the security architecture.” that could be used as useful guideline for minimum OICS security capabilities together with the proposed by NIST SP 800-160 Vol 2.

The special publication NIST SP 800-160 Vol 2.[9] offers a complete set of directions to develop ICS in a secure and resilient way. It actually recognizes the existence of OICS and its context as “[ICS] Some systems are designed to operate without a network connection, at least transiently and often normally. The cyber resiliency solutions and means of assessing system cyber resiliency or solution effectiveness will be limited by whether the system is operating in detached mode.” [9](p. 35)., but there is no specific guidance for those besides when looking to the definition of the approach “Adaptive Management” recommending to “change how mechanisms are used based on changes in the operational environment as well as changes in the threat environment.”[9](p. 93), however these changes are more referred to dynamic responses from the system after a real-time detection recognized by the system (for example, disabling an account after a number of wrong trials), but the definition might correspond, with sufficient purpose, to the hybrid approach we are presenting in this master thesis for OICS.

2.3.6. Other impacting standards

2.3.6.1. GDPR

The Regulation (EU) 2016/679 (General Data Protection Regulation) mandates when personal data stored on ICS can identify any human person action by, for example, using an identification number (ID), to allow the execution of personal information rights. These are commonly known as “ARCO” rights (Access, Rectification, Erasure and Opposition) plus the Limitation of Processing and Portability.

It is very important to define the roles (Data Controller, Data Processor, DPO and Supervisory Authority), responsibilities and scope of each stakeholder involved in the personal information data to comply with these rights in an ICS logging context. These roles need to be defined by the ICS manufacturer, the owner of the ICS and the company hiring the operator of the ICS (which could be the owner itself or not).

The **scope of the ICS manufacturer, when logging identified human actions in the ICS**, would fall into the **Data Processor** role and responsibility, which could be summarized as:

- Ensure the technical means on the ICS or logging system to Access, Rectify and Erase the stored data.
- Put in place the necessary technical mechanisms to protect this information from disclosure.

The **scope of the organization responsible for the ICS** operation would be then as the **Data Controller** as follows:

- It is the ultimate responsible for the logged data and its means (purpose to record it) in the ICS.
- It is also the entity responsible for executing all aforementioned rights (with the technical means provided by the Data Processor or additional ones if they are sent to a centralized server) when a person requests the application of its rights in the frame of its personal data. This must be founded in GDPR legitimate bases and consented, if needed, by the individual whose data is being treated during the hiring process. Also, it needs to consider (Data Processor could collaborate on this regard) that deadlines for the execution of the rights are respected (for example, Access in a maximum of 30 days, and Rectify and Erase the data in a maximum of 10 days).
- It needs to also identify the impact of a security breach on these data (low to none, as normally only the identifier, actions and the related timestamp are recorded in the frame of ICS operation).

There are other roles involving the personal data processing and treatment regarding GDPR (DPO assignation, the pertinent Supervisory Authority applicable to the organization

sector), but this is beyond the scope of the ICS recorded data. It does not need to be said that it is mandatory to do a thorough study in this important matter.[99].

2.3.6.2. CSA, NIS2 and CRA

Cyber Security Act: The European Union's Cybersecurity Act (CSA) of 2019 amplifies cybersecurity across the bloc through with two key objectives. Firstly, it grants the EU Agency for Cybersecurity (ENISA) a permanent mandate, solidifying its role in supporting member states to reach a high level of cybersecurity. Secondly, the CSA established a harmonized EU-wide framework for the certification of ICT products, services, and processes. This framework goal is to simplify compliance for businesses operating within the EU while ensuring a consistent level of cybersecurity throughout the member states [72].

NIS 2 Directive: In 2023, the NIS directive was revised and replaced by the NIS2 directive. Its purpose is to homogenize a high level of cybersecurity across EU members based on a set of requirements and security plans. Its scope was extended to cover more entities such as digital service providers and maintenance service providers. This regulation will require national authorities to integrate these changes into their legal systems for October 13, 2024. [4].

Cyber Resilient Act (CRA): The upcoming CRA proposal will greatly impact manufacturing. It will mandate that all digital assets produced in EU market will need to provide during their whole lifecycle (OT assets have 15-30 years lifespan depending on the sector) to deliver new versions and patches to customers free of vulnerabilities at no cost (with exceptions) [5](paragraph 23). This kind of requirements implies huge costs and a thorough planification by manufacturers on component architecture design to correctly segregate the HW elements prone to receive frequent updates (cyber functions impacted by new vulnerabilities) from those requiring a new homologation with every new line of code (safety functions).[5].

2.3.7. Autonomous Operation with OICS

In the last years, autonomous or driverless operation has been one of the research and development lines in the Transportation sector.

For example, only in Europe there are projects like MODI [16] and PoDIUM [17] searching to improve logistics with autonomous road vehicles, but adapting the legislation and infrastructure still remain two of the main challenges.

The railway sector is the most tangible related to autonomous transport. Driverless operations like UTO GoA4 don't stop increasing year over year (see Figure 12) with Multiple lines spread over the world, especially in Urban (metro and tram) [18][19] and with regulations already being adapted to it [84](p. 16).

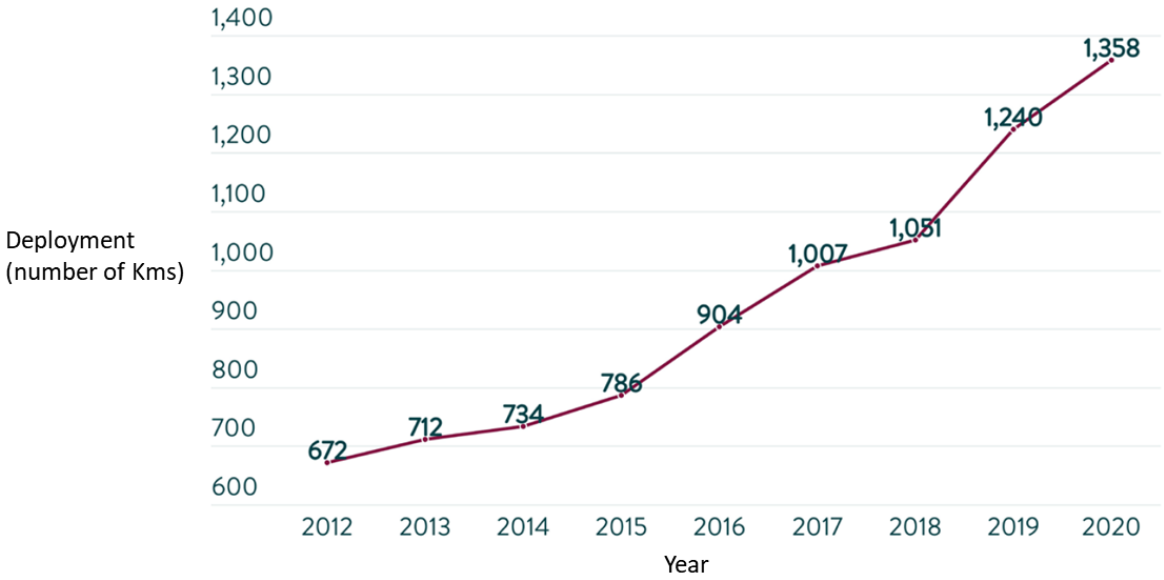

Figure 12 - Evolution of number of kilometers of driverless (GoA4) Urban vehicles (metro and tramways). UITP [19].

In Aviation there have been also considerable advances and tests on autonomous flight besides autopilot systems integrated in most planes these days. For example, *Xwing* is one of the pioneers testing first a remote driving (not autonomous) system in 2020 [81] and then successfully tested a gate-to-gate autonomous mission in February 2021 [82]. *Reliable Robotics* is also in business and performed a full autonomous flight with no one on board in November 2023 [83] making a step forward. Both companies used a Cessna 208B Caravan for these tests' flights.

When looking at Maritime, there are also advances in this regard setting also 4 levels of autonomy, being "degree four" a fully autonomous ship "able to make decisions and determine actions by itself" [100]. The International Maritime Organization (IMO) aims to integrate driverless shipping into its regulatory framework while addressing safety, security, environmental impact, and costs. IMO is developing a non-mandatory Maritime Autonomous Surface Ships (MASS) Code to take effect in 2025, to become mandatory in 2028. Its aim is to regulate autonomous shipping operations. Key issues include defining roles and

responsibilities, addressing cyber risks, and ensuring sufficient safety and environmental protection during trials. A summary of the advances can be seen in IMO article [100].

The nature of railway vehicles following a fixed infrastructure in a "closed" circuit is no doubt the reason why autonomous operation became already a reality in rail industry before other Transport sectors. Indeed, the other sectors require to control free movement in two or even three-dimensional spaces and be aware of its environment with the other vehicles, vessels or planes for safe operation. Thus, while no having human-in-the-loop is even more relevant from a cybersecurity point of view to ensure a prompt reaction on a security incident, the driverless environment needs today a fully connected OICS context to be aware of its environment, thus making irrelevant for our hybrid study purpose with offline periods. Nonetheless, it is a subject worthy of a separate study when regarding to OICS cybersecurity.

2.4. Threats in Transport OICS

The alarming data numbers given by cybersecurity agencies like ENISA [78] and companies like Dragos [2], Fortinet [101]or Kaspersky [102] greatly shows the importance of , this chapter aims to offer a quick summary on OICS threats and provide some references for further research on the topic. Globally, there is limited information on actual threats officially published by the industry, but the research community has been prolific in the topic.

Some Transport sectors have public security risk assessments made by cybersecurity industry working groups. For example, Railway sector did a confidential detailed risk assessment and thus the details inside cannot be disclosure in this work [65], but the threat categorization, threat actor landscape and zone and conduits architecture are public. The American transport association, APTA, performs a security risk assessment in public Bus transit [66] and the Maritime sector performed some evaluation in the OICS but it is limited to the impact assessment. In aviation though, there have not been public security risk assessments but there are public documents from ICAO identifying common threats to aircrafts [56]. Also, in civil Aviation needs to be considered an increased physical protection (see chapter 4.2.2 for an analysis on this) with human-in-the-loop or CCTV in most cases, but it should be assumed that the risks to their OICS are similar to other sectors due to the same threat actor landscape

(see chapter 4.2.1 and Annex A for a discussion on this regard) characteristic to OT environment.

This chapter aims to reinforce the importance in the identification of threats and the assessment needed in the capabilities of potential attackers when considering OICS threats for further discussion (see 4.2.1). For this purpose, besides the industry sources, it will be also mentioned some articles and papers from the cybersecurity research community on specific threats applicable to each sector.

2.4.1. Road vehicles

In the same reference, there is an interesting section in which the Bus transit is compared to Railways, showing the similarities between both and thus the potential applicability of the following evaluation. However, when looking at the consequences of a safety impact in a bus (maximum 100 persons and +/- 100 km/h) or a train (around 300-400 persons and speeds from 100-350 km/h), the severity in human safety of a security incident is even higher than the one depicted below.

First, the level definitions for attackers and physical protection mechanisms are as follows:

- **Physical Access Protection:** ranging from 1 = Physical barrier present; and 3 = No physical barrier.
- **Attacker Skill:** ranging from 1 = High skill needed; to 5 = Only low skill needed.
- **Attacker Effort:** ranging from 1 = High effort/time; to 5 = Low effort only
- **Consequence (Severity):** ranging from 1 = Nuisance, some delay; 4 = Big delay, equipment damage; to 5 = Injury or loss of life.
- **Attacker types:** Insider and Outsider/Intruder.

Then, the risk assessment listed the potential infrastructure points illustrated in Figure 13 and Figure 14:

- “CAD Wi-Fi from bus garage to vehicle before daily run.
- Jamming GPS signal.
- Intercepting/blocking/masquerading AVL/AVM cellular signal to cell tower.
- Hacking AVL/AVM processing center and database.
- Intercepting/blocking/masquerading voice or digital radio signal to tower.
- Hacking control room/dispatch center computers or network connections” [66](p. 18).

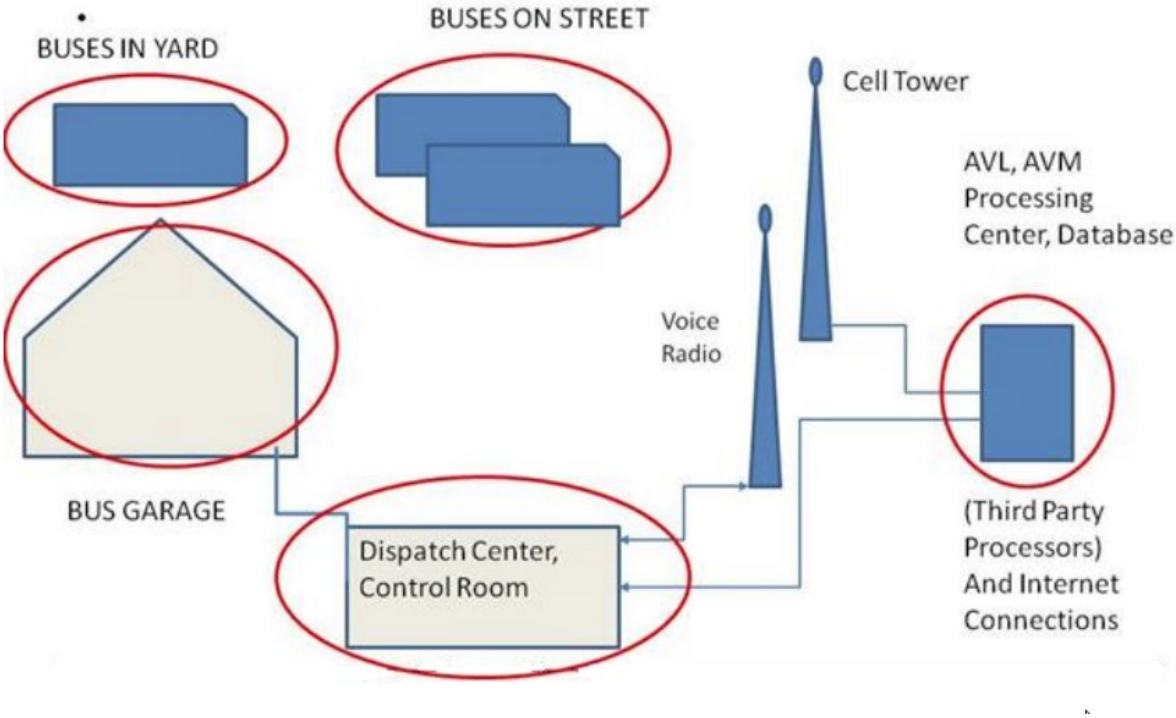

Figure 13 - Attack points for a Bus Transit classical infrastructure. APTA. [66](p. 17).

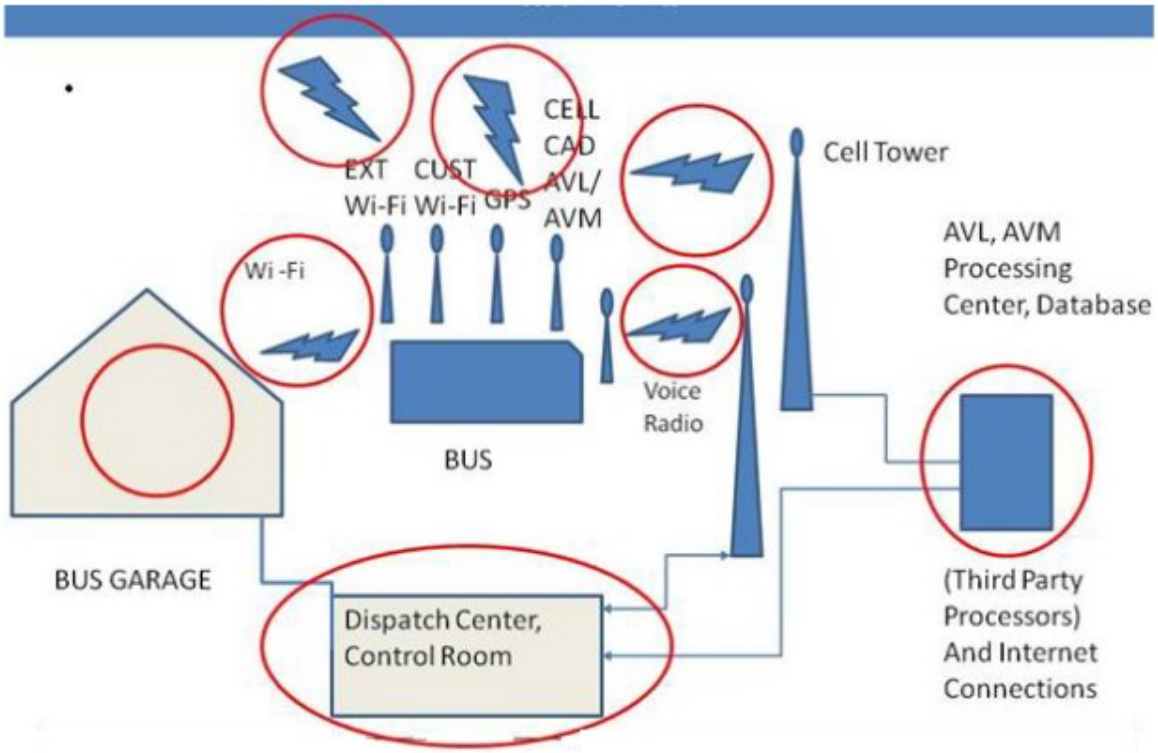

Figure 14 - Attack points on wireless for a Bus Transit classical infrastructure. APTA. [66](p. 18).

Access	Action	Actor	Physical Access Protection	Attacker Skill	Attacker Effort	Consequence (Severity)
Operator TCH Unit	Change settings	Insider	2 Login/password	3	4	3
Operator TCH Unit	Unauthorized access/ driving	Intruder	3 Login/password	1	3	3
J1708 Access Port	Hook up sniffer/packet injection access/change VLU data or VAN commands	Insider	3 Maybe	2	2	3 Disruption
J1708 Access Port	Hook up sniffer/packet injection access/change VLU data, modify J1708 VAN equipment	Intruder	3 Maybe	1	1	2
VLU Laptop Access	Hook up rogue laptop, access/change VLU programming	Insider	3	1	2	5
VLU Laptop Access	Hook up rogue laptop, open up unauthorized channel to engine networks for present or future sabotage	Intruder	1	4	3	5

Access	Action	Actor	Physical Access Protection	Attacker Skill	Attacker Effort	Consequence (Severity)
DVR Manual Access Port	Unauthorized access	Insider	3 Maybe	3 Access, change, delete video record	3 Access, change, delete video record, modify operation of CCTV, DVR network	3
J1939/J1708 Manual Access Port (OBD?)	Unauthorized access, adjust safety-related settings, reprogram safety-related ECM	Insider	3	3	3 Adjust equipment settings to sabotage	5
J1939/J1708 Manual Access Port (OBD)	Adjust equipment settings to sabotage, adjust safety-related settings, reprogram ECUs	Outsider	1	3	3	5

Figure 15 - Extract of threat risk assessment and attacker evaluation on "2016 Bus Electronics". [66](p. 15).

If we take the worst-case threat scenario to summarize, it can be concluded that an outsider attacker with just moderate skills and efforts can succeed in performing an attack with loss of life even when physical protection to access the system is present.

Regarding road vehicles, in 2016, security researcher Craig Smith published The Car Hacker's Handbook [105] and there exists multiple sources like El-Rewini et al. analyzing the threats in road vehicles [106] like and its surface attack, as well as published attacks like the 2-minutes attack to the Tesla Model X described in "Fast, Furious and Insecure" attack performed by Wouters et al. with 300$ kit composed of a key fob, Raspberry Pi and a replacement engine control unit[107].

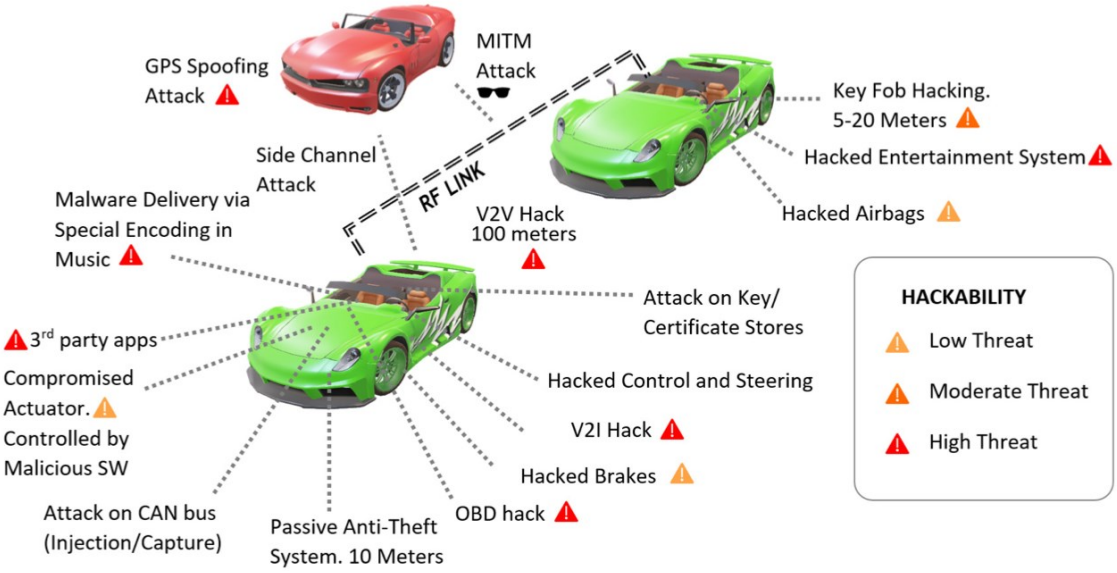

Figure 16 - Attack surface of a common road vehicle with future Vehicular Communication.[106](p. 3).

2.4.2. Railways

For Railways, the first detailed risk assessment done by the European railway-industry project X2RAIL-1 [65] are confidential, but the threat actor landscape, the zone and conduit architecture and the agreed SL-T estimation for each zone by the sector were published in the simplification of the risk assessment done in X2RAIL-3 “Deliverable D8.1 Guidelines for railway cybersecurity” [93] and the ENISA report “Zoning and conduits architecture for railways” [6], being SL-T = 3 for safety-critical assets corresponding to Railway OICS.

The threat landscape is composed of Insider and External actors, and the selected worst-case and typical actor chosen as “Criminal Organization”, with a score of 3 out of 4 in capabilities and motivation, being only greater by Nation-state actors (Governmental Organization) which is depicted in *Figure* 17 and Figure 18 [93].

Threat actors		Capability	Motivation	General description of threat actor
INTERNAL THREAT ACTORS	**Internal Attackers (Insiders)**	**3**	**2**	The internal attacker is typically an employee of the operator or a contractor. This attacker has extensive technical, internal and insider knowledge about the operational environment. The motivation could be driven by ego, curiosity, rebellion and revenge. The access level is the Intranet. The internal attacker has privileged physical and/or logical access to system hardware and software.
EXTERNAL THREAT ACTORS	**State Actor (Governmental organisation)**	**4**	**1**	Concerning the skill level, state actors and criminal organization may be comparable in their employed methods (complex attack campaigns). However, state actors have extensive resources at their disposal and can design new attack tools targeted specifically for a critical infrastructure. Their motivation is industrial espionage (extract intellectual property and obtain sensitive information for black mail purposes) and political aims (create chaos, disruption operation, destruction of systems, media attention). The attacks can be part of a wider cyber-attack with accompanied fake news on social media and denial of services attacks on important telephone hotlines and web sites.
	Criminal organisation	**3**	**3**	A criminal organization employs highly skilled hackers with extensive technical and extensive security knowledge. They use, adapt and create hacking tools and use social engineering methods. Their motivation is financial interest through theft (valuable data, sellable intellectual property) or blackmailing. The access level is the Internet and poorly protected physical interfaces. They employ complex attack campaigns using spear fishing techniques (personalized e-mail with malware) or add an attack device to a poorly protected physical interface thus obtaining a first foothold at a site. With additional tools the lateral movement through the system starts and more systems get compromised. After the scan of the system and identification of access path, the attack is continued to deeper levels (e.g. from office environment to operation control environment). After installing persistent backdoors and the extraction of valuable data, crypto lockers are applied to the compromised devices and ransom is requested from the operator to unlock the system.

Figure 17 - Extract of Threat actor landscape. X2RAIL-3. [93](pp.55-56).

Score	Capability - Description
0	The attacker has none or basic user skills with computers.
1	The attacker can perform simple and publicly available attacks, no research or discover new threat vectors. It is not focused in a particular target system. If they perform a reconnaissance it will be active and easily detectable.
2	The attacker can combine several simple vulnerabilities to create new attack trees and can do basic passive reconnaissance to study the infrastructure of its victim. It will focus mainly in non-patched or not regularly maintained systems.
3	Attacker/s willing to invest the time necessary in passive reconnaissance and do research zero-day vulnerabilities for an attack in order to ensure the intended impact. Have enough skills to craft new exploits and enough resources to perform multiple attacks simultaneously. Can focus on patched or regularly maintained systems if necessary and exploit them by using a zero-day vulnerability.
4	Same as cap. 3 but with more resources

Figure 18 - Capability scoring proposed by X2RAIL-3. X2RAIL-3. [93](p. 56).

Score	Motivation - Description
1	Unawereness of possible impact, no injuries. Test new public hacking tools (no injuries / no significant impact).
2	Disruption of business (availability, intelectual property)
3	Mainly availability impact and gathering of information, reuse of architecture (financial targeting). Disruption, Reputational gain. High disruptions, injuries and kill people. High media impact

Figure 19 - Motivation scoring proposed by X2RAIL-3. X2RAIL-3. [93](p. 56).

Then, the zone and conduit architectures proposed at the time during the first detailed risk assessment [65] and then in the simplified [93] can be seen in Figure 20.

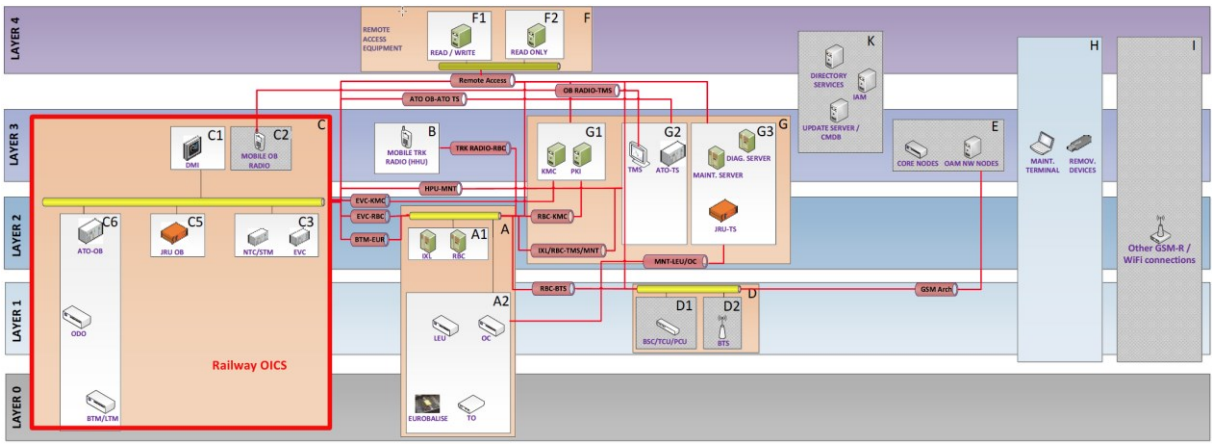

Figure 20 - Zones and Conduits architecture for Railway vehicles. X2RAIL-3. [93](p. 9).

And the proposed SL-T for the zone C3 corresponding to the EVC, the most critical OICS (at OT asset level) in the Railway OICS can be seen in Figure 21.

Zone			
C3 - located in On-board			
Assets			
EVC, NTC/STM			
Description (Zone C3)			
This equipment is responsible for the calculation of the permitted speed in the supervision of the train's march, including the different breaking curves. The information received by the equipment on board contains the geographical data of the selected sections, as well as its maximum speed and the MA. This information is processed for the continuous control and supervision of the movement of the vehicle.			
Rationale (Zone C3)			
Onboard assets with same functionalities and SIL level.			
Geographical Location		**Common Physical Protection**	
On-board		Enclosed local with control access	
Operational Functions	**Purdue Layer**	**Safety-Critical Level**	**SL-T (Target)**
Operational Control	2 (Operational Control)	SIL 4	SL 3

Security Level Vector							
FR1-IAC	FR2-UC	FR3-SI	FR4-DC	FR5-RDF	FR6-TRE	FR7-RA	FCM
3	3	3	3	3	3	3	3

Figure 21 - Example given for generic SL-T for zone C3. X2RAIL-3. [93](p. 63).

Finally, when looking for railway specific threats in the research community, there exist multiple interesting references like the complete compendium of issues and challenges from Yu et al. in 2023 [43] or the paper of Chen et al., dedicated to Urban [108] but to name a few.

2.4.3. Aviation

"Every week, an aviation actor suffers a ransomware attack somewhere in the world, with big impacts on productivity and business continuity" and the reported number of attacks are up with an increase of 530% year-on-year [48]. ICAO considers two categories of threats:

- Indirect facilitation-vector to a subsequent act of unlawful interference, and
- Direct disruption – business continuity (rather than conventional aviation security and safety).

Also, from "Directive 2013/40 / EU obliges the Member States of the European Union to take steps to punish the following offenses as crimes:

- unlawful access to information systems […] at least in the cases that are not minor.
- unlawful interference with systems […] at least in the cases that are not minor.
- unlawful interference with data […].
- unlawful interception […]."[53].

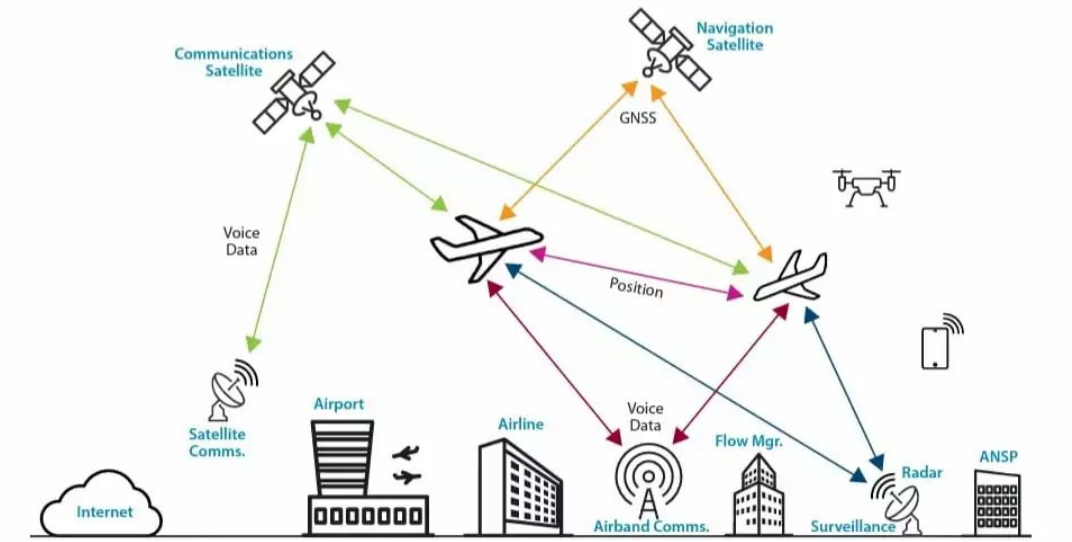

Figure 22 - Aviation global architecture. SOCRadar [55].

As mentioned in chapter 2.3.4, a threat landscape is given by ICAO in the chapter 3.1 of the cyber guide for aircraft [56]. As official statement, we will use them as a summary for OICS threats:

- "Violation of security partitioning, like crossing over the aircraft's domains and into the Aircraft Control Domain (ACD) subsystems or connecting uncertified or unauthorized devices to the ACD or AISD (Aircraft/Airline Information Services Domain).
- Spoofing of authentication mechanisms leading to malicious or unsafe Over-the-Air update or causing misinformation over a flight data or navigation systems leading to unsafe flight conditions or spoofing of telemetry or recordings/records.
- The side-channel attack, buffer overflow exploitation, enabling reverse engineering of the asset, leading to zero-day vulnerability exploitation.
- Denial of Service attack, which may lead to temporary or complete unavailability of essential information, data, function, or service.

- Compromised maintenance or other equipment whilst connecting to the aircraft leads to unauthorized disclosure, malware injection, denial of service attack transfer, or injection/enabling of malicious backdoor."[56](pp. 13-14).

As stated by Hasratyan et al. [11], "A holistic approach is necessary in the risk assessment, requiring collaboration and information sharing between the national authorities and the industry. This fits into the bottom-up feeds from operators and the top-down intelligence from the States. Operators should be made aware of the threat picture pertinent to their activities from a national threat assessment standpoint." [11](p. 21). Such risk assessments should also bring up risks to overcome the fact that "[…] secure aviation communication systems have been long overdue, arguing that cases of existing vulnerabilities being exploited historically are sparse."[54](pp. 13-14).

Finally, multiple independent researchers have identified and proposed attacks [52][53][54] to civil aviation wireless communication systems as ACARS, GNSS or ADB-S. Such OICS aviation threats are generally related to radio communication jamming and spoofing attacks able to deviate a plane due to the lack of message authentication [52](p. 561), but also a shocking attack getting unauthorized access to the navigation system via a smartphone through the public wireless of the plain was claimed by security researcher Chris Roberts in 2015 [64].

2.4.4. Maritime

In Maritime, most of critical systems can be seen defined in IACS UR "Examples of category III systems: Propulsion control system, steering gear control system, electric power system (including power management system), dynamic positioning system (IMO classes 2 and 3)".[31](p. 8). Then, an assessment on the impact of the different categories, being II and III those related to OICS, is given in IACS No. 166 [34] and they are categorized by the potential impact loss as:

- **"LOW**: The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on human safety, safety of the vessel and / or threat to the environment.

- **MODERATE:** The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on human safety, safety of the vessel and / or threat to the environment.
- **HIGH**: The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on human safety, safety of the vessel and / or threat to the environment."[34](p. 28).

Category	Effects	System functionality	Confidentiality	Integrity	Availability
I	Those systems, failure of which will not lead to dangerous situations for human safety, safety of the vessel and / or threat to the environment.	Monitoring function for informational / administrative tasks	Low	Moderate	Low
II	Those systems, failure of which could eventually lead to dangerous situations for human safety, safety of the vessel and / or threat to the environment.	Alarm and monitoring functions Control functions which are necessary to maintain the ship in its normal operational and habitable conditions	Moderate	High	Moderate
III	Those systems, failure of which could immediately lead to dangerous situations for human safety, safety of the vessel and / or threat to the environment.	Control functions for maintaining the vessel's propulsion and steering Safety functions	Moderate	High	High

Figure 23 - CIA impact of an attack in a ship depending on System category (I, II or III). IACS. [34](p. 28).

The adversaries identified in the IACS No. 166 guideline [34] includes Criminal Organizations, interstate adversaries, disgruntled employees, and terrorists; while the most likely security breach scenario was identified as the planting of malware into control systems and a direct remote cyber-attack to vessel OT and IT systems. [34]

Finally, cybersecurity research articles, Potamos et al. [109] provides a comprehensive survey and analysis of common threats and challenges on current maritime cybersecurity, and propose the fusion of OT data from multiple sensors at different Purdue levels to enhance real time or near-real time detection of incidents (see Figure 24). Another interesting article is the one from Progoulakis et al. [51], where is compiled the threats identified in the sector as well a detailed presentation of "[…] existing industry and governmental policies, directives, and standards that cover the subject of cyber security for maritime assets" [51] (p. 3), together with a discussion on several methodologies for risk assessment and mitigation.

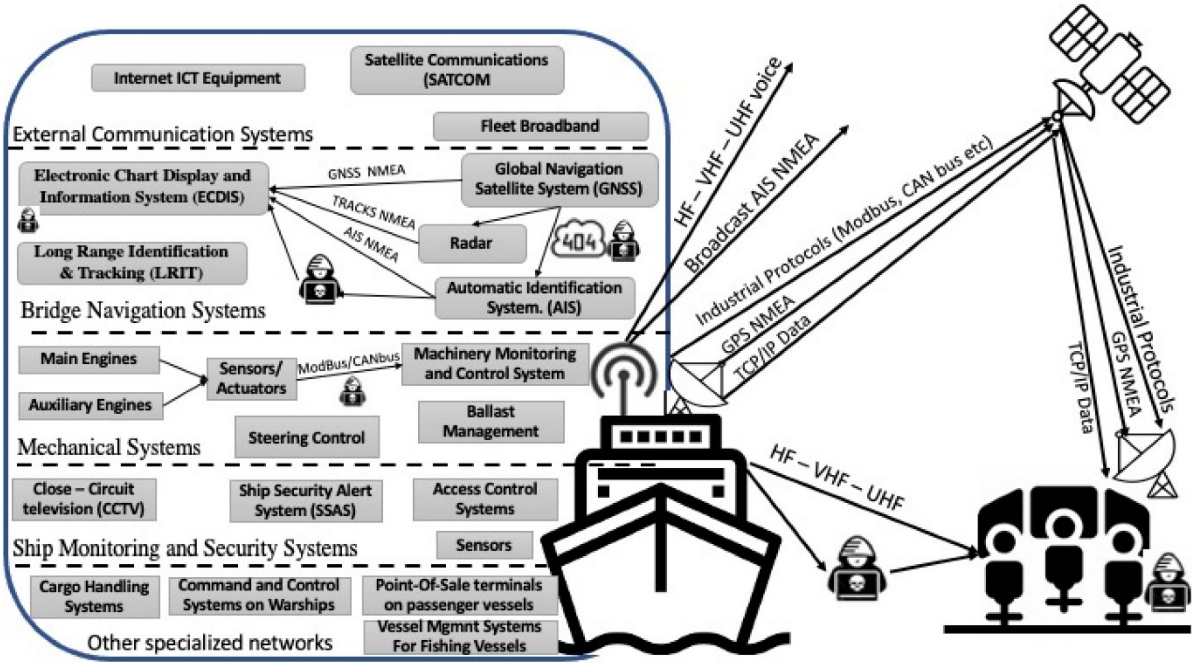

Figure 24 - Maritime assets in cyberspace. Potamos et al. [109](p. 6).

3. Study objectives

3.1. Overall objective

This thesis investigates the key factors influencing the cybersecurity posture and maintainability of Operational Technology (OT) systems within transportation sector fleets. The study aims to identify the specific cybersecurity requirements and considerations that organizations must address to mitigate threats associated during the integration of these systems into Onboard Industrial Control Systems (OICS) while relying on centralized security support for remote and centralized management.

While the focus is given on the Transport sector, these weaknesses are common to other onboard control systems like those of Aerospace and Military sectors.

3.2. Specific objectives

The following are the specific objectives of this study:

- Describe factors affecting SL-T estimation in the OICS context.
- Discuss the current trend of threat actors targeting OT/ICS.
- Depending on the required IEC 62443 SL-C requirements, analyze the mandatory and recommended requirements of the standard requesting LSSS functions for security and fleet management.
- Propose to reduce the SL-C of a critical requirement for the OICS context. (Annex A)
- Propose a hybrid LSSS design approach tailored to the unique challenges of OICS context accompanied by design implementation guidance from NIST SP 800-53 controls and other relevant references.
- Evaluate the benefits of the hybrid design approach in preventing security incidents in LSSS functions.

4. Methodology

The main goal of this methodology is to identify the factors impacting the SL-T estimation on an OICS context and to list the requirements and additional considerations to be injected during a security risk assessment process. While these considerations are based in IEC 62443-3-2 [49], these could be added into other of risk assessments processes like NIST 800-30r1 [73]). The steps followed are:

- Described the assumptions needed.
- Describe the factors impacting the SL-T estimation needed to protect OICS and how they affect the need for LSSS and its design (refer to chapter 2.2.3 for OICS context explanation and 2.2.4 for a description of LSSS fleet management and security purposes).
- List the IEC 62443 requirements needed to centrally manage a fleet of OICS with LSSS (refer to chapter 2.3.5.1 for an IEC 62443 introduction) based in the SL-C needed by the OICS.
- Identify specific considerations when implementing a Hybrid design for the LSSS in OICS context.

4.1. Assumptions

4.1.1. Standard reference

Any cybersecurity system design should be based on well-founded and recognized cybersecurity standards and guidelines. While the final choice and the number of references may depend on applicable country regulations and sector-specific directives and guidelines, the proposed methodology intends to be integrated during the cybersecurity design process following IEC 62443-3-2 [49]. The parts IEC 62443-3-3 [7] and IEC 62443-4-2 [70] will be used when identifying the impacted system and product requirements in which the use of a LSSS is either mandated by a given IEC 62443 SL or, in the case it is not mandated, strongly recommended for security awareness and cost-reduction fleet management purposes (refer to chapter 2.2.4 for a description on these considerations).

Finally, it will be used NIST SP 800-53 Rev.5 [29] for complementary guidance on requirements derived from directions taken from NIST SP 800-82r3 [28] and NIST 800-160 Vol. 2 [9] that the reader may consider convenient to enhance the proposed hybrid design approach in chapter 4.4.

4.1.2. Criticality of OICS

For this methodology, it will be assumed the criticality of OICS as High and having a High Impact in organizations. The rationale has been already discussed in chapter 2.2.3 where we presented how OICS falls into NIST "High-Value Asset" definition [9](p. 63) due to the need to protect from "High Impact" threats [28] and the need to protect from threat actors willing to harm to the nation [73] (p. H-2) like Criminal organizations backed by Nation-state groups in certain countries.

4.2. Security Level Target estimation

IEC 62443-3-2 establishes in the security risk assessment "*ZCR 5.6: Determine SL-T*" clause that "There is no prescribed method for establishing a SL-T. Some organizations chose to establish SL-T based upon the difference between the unmitigated cyber security risk and tolerable risk. Whereas others elect to establish SL-T based on the SL definitions provided in Annex A of this document […]"[49](p. 19).

We saw in chapter 2.2 the specificities of OICS influencing the SL needed. They could be summarized in the following three main factors affecting the SL-T estimation (see Figure 13):

- Threat actors to protect from in chapter 4.2.1. (Additionally, given the current threat actor trends, in Annex A, a discussion about "Could IEC 62443 SL-T=3 be enough for Transport OICS?" is opened when considering current IEC 62443 SL definitions and SL-T estimations from Transport sector and SL definitions.)
- Physical Protection discussed in chapter 4.2.2.
- Connectivity (with LSSS) already presented in chapter 2.2.4.

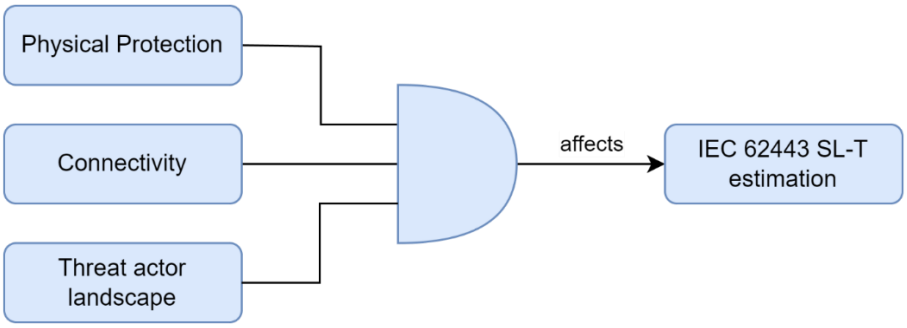

Figure 25 - Characteristics affecting SL-T estimation of an OICS.

Finally, it is illustrated with a diagram where these factors can be introduced in the SL-T estimation workflow.

4.2.1. Threat actor landscape

As described in chapter 2.3.5.1, performing a threat intelligence exercise evaluating threat actor skills, capabilities and motivation are necessary step to correctly estimate the required IEC 62443 SL to be implemented in a system or component. The "*Guide for Conducting Risk Assessments*" NIST SP 800-30r1 [73](Appendix D), proposes guidance on the necessary steps to categorize threat actors based in their *Intent, Capability* and *Targeting*.

A summary in common threat actors is given by Strohmeier et al. [71](p. 227) (see Figure 26).

Threat Agent	Capabilities	Hardware / Cost	Systems of Interest
Passive Observers	Eavesdropping, use of website & mobile apps.	Internet access, $10 SDR receiver stick	ADS-B, Mode S
Script Kiddie / Hobbyist	Eavesdropping, replay attacks, denial of service.	COTS SDR transmitter, $300-$2,000.	ADS-B, Mode S
Cyber Crime	Resources for large-scale operations with sophisticated transponders.	Directional antennas, small UAVs with SDR transmitters, $5,000-$10,000.	ADS-B, Mode S
Cyber Terrorism	Resources for specific high-impact operations, though usually on a limited scale	As with cyber crime but potentially on a smaller, more targeted scale.	ADS-B, TCAS, Mode S
Nation State	Anything physically and computationally possible.	Military-grade radio equipment, capability for electronic warfare.	Any ATC system

Figure 26 - Attacker capabilities overview. Strohmeier et al.[71](p. 227).

While this category has been done in the framework of Aviation, it is based in NIST taxonomy and the definition for common actors is in line with railway industry threat actor landscape considered by European Shift2Rail JU in chapter 2.4.2 and the Maritime sector discussed in 2.3.3. In Shift2Rail working group it was selected a "worst-case threat actor" as Criminal Organization, corresponding to the need to protect at least from IEC 62443 SL 3 actors. As mentioned in chapter 4.1.2 and further analyzed in Annex A, it is more and more common having Criminal Organizations backed by a Nation-state group.

4.2.2. Physical protection as additional layer

Another question intrinsic to OICS and needing special importance is the effectiveness of physical security as an actual layer of defense in our context or not.

Certain organizations strongly insist that applying physical "compensating countermeasures" (formal definition given below) to impede access to the OICS, the SL-C to be implemented in the asset can be reduced, and thus the implicit development costs. Such statement is certainly true in typical "fixed" Critical Infrastructure / OT (and IT) environments where having a *human-in-the-loop* is common practice, but not in a moving ICS sometimes left in poorly or not guarded locations and without connectivity to receive security alerts.

OT assets need to be contextualized and all types cannot be considered with the same **generic** physical protection. For example, physical security in civil aviation (commonly 24-hours CCTV monitored fenced airport perimeters and guarded with guns), is different compared to road vehicles or railway sector (usually isolated yards, siding tracks, halt stops or poorly surveyed stations). APTA depicted the potential attack points on yard and streets in its White Paper regarding the securitization of systems in bus vehicles (see Figure 13). While there are always exceptions and specific contexts where an organization may operate in landing fields or airstrips, small aircraft are still considered an OICS with High impact threats.

In the IT world, there exist recognized methods such as the time-based security model proposed by Schwartau in 1999 [50], which relies on complex IT infrastructures and organizational contingency / response plans to detect the attacks and defend even before it succeeds, but this kind of infrastructure with human-dependent procedures are inapplicable to onboard and offline ICS.

Referencing specialized literature, Smith, C. and Brooks, D. states that physical security also depends on the type of intruders when saying that "Effective and well-designed physical security measures, in conjunction with an appropriate security plan, will deter an opportunist intruder. However, in the case of a determined intruder, these physical security components and measures will only serve as detection, delay, and response layers, as it is considered that with sufficient time and resources any barrier can be breached. [94](p. 105). Ackerman, P. dedicates a chapter to Physical ICS security of its "Industrial Cybersecurity" book where also provides steps to perform an efficient physical ICS security[95](pp. 219-231), however all of them are mainly applicable to the percentage (variable between transport sectors) of OICS that can be qualified as "high" physical security which corresponds to classical OT infrastructures (fixed plants). Ackerman's chapter suggestions, when applicable to OICS context, will merely serve as a deterrence for low/mid motivated attackers, and options like installing expensive robust cabinets with sophisticated authentication mechanisms, when considered in a fleet of hundreds or thousands of assets (see Table 1 for an estimation of the range of fleet size per organization), it will be rarely an option for most of Transportation organization.

	Fleet size (in units)	Physical Protection level (average)
Railway	100-10000 [89]	Low (yards and depots)
Road vehicles	100-10000 [90] (buses only)	Low (parking lots)
Maritime	10-1000 [91]	Medium (Freight vessels and ports)
Aviation	100-1000 [92]	High (commercial airports)

Table 1 - Estimation (average) of physical protection level and fleet size per organization and transport sector.

Entering in the standardization realm, IEC 62443-3-2 mandates in "ZCR 5.4: Determine unmitigated likelihood", that it needs to be considered "[…] countermeasures that are inherent to IACS components and any non-cyber independent protection layers (IPLs) such as physical security, mechanical safeguards […]" IEC 62443-3-2 [49](p. 19). Now, when looking at the definition given by IEC 62443 of a compensating countermeasure, we can also deduce that

for an attacker sufficiently motivated, physical security is a countermeasure easy to bypass in OICS context. "Compensating countermeasure" definition by IEC 62443:

- "(component-level): locked cabinet around a controller that doesn't have sufficient cyber access control countermeasures.
- (control system/zone-level): physical access control (guards, gates and guns) to protect a control room to restrict access to a group of known personnel to compensate for the technical requirement for personnel to be uniquely identified by the IACS;" [7](p. 16).

Analyzing this definition, it can be seen the strong influence of stationary ICS context. At component level, any attacker in an isolated environment is most probably able to circumvent a locked cabinet, especially if common square or triangle keys have been used (you may take a look on the next train trip for those). At control system/zone-level, depending on the OICS, they are rarely between "gates" (despite exceptions as seen before), but it is rarely the case for trains or buses (easily tagged or infringed) and vessels. Having a human guarding with guns is not possible for a whole fleet, and certainly not in locations like desert mines, isolated stations, certain ports or airstrip aerodromes.

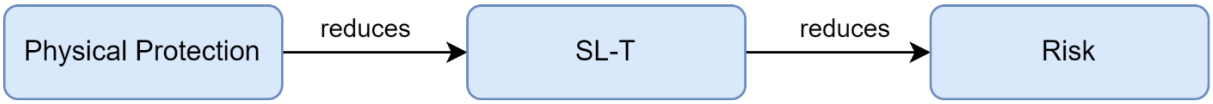

Figure 27 – Generic physical protection impact in SL-T estimation (less effective in OICS context).

As examined, physical protection is an important measure to reduce the SL-T needed in an asset (see in Figure 27 for generic impact), but the characteristics of OICS context reduces considerably the effect of it and needs to be taken in consideration when calculating the likelihood. The OICS context directly implies that embedded security capabilities (SL-C) on OICS need to be increased for any non-highly protected (with human-in-the-loop and continuously surveyed) OICS physical environment. ISASecure itself confirms that "SL1 components can protect from casual or coincidental compromise of the component but **contribute little protection from intentional compromise**. With more focus today on the security of industrial control systems, and with data indicating that these systems are becoming targets […]" [98](p. 22).

Therefore, considering the threat actor landscape of Critical Infrastructure / OT organizations, it can be stated that Physical Protection has a very limited effect in most OICS except in civil aviation. Efficient physical security requires of organizational, technical and human means, and this is not possible in OICS context due to non-connected / shutdown / isolated status with no trusted human-in-the-loop, resulting in a matter of time and right tools to bypass this layer. Nevertheless, and regardless of the ultimate efficiency against worst-case threat actors, physical protection is a necessary defense-in-depth layer and a mandatory stage during likelihood assessment of threats. However, during this calculation, as discussed, it should be taken into account that physical measures are not as effective as in common stationary ICS against worst-case threat actors considered for OICS (see 4.2.1 for threat actor landscape).

4.2.3. Connectivity (for LSSS functions)

As mentioned in chapter 2.2.4, connectivity is important in OICS for several reasons:

- Increased security awareness of the OICS fleet via continuous monitoring of security events.
- Convenient centralized credentials (for example, user accounts and certificates) of the fleet.
- Mitigation or increased surveillance on time-dependent threats (UTC time spoofing).

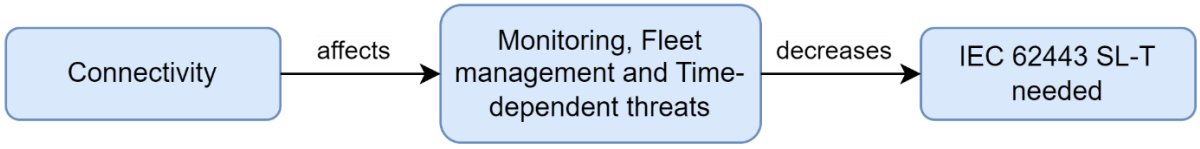

Figure 28 - Impact of Connectivity in OICS in SL-T estimation

As mentioned, with connectivity, LSSS services are not only useful for fleet management but also for security through continuous monitoring. A more detailed description is provided in the chapter on LSSS (2.2.4) and depicted in Figure 9. Also, fleet size is important when evaluating the need for centralized management of the OICS or building/increasing the network infrastructure to facilitate it. In any case, seeing the average cost of OT attacks and the increase in costs if maintainers need to go to each OICS to update their credentials when

an employee is leaving the company, the investment in a centralized management is easily justified.

To summarize the impact of connectivity in the OICS context: the shorter blind periods an OICS has, the fewer security requirements are needed. Figure 28 and Figure 29 illustrate how connectivity affects the SL-T estimation. Therefore, organizations aiming for centralized fleet management (Access, Monitoring and SW Repository LSSS functions) and looking to reduce security implementation costs in their OICS, can achieve this by ensuring better availability for LSSS services.

4.2.4. SL-T estimation workflow

This chapter's goal is to present the workflow depicted in Figure 30 as a summary on how the SL-T estimation is impacted by the different factors described in this methodology. The SL-T estimation should not be reduced to such workflow, its unique purpose is to illustrate when considerations introduced in our methodology influence the process of design and evaluation of the SL-T. Following steps ZCR 5.1 to ZCR 5.6 corresponding to Detailed Risk Assessment process defined by IEC 62443-3-2 [49](pp. 16-22) is always advised.

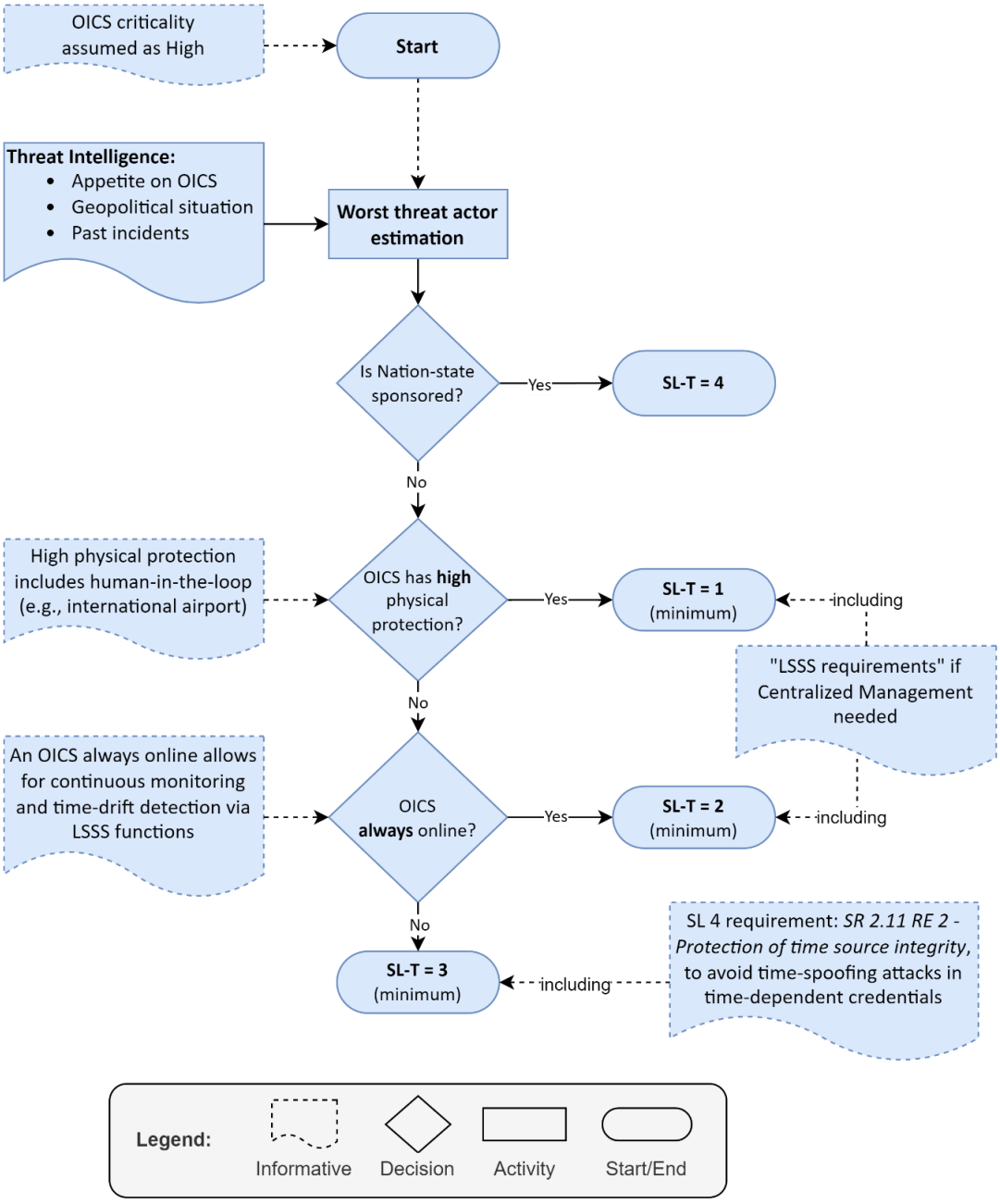

Figure 29 - Workflow for OICS SL-T estimation consideration.

4.3.IEC 62443 requirements and recommendations for LSSS

The goal of this chapter comprises the following items:

- Provide a list of IEC 62443-3-3 [7] (and 4-2 [70] specific CRs not similar to those of 3-3) requirements per SL-C where the use of a LSSS function is strongly recommended **(R)** for centralized fleet management purposes or Mandatory **(M)**. (In addition, in Annex A it is discussed why an SL-C 4 requirement like IEC 62443-3-3 "SR 2.11 – Protection of time source integrity" should be implemented starting from SL-C 1 in OICS context.

As described in chapter 2.2.4 (also see Figure 8), LSSS are imposed either by a given IEC 62443 SL-C requirement or when an organization wants to ease the management of security functions in a fleet regardless of the SL-C needed. To give a concrete example: The requirement "SR 1.5 – Authenticator management" (Table 2) is associated to a design estimated to have SL-C = 1. While the standard does not impose a centralized service like AUTH LSSS for managing authenticators, we strongly recommend (R in the table) its use in the context of an OICS fleet for obvious reasons (refer to chapter 2.2.4 for a rationale on LSSS usage and its security advantages). Guidance on LSSS hybrid design for OICS context is given in the following chapter (4.4).

N.B.: As mentioned in chapter 2.2.4, for the purpose of this study, it is assumed that the data hosted in SW REPO centralized service is authentic and pushed for deployment by a trusted user through a secure remote interface able to preserve its confidentiality, integrity and authenticity.

4.3.1. SL-C = 1 requirements related to LSSS

The requirements suggesting the use of LSSS for a SL-C = 1 can be seen in Table 2.

IEC 62443-3-3 and/or 4-2 requirement	AUTH	TIME	MONITORING	SW REPO
SR 1.1 – Human user identification and authentication	R			
SR 1.3 – Account management	R			
SR 1.4 – Identifier management	R			
SR 1.5 – Authenticator management	R			
SR 1.6 – Wireless access management	R			
SR 2.8 – Auditable events			R	
SR 2.10 – Response to audit processing failures			M	
SR 3.2 – Malicious code protection				R
EDR 3.10 – Support for updates (at least non-safety part)				R

Table 2 - SL-C = 1 requirements needing LSSS for appropriate fleet management.

These SL-C=1 aim to protect from casual or coincidental violations [7](p. 73). by authenticating humans and wireless devices, registering events, reporting logging service failures, protecting from malicious code and supporting updates.

See chapter 2.2.4.1 for related threats and 4.4 for implementation recommendations.

4.3.1.1. Mandatory (M) requirements needing a LSSS

At this level, the standard only forces to alert personnel when there is a loss or failure on an essential services or functions supporting audit processing.

4.3.1.2. Recommended (R) requirements needing a LSSS

With the recommended requirements in the list integrated with AUTH, MONITORING and SW REPO LSSS, will keep the fleet with updated authenticators and software, reporting intrusion

attempts in a timely and centralized way and critically reducing maintenance costs in a fleet of hundreds or thousands of assets.

4.3.2. SL-C = 2 requirements related to LSSS

The requirements suggesting the use of LSSS for a SL-C = 2 are those selected for previous SL-C levels + the following requirements listed in Table 3.

IEC 62443-3-3 and/or 4-2 requirement	AUTH	TIME	MONITORING	SW REPO
SR 1.1 RE 1 – Unique identification and authentication (Human Users)	R			
SR 1.2 – Software process and device identification and authentication	R			
SR 1.6 RE 1 – Unique identification and authentication (Wireless entities)	R			
SR 1.8 – Public key infrastructure certificates	M			
SR 1.9 – Strength of public key authentication	R	R		
SR 2.11 – Timestamps		R		
EDR 3.10 RE 1 – Update authenticity and integrity (Embedded devices)		R		R
EDR 3.12 – Provisioning product supplier roots of trust (Embedded Devices)	R			
EDR 3.13 – Provisioning asset owner roots of trust (Embedded Devices)	R			
EDR 3.14 RE 1 – Authenticity of the boot process (Embedded Devices)		R		
SR 6.2 – Continuous monitoring			M	
SR 7.8 – Control system component inventory			R	

Table 3 – SL-C = 2 requirements needing LSSS for appropriate fleet management

A SL-C=2 aims to protect from intentional violations using simple means, low resources and motivation and generic skills. [7](p. 73).

See chapter 2.2.4.1 for related threats and 4.4 for implementation recommendations.

4.3.2.1. Mandatory (M) requirements needing a LSSS

At this level, there are only 2 mandatory requirements. These can be deduced when reading the rationale and supplemental guidance of the standard for those requirements. They imply AUTH (PKI) and MONITORING (Log Collector + SIEM) LSSS components for PKI-based authenticators management and continuous monitoring of the fleet.

4.3.2.2. Recommended (R) requirements needing a LSSS

The recommended requirements in the list provide the capability to update, perform continuous monitoring and report asset inventory, manage unique (human) accounts for users, the generic accounts for processes (services) and devices, and support the use of a PKI infrastructure to help with related authenticators and verify the authenticity of related elements. Having LSSS functions like AUTH, MONITORING and TIME, facilitates the management of these functions, especially the individual human accounts, in a centralized way by allowing the OICS fleet to maintain the freshness needed on authenticators, to validate authenticity and report in a timely-manner security incident. SW REPO will help in deploying updates in a centralized manner as well.

4.3.3. SL-C = 3 requirements related to LSSS

The requirements suggesting the use of LSSS for a SL-C = 3 are those selected for previous SL-C levels + the following requirements listed in Table 4.

IEC 62443-3-3 and/or 4-2 requirement	AUTH	TIME	MONITORING	SW REPO
SR 1.2 RE 1 – Unique identification and authentication (SW process and Devices)	R			
SR 1.3 RE 1 – Unified account management	R			
SR 1.7 RE 1 – Password generation and lifetime restrictions for human users	R	R		
SR 2.1 RE 3 – Supervisor override	M			
SR 2.8 RE 1 – Centrally managed, system-wide audit trail			M	
SR 2.9 RE 1 – Warn when audit record storage capacity threshold (applies to buffering mechanism)			M	
SR 2.11 RE 1 – Internal time synchronization / System-wide time source for components (CR 2.11 RE 1)		M		
SR 2.13 RE 1 – Active monitoring			M	
SR 3.2 RE 2 – Central management and reporting for malicious code protection			M	
SR 3.4 RE 1 – Automated notification about integrity violations			M	
EDR 3.11 RE 1 – Notification of a tampering attempt (Embedded devices)			M	
SR 6.1 RE 1 – Programmatic access to audit logs / (At 4-2 level, the CR suggests sending to centralized system)			R / M	
SR 7.6 – Machine-readable reporting of current security settings			R	

Table 4 – SL-C = 3 requirements needing LSSS for appropriate fleet management

A SL-C=3 aims to protect from intentional violations using sophisticated means, moderate resources and motivation and specific ICS skills.[7](p. 73).

See chapter 2.2.4.1 for related threats and 4.4 for implementation recommendations.

4.3.3.1. Mandatory (M) requirements needing a LSSS

At this level, there are 8 mandatory requirements imposing a centralized management of security functions of the fleet. Besides supervisor overriding needing AUTH LSSS support to ease its management (could be done using an out-of-band mechanism as proposed in the hybrid design in chapter 4.4.1), remaining mandatory requirements are related to MONITORING (Log Collector + SIEM) LSSS functions components to ensure continuous monitoring and response for security incidents in a timely manner.

4.3.3.2. Recommended (R) requirements needing a LSSS

The recommended requirements in the list are related again to the capability to update and manage unique (entity-level) accounts authenticators, this time including also SW processes (services) and devices. Having LSSS functions like AUTH and TIME, facilitates the management of these functions in a centralized way by allowing the OICS fleet to maintain the freshness needed on authenticators.

4.3.4. SL-C = 4 requirements related to LSSS

The requirements suggesting the use of LSSS for a SL-C = 4 are those selected for previous SL-C levels + the following requirements listed in Table 5.

IEC 62443-3-3 and/or 4-2 requirement	AUTH	TIME	MONITORING	SW REPO
SR 1.7 RE 2 – Password lifetime restrictions for all users	R	R		
SR 2.1 RE 4 – Dual approval	*M			
SR 2.11 RE 2 – Protection of time source integrity (for System-wide time source derived from CR 2.11 RE 1)		M		
SR 3.3 RE 2 – Security functionality verification during normal operation			R	

Table 5 – SL-C = 4 requirements needing LSSS for appropriate fleet management

A SL-C=4 is the highest protection considered by IEC 62443. It aims to protect from intentional violations using sophisticated means, with extended resources, high motivation and specific ICS skills.[7](p. 73).

See chapter 2.2.4.1 for related threats and 4.4 for implementation recommendations.

4.3.4.1. Mandatory (M) requirements needing a LSSS

At this level, there are 2 mandatory requirements imposing a centralized management of security functions of the fleet. First, is the protection of the integrity of a retrieved centralized time-source. Second, the requirement 2.1 RE 4 mandates dual approval mechanism for critical actions impacting the industrial process, but this could arguably need a centralized management (marked as *M in Table 5). This kind of critical procedure, from a remote and centralized system, could be needed when an OICS has mechanism to update safety-related parts of the system, where one person would deploy the update and check its deployment (first approval) and another person connects again to perform additional checks on the system (second approval), but this may have homologation issues to be deeply analyzed.

4.3.4.2. Recommended (R) requirements needing a LSSS

The recommended requirements in the list are related again to the capability to manage (renew) individual passwords, this time including SW processes (services) and devices in addition to human passwords in the previous SL-C level. Also, it is recommended to report to the pertinent centralized MONITORING service the results of verifications performed during operation on security functions. Having the related LSSS functions will facilitate the management of these functions in a centralized way by allowing the OICS fleet to maintain the freshness needed on authenticators and report security events.

4.4. OICS hybrid design approach for LSSS

Common ICS cybersecurity requirements applies as well to OICS, but as described in chapter 2.2.3, the OICS operational context brings issues both to security resilience and fleet maintainability if the requirements imposing them have been implemented without taking into account the following considerations.

4.4.1. AUTH – LSSS hybrid design considerations

Threat examples: see chapter 2.2.4.1.

Context: After an offline period like days, weeks or months, the authenticators database listing users and devices that are allowed to access the OICS could not be up to date. This means that authenticators in the system could belong to employees or devices no longer

trusted by the organization. A hybrid design for an authentication mechanism is necessary to address the updates of authenticators database and the fallback to an offline mode without relying on connectivity with the AUTH function. AUTH function design relying in TIME-dependent data like checking an expiry date, could pose challenges as well (See chapter 4.4.2). A hybrid design taking into account this context is necessary to allow seamless account management for the whole fleet.

- **LSSS connectivity is available:**
  - Integrate an IAM to the design: After a configurable number of days, the account management system should not allow the nominal authentication of users except if the authenticators and time-dependent artefacts like CRL are into valid freshness range. This could be achieved by starting the OICS and waiting until the authenticator database checks for new updates from IAM and PKI server.
- **LSSS connectivity is not available:**
  - If the AUTH services are not reachable, implement a Zero-Trust authentication method. An example would be:
    1. The OICS is in non-connected authentication mode. Each OICS contains a list of OTPs/tokens known by a trusted administrator "TA" located in a control center or SOC. The OICS and the SOC database of OTPs/tokens per OICS is *regularly* updated when connection with LSSS exists. The organization is also aware which OICS should be in non-connected mode as per situational awareness of its fleet.
    2. The OICS first identifies the user U with local credentials, and then requests an OTP code to authenticate the user U.
    3. TA gave user U one OTP code corresponding to the OICS via an out-of-band mechanism (for example by telephone when user had GSM network).
    4. User U introduces a valid OTP/token and OICS accepts the connection.

- **Recommended and additional guidance for implementation from NIST SP 800-53 [29] controls:**
  - IA-2 – Identification and Authentication (organizational users)
    - IA-2(13) – Out-of-band
  - IA-4 – Identifier Management
  - IA-5 – Authenticator Management
    - IA-5(8) – Multiple system accounts
    - IA-5(13) – Expiration of cached authenticators
  - IA-10 – Adaptive Authentication
  - CP-13 – Alternative Security Mechanisms
  - MA-5 – Maintenance Personnel
  - MA-6 – Timely Maintenance
    - MA-6(3) – Automated Support for Predictive Maintenance
  - SC-37 – Out-of-Band Channels
  - SI-14 – Non-Persistence
- **Additional comments:**
  - When PKI-related revocation mechanisms are used for authentication mechanism, in addition to outdated human credentials seen above, *TIME*-dependent attacks like UTC spoofing also impact authentication mechanisms in OICS at startup.
  - Secure communication between the OICS and AUTH functions are obviously considered as secure (for example, through a VPN between both entities or with a TLS connection).

4.4.2. TIME – LSSS hybrid design considerations

Threat examples: see chapter 2.2.4.1.

Context: Retrieving the UTC time from an external time-source could result in an insecure or not operational condition (as a hard-fail in an authentication mechanism due to an expired certificate) due to time-spoofing. A hybrid design to provide a valid and fresh UTC time is necessary.

- **LSSS connectivity is available:**
  - Implement a secure Network Time Protocol to avoid time-spoofing: This can be achieved by implementing NTS protocol [68], which requires mutual authentication between the OICS and the TIME service. This protocol provides integrity and authenticity of the retrieved time data.
  - Define a log event reporting the synchronized time regularly. This event will increase situational awareness of the time used by the OICS to detect potential incongruencies.
- **LSSS connectivity is not available:**
  - Implement a mechanism to avoid "anti-time-backwards" by registering the last known time, as for example the using the last timestamp in log services.
  - Establish a multi-source time comparison: GNSS-based UTC time could be used as an additional time source; however, it is also the easiest signal to spoof due to its public nature.
- **Recommended and additional guidance for implementation from NIST SP 800-53 [29] controls:**
  - AU-8 – Time stamps
  - AU-12 – Audit record generation
    - AU-12 (1) – System-wide and time-correlated audit trail
  - SC-45 – System time synchronization
    - SC-45 (1) – Synchronization with authoritative time source
    - SC-45 (2) – Secondary authoritative time source

- **GNSS-based time source considerations:** If GNSS is to be used as a time-source, the NCCIC (National Cybersecurity & Communications Integration Center), published *"Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure"* to help increasing the reliability of the retrieved data. Human-in-the-loop is still recommended, especially to avoid spoofing threats dependent on GNSS position or UTC retrieval in all sectors.

4.4.3. MONITORING – LSSS hybrid design considerations

Threats: see chapter 2.2.4.1.

Context: When there is no connection between OICS and MONITORING function due to a shutdown OICS or a jammed signal, the system could have been or currently being under attack without possibility to the organization for reacting to such incident and prevent a dangerous condition.

- **LSSS connectivity is not available:**
  - Implement a reliable log mechanism able to buffer and track reception of security events and alerts by the centralized log server (MONITORING LSSS function) in Non-Volatile memories. This can be achieved by using for events and audit trail recordings libraries implementing either the open-source RELP (Reliable Event Logging Protocol) integrated in libraries like *Rsyslog* [110], or commercial solutions like Syslog-ng through the integration of "Reliable Log Transfer Protocol", which is available in the open-source library syslog-ng but in its "Premium Edition" [111]. There exist further studies implementing reliable logging protocols but are less standard [112].
  - Implement a mechanism able to alert a human-in-the-loop: In the case the connectivity is lost in a non-scheduled moment (for example, due to a jamming attack by a passenger), the MONITORING LSSS function needs to implement a mechanism in which the human-in-the-loop in the OICS can be warned. In this way, the trusted human may use out-of-band communication means to prevent the control center or SOC of a suspicious activity.

- **Recommended and additional guidance for implementation from NIST SP 800-53 [29] controls:**
  - AC-4 (7) – One-way flow mechanism (needs thorough analysis depending on operational needs)
  - AU-2 – Event logging
  - AU-5 – Response to audit logging process failures
    - AU-5 (2) – Real-time alerts

- SI-4 – System monitoring
  - SI-4 (1) – System-wide intrusion detection system
  - SI-4 (2) – Automated tools and mechanisms for real-time analysis (SIEM)
  - SI-4 (6) – System-generated alerts
  - SI-4 (7) – Automated response to suspicious events
  - SI-4 (14) – Wireless intrusion detection
- SI-7 (8) - Auditing capability for significant events
- SC-40 – Wireless link protection
  - SC-40 (1) – Electromagnetic interference

- **Additional comments:**
  - It could be used jamming attack detection solution in order to create a related security event.
  - Secure communication between the OICS and MONITORING functions are obviously considered as secure (for example, through a VPN between both entities and with an interface protected with TLS connection)

4.4.4. SW REPO – LSSS Design considerations

There has not been identified hybrid needs for SW REPO LSSS at the time besides derived designs regarding AUTH, TIME and MONITORING after deploying an update in the OICS. However, there will be contextualized the needs (for fleet management purpose) and challenges for future works.

Threats: see chapter 2.2.4.1.

Context: Not updating and deploying updates in a timely manner could open windows of opportunity to threat actors in the OICS. For this, the OICS needs to be designed in a way that allows for receiving SW updates in a secure way from a centralized SW repository, check the authenticity prior to installation and install it without human intervention. For that, a correct segregation of the OICS architecture is needed to separate safety-related (with heavy homologation/approval needs for any change) from non-safety SW.

Considerations and additional guidance during the design of an automatic SW deployment from NIST SP 800-53 [29] controls:

- Patch management
    - CM-2 – Baseline configuration
        - CM-2 (3) – Retention of previous configuration (if a new deployed version did not succeed after several trials.
    - SI-2 – Flaw remediation
        - SI-2 (5) – Automatic software and firmware updates
        - SI-2 (6) – Removal of previous version of software and firmware (this needs to be carefully planned by each organization by taking into account previous CM-2 (3) control and their particular context.
- **Additional comments:**
    - Secure communication between the OICS and SW REPO function is obviously considered as secure (for example, through a VPN between both entities and with an interface protected with TLS connection).

4.4.5. Hybrid LSSS Reference Architecture

The "LSSS reference architecture" depicted in Figure 30, it is intended to show, at a high level, the elements present in any in any hybrid reference architecture for an organization willing to have a centralized OICS fleet management by maintaining security in an OICS context. As mentioned at the beginning of chapter 4, this is to be integrated in the Zone & Conduit (Z&C) architecture defined in IEC 62443-3-2 step *ZCR 3 – "Partition the SUC into zones and conduits"* [49](p. 14), and that needs to be done for each particular context to help the SL-T estimation by also taking into account the considerations given in chapters 4.4.1 to 4.4.4.

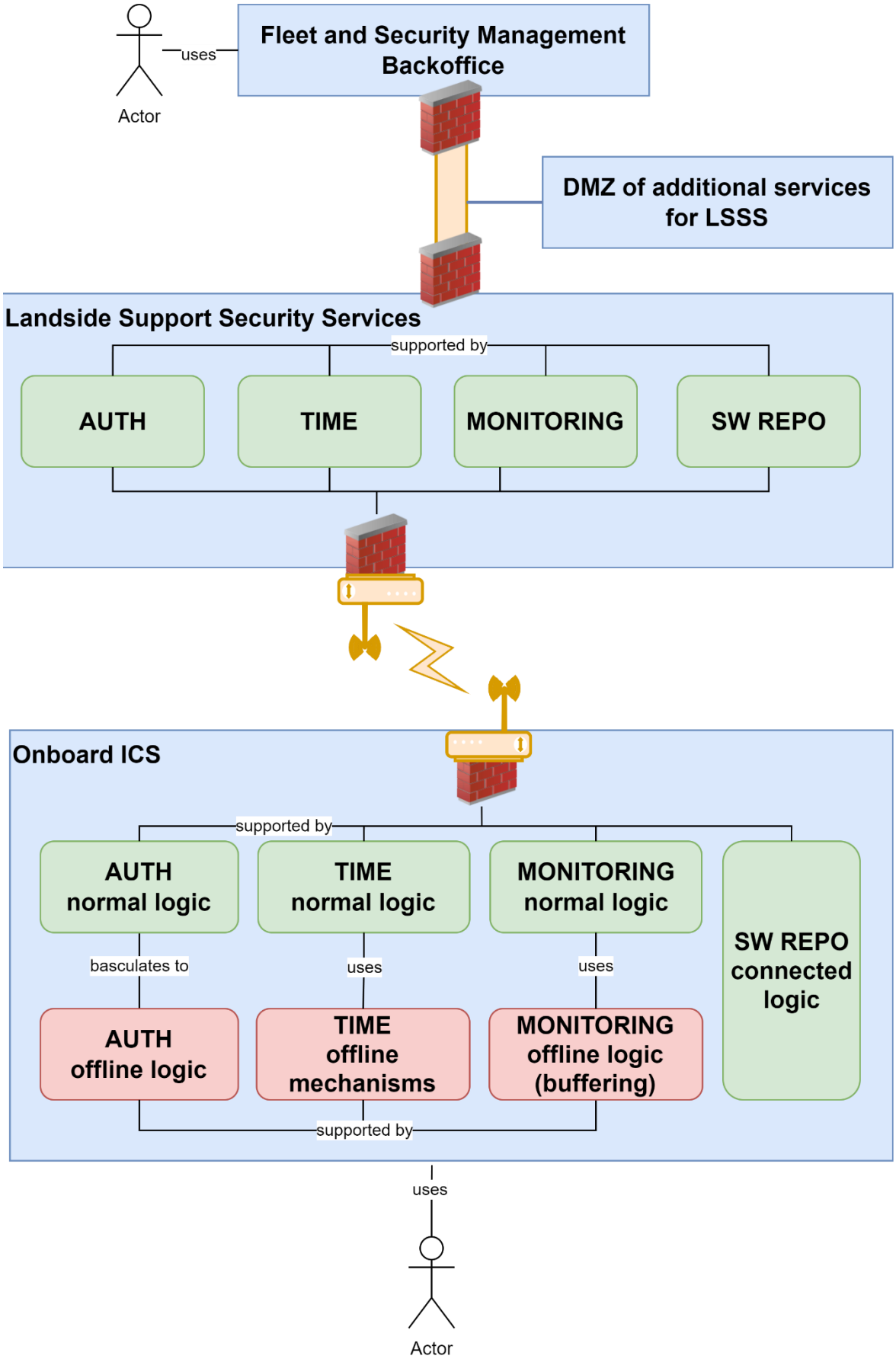

Figure 30 - Hybrid OICS reference architecture

4.5. Evaluation

Trying to evaluate the efficiency of the proposed hybrid approach methodology entails many challenges that are impossible to match all the specificities, maturity and resources of organizations willing to implement this methodology. However, besides making some estimations based on very specific data, it can be summarized the factors to take into account for such evaluation by each organization.

4.5.1. Factors influencing the evaluation costs

- Number of OICS to manage in the fleet.
- The number of components to manage in each OICS vehicle.
- Maintainability cost of needing to go to each OICS (number of people, permissions to access the vehicle, unmounting time to access the components, etc.).
- The SL-T required in the OICS based in the factors mentioned in chapter 4.2.
- Maturity in cybersecurity by engineering teams to develop the hybrid approach mechanism proposed.
- The cost of implementing the LSSS based on the SL-T and fleet management needs.
- The cost of a security incident in a safety-critical asset.

4.5.2. Use case without AUTH LSSS Hybrid design approach

The use case will be based on OICS in the railway sector needing to update the authenticators database of a whole fleet of trains.

A. Turnover of maintenance staff (1 leaving and new employee) having access to OICS = **6 months** (twice per year).
   - Remark: this is, every 6 months, the authenticator database is obsolete and needs to be updated to avoid a cyber incident.

B. Lifespan of an OICS = **20 years**.

C. **No. of OICS vehicles (trains) in the fleet: 400** (average based on Table 1).
   - **No. of OT assets in the fleet:** 5 x 400 = 2000. (5 for simplification purposes).

D. **Maintainability cost** intervention per train: 8 hours with a maintainer = **$2000.**
   - Remark: Considering specific HSE precautions, moving vehicle to yard, unmounting carenage, electrifying the vehicle, etc.)

E. **SL-T estimated to 2** (to highlight the importance of such architecture in a "best-case scenario"). Corresponding to implement "AUTH" requirements of Table 3.

F. **Fixed costs of implementing AUTH LSSS hybrid approach for SL-T=2** in 4.4.1 = ≈$2,000,000 = **$2M**.

- Remark: takes into account the fixed cost of developing the function + the needed LSSS equipment (IAM, PKI and maintenance cost) as fixed costs + risks.

G. Maturity of engineering team in cybersecurity to develop a Secure-by-design hybrid mechanism: **High = 1.0** (for simplification purpose and estimate with "best-case scenario" for an organization).

- Remark: For this study purpose, we will estimate multipliers to the estimated cost of the development with: High=1.0 (no additional cost), Medium= 1.5 (+50% of effort) and Low=2.0 (+100% of cost effort needed to catch up on Secure-by-design techniques).

H. **Operational costs of AUTH LSSS per year** = 24h available person as 63.50$ hour = $1524 x 365 day = $556.260 (round to $560,000) per year.

- Remark: cost may vary depending on where the 24h LSSS support service is located, it has been estimated to 63.50$ hour from [2](p. 17) for simplicity.

I. **Average cost of a cybersecurity incident in OT/ICS industry** = **$2,989,550** [2](p. 3).

- Remark: For the purpose of this thesis, it has been used a report calculating the cost of the incident and its response of an OT/ICS incident (the "pure" cost counting only replacement, downtime, legal and regulatory fines is little over $2M). The average is calculated in the OT/ICS industry in a generic way, not Transport-specific, and where 63% of respondents experienced an OT/ICS attack in the past two years from the date of the report.

4.5.2.1. Results of use case

Taking into account that the incident in our use case scenario has been performed due to an attack in an obsolete authenticator database of 1 to several OICS vehicles, we can calculate the cost of avoiding it with and without a Hybrid AUTH design in place.

Cost to avoid an attack without AUTH Hybrid design:

- Cost per year of maintenance interventions for keeping an updated authenticators database in a fleet of 400 trains: 2A x C x D = 1 x 400 x $2000 = $1,600,000 / year x 20 years =

$32M / lifespan (20 years).

Cost with AUTH Hybrid design:

- Fixed costs (F x G) + Operational costs per year (B x H) = $2M + (20 x $560,000) =

$13,2M / lifespan (20 years).

It can be seen, how only with the maintainability costs associated to maintain a fleet without our design is roughly 2.5 times more expensive than investing in an AUTH LSSS Hybrid design to maintain and secure a fleet of 400 vehicles, without considering the cost (when not having our design) of a potential breach in the system due to an obsolete authenticators database.

Moreover, the probability of having a cybersecurity incident in the future as per Ponemon report [2] is of 63% X 2 (years) = 33% / year, however these percentages are global to an organization, not specifically on their OICS assets. Nevertheless, the fact of having a fleet of hundreds / thousands of assets and the kind of threat actors from which OT/ICS needs to be protected 4.2.1 may increase the probability. As always, by the nature of risk definition itself, it is hard to quantify in an empiric way, but the increasing numbers on security incidents and the current trends on threat actor landscape shows evidence of the need on enhancing the cybersecurity in OICS context.

4.5.3. Final words in evaluation

Even if the recommended requirements are general and flexible enough to be adapted to any organization in the transport sector needing to secure and manage a fleet, the final cost for implementation of our proposal depends on the varying levels of organizational maturity in cybersecurity and the specific context of potential cybersecurity risks. The lack of detailed knowledge regarding organizations makes challenging to quantify the implementation costs. Any associated costs are primarily incremental, as many organizations may have already implemented some security controls prior to our hybrid design approach and be aligned with industry standards like IEC 62443 minimizing costs of adaptation. In any case, entities that do

not adopt these requirements face higher cybersecurity risks, potentially leading to significant safety impact and associated costs, thus highlighting the importance of proactive cybersecurity practices to prevent future liabilities.

5. Conclusions and Future Work

5.1.1. Conclusions

In this thesis, first, we presented the uniqueness of Onboard ICS (OICS) context regarding cybersecurity challenges in the Transport sector and the use of centralized landside support shared services (LSSS) to support both cybersecurity functions and maintainability compared to classical OT/ICS fixed infrastructure and the threats associated to classical LSSS design versus OICS context showing the need for a hybrid design. Next, we analyzed the current applicable cybersecurity normative and drew attention to a lack of consideration of the OICS context regarding cybersecurity and fleet management. We finished our background on the topic offering an overview of current threats to each transportation sector and reference architecture of OICS.

Our methodology proposed is based in IEC 62443 [49] as standard framework to develop a hybrid design of LSSS function. For that, we first described the factors affecting a SL-T workflow estimation on the OICS context and how integrate them, being these the following:

- The threat actor landscape, challenging the current security level (SL) definition considering new trends on threat actors.
- The physical protection has a defence-in-depth layer, showing proof on how has little effect in an OICS context
- The connectivity with LSSS function, and how it plays a big role in cyber resiliency of OICS.

Then, we analyzed which are the mandatory and recommended IEC 62443 requirements needing to integrate a LSSS function for both security and fleet management purposes, depending on the SL-C needed and we proposed to descend drastically the SL-C of a critical requirement for OICS context. Finally, based in the presented LSSS, we proposed a hybrid LSSS design approach for OICS while providing additional guidance from NIST SP 800-53 [29] controls and potential technical choices and references for inspiration.

Finally, we evaluated, without even the need for a worst-case scenario, how an organization can benefit from our design to avoid a security incident with and without implementing our hybrid design approach in one of the LSSS functions. Our methodology provided a reduction of 2.5 times in the cost of maintaining a fleet secure. It is clear how our design offers a major increase in maintainability while conserving the security robustness needed for the SL-T estimated.

5.1.2. Future work

The study performed in this master thesis can be improved with the following work streams:

- Evaluate further the impact of presented factors in a defence-in-depth strategy to enhance cyber resilience like the one proposed by NIST SP 800-160.
- In-deep analysis of the OICS context for each Transport sector to confront the assumptions given for connectivity for fleet management.
- Investigate the impact of human-in-the-loop as possible countermeasure and its impact in the SL-T estimation.
- Explore further the Hybrid design to follow a ZTA for Onboard ICS by following NIST SP 800-82r3 [28](p.75) ZTA principles for OT.
- Investigate this approach on driverless OICS cybersecurity context like drones and UAVs.
- Perform a detailed risk assessment on OICS per transport sector using MITRE ATT&CK for ICS framework to further identify threats in the context of an OICS hybrid approach [113].
- Further analyze the adaptation and identification of controls related to the 14 techniques when applying the cyber resiliency engineering framework proposed by NIST SP 800-160 Vol. 2, Rev. 1 [9](p. 13).

REFERENCES

[1] Buffet, W. (May 6, 2017). *BUFFETT: This is 'the number one problem with mankind'* [Annual stakeholders meeting]. Business Insider. Available: https://www.businessinsider.com/warren-buffett-cybersecurity-berkshire-hathaway-meeting-2017-5.

[2] Ponemon Institute. (November 2021). *The 2021 state of industrial cybersecurity: The risks created by the cultural divide between the IT & OT teams*. Ponemon Institute. Available: https://hub.dragos.com/hubfs/Reports/2021-Ponemon-Institute-State-of-Industrial-Cybersecurity-Report.pdf?hsLang=en.

[3] International Electrotechnical Commission. (2009). *IEC TS 62443-1-1:2009*. Technical Specification. Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models. Available: https://webstore.iec.ch/publication/7029.

[4] Directive (EU) 2022/2555. *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).* Available: https://eur-lex.europa.eu/eli/dir/2022/2555.

[5] Regulation (EU) 2019/1020. *Proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (Cyber Resilient Act)*. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454.

[6] ENISA. (February 2022). *Zoning and conduits for railways*. European Rail ISAC. Available: https://www.enisa.europa.eu/publications/zoning-and-conduits-for-railways.

[7] International Electrotechnical Commission. (2013). *IEC 62443-3-3:2013*, *International Standard. Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels*, *Edition 1.0*. Available: https://webstore.iec.ch/publication/7033.

[8] National Institute of Standards and Technology. (August 31, 2012*). Roadmap to Secure Control Systems in the Transportation Sector* (p. 5). Available: https://www.cisa.gov/sites/default/files/documents/TransportationRoadmap20120831.pdf.

[9] National Institute of Standards and Technology. (December 2021). *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*. NIST Special Publication 800-160, Volume 2, Revision 1. Available: https://doi.org/10.6028/NIST.SP.800-160v2r1.

[10] American Public Transportation Association. (May 2023). *Operational Technology Cybersecurity Maturity Framework (OT-CMF) Overview Part 1: Guidance in Maturing an OT Cybersecurity Program*. APTA SS-CCS-RP-006-23. Control and Communications Security Working Group. Available: https://www.apta.com/research-technical-resources/standards/security/apta-ss-ccs-rp-006-23/.

[11] Hasratyan et al. (2020) *ECSO Transportation Sector Report, Cyber security for road, rail, air, and sea. WG3 I Sectoral Demand.* European Cyber Security Organisation (ECSO), 59p. Available: https://hal.science/hal-02531033.

[12] Parker, D. B. (1998). *Fighting computer crime: A new framework for protecting information*. Wiley.

[13] Verve Industrial Protection (2024). *The Ultimate Guide to Using IEC 62443 to Protecting OT Systems with IEC 62443*. Retrieved from https://verveindustrial.com/resources/blog/the-ultimate-guide-to-protecting-ot-systems-with-iec-62443/.

[14] National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. Available: https://doi.org/10.6028/NIST.CSWP.29.

[15] International Organization for Standardization & International Electrotechnical Commission. (2022). *ISO/IEC 27001:2022, International Standard - Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. Third edition. Available: https://webstore.iec.ch/publication/79694.

[16] Connected Cooperative Automated Mobility. (n.d.). *MODI project*. CCAM. Retrieved June 18, 2024, from https://www.ccam.eu/projects/modi/.

[17] Connected Cooperative Automated Mobility. (n.d.). *PoDIUM project*. CCAM. Retrieved June 18, 2024, from https://www.ccam.eu/projects/podium/.

[18] Rio Tinto. (n.d.). *Automation – Autonomous train*. Rio Tinto. Retrieved June 18, 2024, from https://www.riotinto.com/en/mn/about/innovation/automation.

[19] International Association of Public Transport. (2023). *Automated metros*. UITP. Retrieved June 18, 2024, from https://www.uitp.org/topics/automated-metros/.

[20] Daza Pastrana et al. (2017). *X2RAIL-1, Deliverable 8.1 - Selection of the "Secure-By-Design" standard*. Shift2Rail Joint-Undertaking, Innovation Programme 2, TD 2.11. Available:

https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5b7441095&appId=PPGMS.

[21] Fouques et al. (May 2024). *Cybersecurity Black Box made easy cybersecurity norms and standards that are applicable to railways*. Alstom. For Signal und Draht [p. 43-51] magazine.

[22] CENELEC. (2021). *CLC/TS 50701:2021 – Railway applications – Cybersecurity*. Technical Specification. Available: https://tienda.aenor.com/norma-une-clc-ts-50701-2021-n0066300.

[23] CENELEC. (2017). *EN 50126-1:2017 – Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process.* Standard. Available: https://connect.snv.ch/en/sn-en-50126-1-2017.

[24] European Union Agency for Railways. (2009). *Common Safety Method for Risk Evaluation and Assessment (CSM-RA)*. Available: https://www.era.europa.eu/domains/common-safety-methods/risk-evaluation-assessment-csm_en.

[25] International Electrotechnical Commission. (n.d.). *IEC TC9/PT 63452 – Railway applications – Cybersecurity*. Available: https://www.iec.ch/dyn/www/f?p=103:14:405172316768605::::FSP_ORG_ID:28802.

[26] American Public Transportation Association. (n.d.). *About APTA*. Retrieved June 22 from https://www.apta.com/about/.

[27] American Public Transportation Association. (2016). *Securing Control and Communications Systems in Rail Transit Environments – Part IIIb: Protecting the Operationally Critical Security Zone*. APTA SS-CCS-004-16. Control and Communications Security Working Group. Available: https://www.apta.com/research-technical-resources/standards/security/apta-ss-ccs-rp-004-16/.

[28] National Institute of Standards and Technology. (September 2023). NIST Special Publication 800-82, Revision 3 – *Guide to Operational Technology (OT) Security.* NIST SP 800-82r3. Available: https://doi.org/10.6028/NIST.SP.800-82r3.

[29] National Institute of Standards and Technology. (September 2020). *NIST SP 800-53, REV. 5 – Security and privacy controls for information systems and organizations*. Available: https://doi.org/10.6028/NIST.SP.800-53r5.

[30] Cambridge University Press. (n.d.). Seguridad. In *Cambridge Spanish-English dictionary*. Retrieved June 22, 2024, from https://dictionary.cambridge.org/us/dictionary/spanish-english/seguridad.

[31] International Association for Classification Societies. (June 2023). *IACS UR E22, Computer-based systems – Revision 3*. IACS Unified Requirements. Available: https://iacs.org.uk/resolutions/unified-requirements/ur-e/ur-e22-rev2-cln-2.

[32] International Association for Classification Societies. (November 2023). *IACS UR E26 Cyber resilience of ships – Revision 1*. IACS Unified Requirements. Available: https://iacs.org.uk/resolutions/unified-requirements/ur-e/ur-e26-new.

[33] International Association for Classification Societies. (September 2023). *IACS UR E27, Cyber resilience of on-board systems and equipment – Revision 1*. IACS Unified Requirements. Available: https://iacs.org.uk/resolutions/unified-requirements/ur-e/ur-e27-rev1.

[34] International Association for Classification Societies. (April 2022). *IACS Rec 166 – Recommendation on Cyber Resilience – New Corr.2*. IACS Recommendations. Available: https://iacs.org.uk/resolutions/161-180/rec-166-new-corr2-cln/rec-166-new-corr2-cln.

[35] Regulation (EU) 2019/2144. *Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users.* Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R2144.

[36] Directive (EU) 2016/798. *Directive (EU) 2016/798 of the European Parliament and of the Council of 11 May 2016 on railway safety*. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0798.

[37] Regulation (EU) 2018/1139. *Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014, and Directives 2014/30/EU and 2014/53/EU, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 and Council Regulation (EEC) No 3922/91*. Available : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1139.

[38] Directive 2014/90/EU. *Directive 2014/90/EU of the European Parliament and of the Council of 23 July 2014 on marine equipment and repealing Council Directive 96/98/EC. Available:* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0090.

[39] International Air Transport Association. (n.d.). Operations, Safety & Security Certification. Retrieved June 22, 2024, from https://www.iata.org/en/services/certification/operations-safety-security/.

[40] European Railway Agency. (n.d.). *Applications for Single Safety Certificates (SSCs)*. Retrieved June 22, 2024, from https://www.era.europa.eu/domains/applicants/applications-single-safety-certificates_en.

[41] International Maritime Organization. (n.d.). *Maritime Safety*. Retrieved June 22, 2024, from https://www.imo.org/en/OurWork/Safety/Pages/default.aspx.

[42] Williams, T.J. (1994). *The Purdue Enterprise Reference Architecture*. Computers in Industry, Volume 24, Issues 2–3, pp. 141-158. Available: https://doi.org/10.1016/0166-3615(94)90017-5.

[43] Yu et al. (2023). *Security of railway control systems: A survey, research issues and challenges*. High-speed Railway, Volume 1, Issue 1, Pages 6-17. Available: https://doi.org/10.1016/j.hspr.2022.12.001.

[44] National Highway Traffic Safety Administration. (n.d.). Laws and regulations. United States Department of Transportation. Retrieved June 23, 2024, from https://www.nhtsa.gov/laws-regulations.

[45] American Public Transportation Association. (2013). *Securing Control and Communications Systems in Rail Transit Environments – Part II: Defining a Security Zone Architecture for Rail Transit and Protecting Critical Zones*. APTA SS-CCS-RP-002-13. Recommended Practice. Control and Communications Security Working Group. Available: https://www.apta.com/research-technical-resources/standards/security/apta-ss-ccs-rp-002-13/.

[46] American Public Transportation Association. (2015). *Securing Control and Communications Systems in Rail Transit Environments – Part IIIa: Attack Modeling Security Analysis White Paper*. APTA SS-CCS-WP-003-15. White Paper. Control and Communications Security Working Group. Available: https://www.apta.com/research-technical-resources/standards/security/apta-ss-ccs-wp-003-15/.

[47] American Public Transportation Association. (2010). *Securing Control and Communications Systems in Transit Environments – Part 1: Elements, Organization and Risk Assessment/Management*. APTA SS-CCS-RP-001-10. Recommended Practice. Control and

Communications Security Working Group. Available: https://www.apta.com/research-technical-resources/standards/security/apta-ss-ccs-wp-003-15/.

[48] EUROCONTROL EATM-CERT Services. (2021). *Think Paper #12 - 5 July 2021 – Aviation under attack from a wave of cybercrime.* EUROCONTROL. Available: https://www.eurocontrol.int/publication/eurocontrol-think-paper-12-aviation-under-attack-wave-cybercrime.

[49] International Electrotechnical Commission. (2020). *IEC 62443-3-2:2020, International Standard. Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design, Edition 1.0*. Available: https://webstore.iec.ch/publication/30727.

[50] Schwartau, W. (1999). *Time Based Security – Practical and Provable Methods to Protect Enterprise And Infrastructure, Networks and Nation*. Interpact Press. Available: https://winnschwartau.com/wp-content/uploads/2019/06/TimeBasedSecurity.pdf.

[51] Progoulakis et al. (December 2021). *Cyber Physical Systems Security for Maritime Assets.* J. Mar. Sci. Eng. 2021, 9, 1384. Available: https://doi.org/10.3390/jmse9121384.

[52] Ishtiaq et al. (December 2021). *Cybersecurity Vulnerabilities and Defence Techniques in Aviation Industry*. Proceedings of the 3rd International Conference on Integrated Intelligent Computing Communication & Security. Atlantis Highlights in Computer Sciences, volume 4, Pages 559-567. Available: https://doi.org/10.2991/ahis.k.210913.071.

[53] Pyzynski, M and Bacerzak, T. (2021). *Cybersecurity of the Unmanned Aircraft System (UAS)*. Journal of Intelligent & Robotic Systems (2021) 102: 35. Available: https://doi.org/10.1007/s10846-021-01399-x.

[54] Choudhary et al. (2022). *Aviation attacks based on ILS and VOR vulnerabilities.* Journal of Surveillance, Security and Safety. 3, no.2: 27-40. Available: http://dx.doi.org/10.20517/jsss.2021.17.

[55] SOCRadar. (July 2023). *Threat Landscape in the Aviation Industry for H1 of 2023*. Retrieved June 25, 2024, from https://socradar.io/threat-landscape-in-the-aviation-industry-for-h1-of-2023/.

[56] International Air Transport Association. (February 2021). *Aviation Cyber Security Guidance Material – Part 2 (Aircraft)*. IATA. Available: https://go.updates.iata.org/l/123902/idance-material-part2-aircraft/j39vh5.

[57] European Organisation for Civil Aviation Equipment. (2014). *ED-202A - Airworthiness Security Process Specification*. EUROCAE. Available: https://eshop.eurocae.net/eurocae-documents-and-reports/ed-202a/.

[58] Radio Technical Commission for Aeronautics. (2014). *DO-326A - Airworthiness Security Process Specification*. RTCA. Available: https://my.rtca.org/productdetails?id=a1B36000001IcfuEAC.

[59] European Organisation for Civil Aviation Equipment. (2018). *ED-203A - Airworthiness Security Methods and Considerations*. EUROCAE. Available: https://eshop.eurocae.net/eurocae-documents-and-reports/ed-203a/.

[60] Radio Technical Commission for Aeronautics. (2018). *DO-356A - Airworthiness Security Methods and Considerations*. RTCA. Available: https://my.rtca.org/productdetails?id=a1B36000006xdvvEAA.

[61] International Civil Aviation Organization. (December 2022). *Compilation of Cyber Security Regulations, Standards, and Guidance Applicable to Civil Aviation, Edition 4.0.* ICAO. Available: https://www.iata.org/contentassets/4c51b00fb25e4b60b38376a4935e278b/compilation-of-cyber-regs.pdf.

[62] European Organisation for Civil Aviation Equipment. (2014). *ED-204A – Information Security Guidance for Continuing Airworthiness.* EUROCAE. Available: https://eshop.eurocae.net/eurocae-documents-and-reports/ed-204a-information-security-guidance-for-continuing-airworthiness.

[63] Radio Technical Commission for Aeronautics. (2020). *DO-355A – Information Security Guidance for Continuing Airworthiness*. RTCA. Available: https://my.rtca.org/productdetails?id=a1B1R00000GshsyUAB.

[64] Zetter, K. (2015). *Feds Say That Banned Researcher Commandeered a Plane*. Wired. Available: https://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane/.

[65] Daza Pastrana et al. (2019). *X2Rail-1, Deliverable D8.7 – Application of the risk assessment to the railway signalling system*. Shift2Rail Joint Undertaking, Innovation Programme 2, X2RAIL-1, Start-up activities for Advanced Signalling and Automation Systems.

[66] American Public Transportation Association. (2019). *Securing Control and Communications Systems in Transit Bus Vehicles and Supporting Infrastructure*. APTA SS-CCS-WP-005-19. White Paper. Control and Communications Security Working Group. Available: https://www.apta.com/research-technical-resources/standards/security/apta-ss-ccs-wp-005-19/.

[67] Wischy Hernadez et al. (November 2020). *X2RAIL-3 – D8.2-2 – Generic cybersecurity architecture and shared security services*. Shift2Rail Joint Undertaking, Innovation Programme 2 – X2RAIL-3, Advanced Signalling, Automation and Communication System (IP2 and IP5) – Prototyping the future by means of capacity increase, autonomy and flexible communication.

[68] International Engineering Task Force. (September 2020). *RFC 8915 – Network Time Security for the Network Time Protocol (RFC 8915)*. IETF. Available: https://www.rfc-editor.org/rfc/rfc8915.html.

[69] Otto, G. (2016). *NIST ups transparency in new crypto standards*. FedScoop. Retrieved June 26, 2024 from https://fedscoop.com/nist-ups-transparency-in-new-crypto-standards/.

[70] International Electrotechnical Commission. (2013). *IEC 62443-4-2:2019*, *International Standard. Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components*, *Edition 1.0*. Available: https://webstore.iec.ch/publication/34421.

[71] Strohmeier et al. (2016). *Assessing the Impact of Aviation Security on Cyber Power*. 2016 8th International Conference on Cyber Conflict [223-239], NATO CCD COE Publications. Available: https://ccdcoe.org/uploads/2018/10/Art-14-Assessing-the-Impact-of-Aviation-Security-on-Cyber-Power.pdf.

[72] Regulation (EU) 2019/881. *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*. Available: http://data.europa.eu/eli/reg/2019/881/oj.

[73] National Institute of Standards and Technology. NIST Special Publication 800-30, Revision 1 – Guide for Conducting Risk Assessments – Information Security. NIST SP 800-30r1. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

[74] Microsoft. (May 2023). *Microsoft shifts to a new threat actor naming taxonomy*. Microsoft's Threat Intelligence blog. Available: https://www.microsoft.com/en-us/security/blog/2023/04/18/microsoft-shifts-to-a-new-threat-actor-naming-taxonomy/.

[75] Warrick, J. & Nakashima, E. (May 18, 2020). *Officials: Israel linked to a disruptive cyberattack on Iranian port facility*. The Washington Post. Retrieved on June 27, 2024, from https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-

cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html.

[76] Reuters. (July 9, 2021). *Hackers breach Iran rail network, disrupt service*. Retrieved on June 27, 2024, from https://www.reuters.com/world/middle-east/hackers-breach-iran-rail-network-disrupt-service-2021-07-09/.

[77] Kadosh, O. (August 2023). *Analyzing the Rise of State-Sponsored Cyber Attacks*. Retrieved June 27, 2024 from https://findings.co/analyzing-the-rise-of-state-sponsored-cyber-attacks/.

[78] European Union Agency for Cybersecurity. (October 2023). *Threat Landscape 2023*. ENISA. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.

[79] Trellix. *In the Crosshairs: Organizations and Nation-State Cyber Threats*, *Trellix Global Threat Research*. Available: https://www.trellix.com/assets/docs/trellix-csis-organizations-and-nation-state-cyber-threats-report.pdf.

[80] Monaco, L. O., & Polite Jr., Kennet. (October 20, 2021). *Deputy Attorney General Lisa O. Monaco and Assistant Attorney General Kenneth A. Polite Jr. Deliver Opening Remarks at the Criminal Division's Cybersecurity Roundtable on 'The Evolving Cyber Threat Landscape,'*. Office Public Affairs, U.S. Departement of Justice. October 20, 2021, https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-and-assistant-attorney-general-kenneth-polite-jr.

[81] Barber, G. (August 20, 2020). *This Plane Flies Itself. We Went for a Ride*. Wired. Available: https://www.wired.com/story/autonomous-plane-xwing/.

[82] Xwing. (April 15, 2021). *Xwing Gate to Gate – Short Version – Feb 2021. Youtube. Available: https://www.youtube.com/watch?v=OxJlFPdUSmQ*.

[83] Reliable Robotics. (December 6, 2023). *Reliable Robotics remotely operates a large cargo aircraft with no one on board*. Available: https://www.youtube.com/watch?v=w2O4hgNCMd4.

[84] European Union Agency for Railways. (2017). *X2Rail–1 ATO over ETCS (up to GoA4)*. CCRCC 2017 Conferences. Available: https://www.era.europa.eu/system/files/2022-11/ccrcc_2017_ato_era_en.pdf.

[85] National Cybersecurity Authority. (2022). *Operational Technology Cybersecurity Controls – (OTCC -1: 2022)*. NCA (Saudi Arabia). Available: https://www.nca.gov.sa/otcc_en.pdf.

[86] Nippon Kaiji Kyokai (ClassNK). (November 29, 2023). *Guidelines for cyber resilience of on-board systems and equipment, Edition 1.0, Cyber Resilience of Systems Equipment*. Available:

https://www.classnk.or.jp/hp/pdf/activities/cybersecurity/gl_cyber_resilience_of_onboard_systems_and_equipment_e202311.pdf.

[87] CENELEC. (2018). EN 50129:2020 – *Railway applications – Communication, signalling and processing systems - Safety related electronic systems for signalling.* Available: https://en.tienda.aenor.com/norma-une-en-50129-2020-n0063513.

[88] Palo Alto Networks. (2023). *SIEM Solutions in SOC*. Retrieved on June 30, 2024 from https://www.paloaltonetworks.com/cyberpedia/siem-solutions-in-soc.

[89] European Commission. (June 24, 2024). *Locomotives and railcars by source of energy*. Eurostat. Available: https://doi.org/10.2908/RAIL_EQ_LOCON.

[90] Alsa (n.d.). *Alsa at a glance*. Retrieved on June 30, 2024 from https://www.alsa.com/en/web/bus/about-alsa.

[91] Statista. (2024). *Leading containers shipping companies worldwide based on number of ships as of April 30, 2022*. Retrieved June 30, 2024 from https://www.statista.com/statistics/263291/container-shipping-companies-worldwide-number-of-ships/.

[92] My flight right. (May 2023). *Biggest airlines in the world*. Retrieved on June 29, from https://myflyright.com/blog/biggest-airlines-in-the-world/#:~:text=With%20a%20fleet%20size%20of,serves%20over%2050%20countries%20worldwide.

[93] Pidrman et al. (December 2020). X2RAIL-3, *Deliverable 8.1 – Guidelines for railway cybersecurity part 1 – Simplified Risk Assessment*. Shift2Rail Joint-Undertaking, Innovation Programme 2, TD 2.11. Available: https://projects.shift2rail.org/download.aspx?id=8344db3e-0997-4f31-9a65-c28de673b2dc.

[94] Smith, C. & Brooks. D. (2013). *Security Science – The Theory and Practice of Security*. Available: https://doi.org/10.1016/C2011-0-06978-8.

[95] Ackerman, P. (2017). Industrial Cybersecurity – Efficiently secure critical infrastructure systems. Packt. Available: https://www.packtpub.com/en-us/product/industrial-cybersecurity-9781788395151.

[96] Callan, T. (January 16, 2024). *PKI & Identity and Access Management (IAM)*. Sectigo. Retrieved on July 2, 2024, from https://www.sectigo.com/resource-library/pki-identity-and-access-management-iam.

[97] Internet Engineering Task Force. (). (2008, May 22). *RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile [Standards Track]*. Available: https://datatracker.ietf.org/doc/html/rfc5280.

[98] ISASecure. (February 2024). *The Case for ISA/IEC 62443 Security Level 2 as a Minimum for COTS Components*. Available: https://www.isasecure.org/hubfs/The-Case-for-ISA-IEC-62443-Security-Level-2-as-a-Minimum-FINAL.pdf?hsLang=en.

[99] Regulation (EU) 2016/679. *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 Data Protection Regulation)*. Available: http://data.europa.eu/eli/reg/2016/679/2016-05-04.

[100] International Maritime Organization. (n.d.). *Autonomous shipping – In focus*. Retrieved on July 3, 2024, from https://www.imo.org/en/MediaCentre/HotTopics/Pages/Autonomous-shipping.aspx.

[101] Fortinet. (2024). *2024 State of Operational Technology and Cybersecurity*. Retrieved on July 3, 2024, from https://www.fortinet.com/resources/reports/state-of-ot-cybersecurity.

[102] Kaspersky. (March 2024). Threat landscape for industrial automation systems – Statistics for H2 2023. Kaspersky ICS CERT. Retrieved on July 3, 2024, from https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-Threat-landscape-for-industrial-automation-systems-Statistics-for-H2-2023-En.pdf.

[103] Goward, D. (2020). *New GPS 'Circle Spoofing' Moves Ship Locations Thousands of Miles*. GPS World. Retrieved on July 3, 2024, from https://www.gpsworld.com/new-gps-circle-spoofing-moves-ship-locations-thousands-of-miles/.

[104] Robinson, D. (2017). DEF CON 25 - David Robinson - Using GPS Spoofing to control time. DEF CON 25 Conferences. Available: https://www.youtube.com/watch?v=isiuTNh5P34.

[105] Smith, C. (2016) *The Car Hacker's Handbook: A Guide for the Penetration Tester*. No Starch Press. Available: https://nostarch.com/carhacking.

[106] El-Rewini et al. (2020). *Cybersecurity challenges in vehicular communications*. Vehicular Communications, Volume 23, June 2020, 100214. Available: https://doi.org/10.1016/j.vehcom.2019.100214.

[107] Wouters et al. (2019). Fast, Furious and Insecure: Passive Keyless Entry and Start Systems in Modern Supercars. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2019(3), 66–85. Available: https://doi.org/10.13154/tches.v2019.i3.66-85.

[108] Chen et al. (2015). *Security Analysis of Urban Railway Systems: The Need for a Cyber-Physical Perspective*. Available: http://link.springer.com/10.1007/978-3-319-24249-1_24.

[109] Potamos et al. (May 27, 2024). *Enhancing Maritime Cybersecurity through Operational Technology Sensor Data Fusion: A Comprehensive Survey and Analysis*. Sensors 2024, 24, 3458. Available: https://doi.org/10.3390/s24113458.

[110] Rainer Gerhards. (n.d.). *Rsyslog – The rocket-fast system for log processing*. Retrieved July 4, 2024, from https://www.rsyslog.com/doc/index.html.

[111] One Identity. (n.d.). *syslog-ng – Open Source Edition 3.17 - Administration Guide*. Retrieved July 4, 2024, from https://www.syslog-ng.com/technical-documents/doc/syslog-ng-open-source-edition/3.17/administration-guide/51#:~:text=Use%20reliable%20disk%2Dbased%20buffering,grows%20as%20new%20messages%20arrive.

[112] Scheer, E. (2022). *Distributed Logging Transport for Unreliable and Lossy Networks*. Available: https://matheo.uliege.be/zip/2268.2/16294.

[113] MITRE. (2023). MITRE ATT&CK for ICS. MITRE Corporation. Available: https://attack.mitre.org/matrices/ics.

[114] International Organization for Standardization & Society of Automobile Engineers. (2021). *ISO/SAE 21434:2021 (E), International Standard – Road Vehicles - Cybersecurity Engineering*. First edition. Available: https://www.iso.org/standard/70918.html.

[115] National Highway Traffic Safety Administration. (2022). *Cybersecurity Best Practices for the Safety of Modern Vehicles*. Available: https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-tag.pdf.

[116] William Gouse, S et al. (2022). *SAE proposals to UNECE WP.29 related to automotive cybersecurity*. Informal document GRVA-13-28. Available: https://unece.org/sites/default/files/2022-05/GRVA-13-28e.pdf.

[117] BIMCO et al. (2021). *The guidelines on cyber security onboard ships, Version 4.*Available: https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships.

[118] Digital Container Shipping Association's (DCSA). (March 2020). *DCSA Implementation Guide for Cyber Security on Vessels, v1.0.* Available: https://dcsa-website.cdn.prismic.io/dcsa-

website/65ae6dab38f662e9dd212313_20220310_DCSA-Implementation-Guideline-for-BIMCO-Compliant-Cyber-Security-on-Vessels-v1.0.pdf.

Annex A

Could IEC 62443 SL-T=3 be enough for Transport OICS?

To begin with an example of a reference SL-T level in Transport sector, the public ENISA report for railway zones and conduit architecture states that "Currently the proposed SL-T for devices in the signalling domain is SL-T 3. In some cases, SL-T 2 is also applied, which depends on the risk for the zone" [6]. While this is true for railway environment in Europe due to a "somehow" stable geopolitical status, if we consider national regulations mandated by some governments like Saudi Arabia to protect their OT/ICS assets including "[…] all devices, systems, or networks used to operate and/ or automate industrial processes" [85] (p. 8), we can observe requirements of the kind "2-2-1-6 Dual approval and explicit privilege escalation mechanisms for sensitive actions within the OT/ICS environment must be employed." [85] (p. 23), which corresponds to an IEC 62443-3-3 "SR 2.1 RE 4 – Dual approval" requested for SL-T 4.

While passing to a SL-T 4 is considered by IEC 62443 standard as being in the attacker definition of a nation-sponsored threat actor, if we observe recent trends in Transportation tenders like those from Saudi Arabia or Israel, it is reasonable to question if an organization with a fleet of moving critical infrastructure assets like OICS can ensure their cyber resilience given the unlimited resources and capabilities of worst-case threat actors discussed.

This assumption is pertinent when observing how non-state and state-sponsored attacks are closing the gap and "[…] forming alliances of convenience, alliances of opportunity and sometimes alliances by design with nation-state actors" as reported by US Government [80] or the creation ENISA threat actor category "State-nexus threat groups" [78](p. 20) and when speaking about threats techniques and resources needed. Some articles on this trend are the latest Microsoft threat actor taxonomy declaring have identified "[…] 160 nation-state actors" [74], the timeline of 2023 nation-sponsored attacks proposed by Kadosh, O [77], or the report by *Trellix* in which they declared that 86% of companies are somewhat sure that received attacks backed by nation-sponsored groups [79](p. 6) like nation-sponsored attacks to Iranian airport by Israel [75] or yet another attack to Iranian railway infrastructure [76] but to name a few.

Actor category	Type	Family Name
Nation state	China	Typhoon
	Iran	Sandstorm
	Lebanon	Rain
	North Korea	Sleet
	Russia	Blizzard
	South Korea	Hail
	Turkey	Dust
	Vietnam	Cyclone

Figure 31 - Extract from new Nation-state Threat Actor's Taxonomy. Microsoft [74].

Certainly, this question deserves an in-deep analysis and the consideration by technical committees responsible for ICS standardization like IEC Technical Committee 65 (IEC 62443) [70](p. 12) to adapt security levels control mechanisms to match newer threat actor landscape with Security Levels.

To conclude, in the context of Transport OICS it can be assumed, with the evolving reduction of efforts needed to perform complex attacks, and the hacking-as-a-service trend of criminal organizations being backed by nation-states actors [52](p. 561) [78](p. 72), that it is a matter of time that the Transportation sector will be pointed out in a global manner by threat actors with high resources, capabilities, motivation and specific ICS skills, regardless of the corresponding SL definition. This tendency may imply that OICS manufacturers should start investing in delivering SL 4 capable systems to be able to not only win contracts in stable geopolitical customers' countries, but also cover emerging markets like Middle-East.

Why SR 2.11 RE 2 level should be lowered (a lot)

When looking to IEC 62443-3-3 "SR 2.11 – Protection of time source integrity" requirement, the dependency of time and the hybrid nature of OICS, we may affirm that the IEC standard did not take into consideration OICS context when setting such requirement to the highest possible security level (SL-C = 4).

As mentioned in first chapters, when comparing the operational context of typical ICS plant and OICS, the assumptions on physical protection and network reliability are very different (refer to 2.2.3 and 4.2.2 for extended discussion). If in addition, we consider the threat actor landscape of OT assets and the easiness nowadays on performing spoofing attacks both on location and time from GNSS signals [51][54][53][103][104] but to name a few, it is evident that the minimum SL-C to protect this function should be reduced.

In the context of OICS, we saw in chapter 4.3.2 that a centralized TIME LSSS providing a reliable time-source is requested from SL-C = 2, but this was lowered to SL 1 in the newer IEC 62443-4-2 (2019) [70](p. 44). At these SLs, only timestamps (SR 2.11) are needed in the devices (both standard parts should be revised to be aligned, but this is another topic). Then, at SL-C = 3, appears the first suggestion to have a system-wide time retrieved from "recognized external time sources" like GNSS to synchronize the internal OICS clocks, but without recommendation to protect this operation. Only at SL-C = 4, the requirement to protect the integrity (not the authenticity) of the time source retrieval is required. The reason of why only protect integrity and not authenticity could be due to the only system-wide time-source recommendations given on the standard, which is satellite-based but this should be used only as an additional source or backup for comparison, as recommended in chapter 4.4.2 when defining the cybersecurity considerations for a TIME LSSS Hybrid design.