



UNIVERSIDADE D
COIMBRA

João Nunes

SECURITY FOR RAILWAY INFRASTRUCTURE

Dissertation in the context of the Master in Information Security, advised by Professors Paulo Simões and Tiago Cruz and presented to the Department of Informatics Engineering of the Faculty of Sciences and Technology of the University of Coimbra.

June 2025



DEPARTAMENTO DE
ENGENHARIA INFORMÁTICA
**FACULDADE DE
CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE D
COIMBRA**

João Nunes

SECURITY FOR RAILWAY INFRASTRUCTURE

**Dissertation in the context of the Master in Information Security, advised by
Professors Paulo Simões and Tiago Cruz and presented to the Department of
Informatics Engineering of the Faculty of Sciences and Technology of the
University of Coimbra.**

June 2025



DEPARTAMENTO DE
ENGENHARIA INFORMÁTICA

FACULDADE DE
CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE DE
COIMBRA

João Nunes

SEGURANÇA PARA INFRAESTRUTURAS DE TRANSPORTE FERROVIÁRIO

**Dissertação no âmbito do Mestrado em Segurança Informática, orientada
pelos Professores Paulo Simões e Tiago Cruz e apresentada ao Departamento
de Engenharia Informática da Faculdade de Ciências e Tecnologia da
Universidade de Coimbra.**

Junho 2025

Acknowledgements

I would like to thank for all the support from professors Paulo Simões and Tiago Cruz.

Abstract

The Railway industry is currently undertaking a big step towards digitization. Railway systems are a critical infrastructure of a region or country, moving goods and passengers. Nowadays railway systems being increasingly digital, and completely interconnected.

Railway infrastructure is a critical Operational Technology (OT) system, with some characteristics, such as being expected to work 24x7, 365 days a year. If something does not work as planned, and the OT system is compromised, it can cause a train accident, or interrupt traffic, the losses can be very high, in the standpoint of business and as well as for the safety of passengers, staff and ultimately to human life. So, it becomes a critical target for cyber-warfare from terror groups and foe nations. Even minor disruptions in critical rail systems can result in temporary product shortages that can cause significant harm to national security. Prolonged disruptions in the flow of commodities could lead to widespread supply chain disruptions, with ripple effects across the economy. Disruptions and delays can affect industries that depend on the commodities transported by the railroads, which becomes a matter of national defence.

Due to cyber-threats to railway systems, the industry, suppliers, integrators, operators and governing agencies had the need to develop standards, technical specifications and guidelines, to help to protect these systems. It is also intended to reach a level of harmonization of the implemented measures and controls across the same geographical space. In this dissertation, it will be depicted what norms and standards have been, or are being developed, and implement across the European Union member states and the United States of America, that are specifically applicable to the railway ecosystem. There is also a succinct description of which cyber-related European legislation applied to railway operators as suppliers of essential services. It also covers in detail what are the necessary steps to apply CENELEC Technical Specification CLC/TS 50701 - Railway applications - Cybersecurity (TS50701).

The latter portion of this dissertation details the development of a software application designed for anomaly detection within critical communication messages on the train's internal bus, specifically those exchanged between the control system and its peripherals. Identified anomalies may represent sensor or actuator failures or malicious control system tampering.

Keywords

Railways, OT security, cybersecurity, Critical infrastructure security, TS50701

Resumo

A indústria ferroviária está atualmente a dar um grande passo em direção à digitalização. Esta é uma indústria onde a esperança de vida dos equipamentos operacionais é por vezes superior a 30 anos, e atualmente, à medida que a tecnologia avança, também os equipamentos ferroviários seguem esta tendência. Os sistemas ferroviários são uma infraestrutura crítica de uma região ou país, movimentando mercadorias e passageiros. Com os sistemas ferroviários cada vez mais digitais e completamente interligados.

A infraestrutura ferroviária é um sistema de Tecnologia Operacional (TO) crítico, com algumas características, como de funcionar 24 horas por dia, 7 dias por semana, 365 dias por ano. Se algo não funcionar como esperado, e o sistema de OT ficar comprometido, isto pode potencialmente causar um acidente ferroviário, ou interromper o tráfego. Os prejuízos podem ser muito elevados do ponto de vista financeiro como também a nível da segurança dos passageiros, funcionários e em última análise, para a vida humana. Assim, torna-se um alvo crítico para a guerra cibernética de grupos terroristas e nações inimigas. Mesmo pequenas perturbações em sistemas ferroviários críticos, podem resultar em escassez temporária de produtos que podem causar danos significativos à segurança nacional. As perturbações prolongadas no fluxo de mercadorias podem levar a perturbações generalizadas na cadeia de abastecimento, com efeitos em cascata em toda a economia. Interrupções e atrasos podem afetar indústrias que dependem das mercadorias transportadas pelas ferrovias, o que se pode tornar numa questão de defesa nacional.

Devido às ameaças cibernéticas aos sistemas ferroviários, a indústria, fornecedores, integradores, operadores e agências governamentais tiveram a necessidade de desenvolver normas, especificações técnicas e recomendações, para ajudar a proteger esses sistemas, como também a alcançar um nível de homogeneidade do tipo de medidas implementadas no mesmo espaço geográfico. Nesta dissertação serão descritas quais normas e recomendações foram, ou estão sendo desenvolvidos e implementados nos estados membros da União Europeia e nos EUA, que são especificamente aplicáveis ao ecossistema da ferrovia. Há também uma descrição sucinta de qual legislação europeia relacionada com o ciberespaço que é aplicada aos operadores ferroviários enquanto fornecedores de serviços essenciais.

Também serão mostrados detalhadamente quais são os passos necessários para aplicar a especificação técnica europeia European Electrotechnical Committee for Standardization (CENELEC) TS50701.

A última parte desta dissertação descreve detalhadamente o desenvolvimento de uma aplicação de software concebida para a deteção de anomalias em mensagens críticas no bus interno do comboio, especificamente aquelas trocadas entre o sistema de controlo e os seus periféricos. As anomalias identificadas podem representar falhas em sensores ou atuadores, ou adulteração maliciosa do sistema de controlo.

Palavras-Chave

Ferrovia, Segurança, Tecnologia Operacional, Segurança de Infraestruturas Críticas, TS50701

The contributions of this thesis resulted in the following publications in international peer-reviewed conferences and journals:

Conference papers:

- "Railway Infrastructure Cybersecurity: an overview" [1] , presented at the 23rd European Conference on Cyber Warfare and Security, in June of 2024, held in the University of Jyväskylä, Jyväskylä, Finland.

Contents

1	Introduction	1
1.1	Context	1
1.2	Dissertation Objectives	1
1.3	Work schedule	2
1.4	Document Structure	3
2	Context of Railway Cyber-Security	5
2.1	Introduction	5
2.2	Cyber threat landscape	6
2.3	Railway Cyber attacks	9
2.4	Governance framework	11
2.4.1	Railway Cybersecurity Regulation in the European Union .	11
2.4.2	Railway Cybersecurity Regulation applied in the United States	15
2.5	Difference between Safety and Security in Railway	34
2.6	Cyber Risk Scenario - IxL & ATS SYSTEMS	37
2.6.1	IxL Main vulnerabilities	39
2.6.2	ATS Vulnerabilities	39
2.6.3	ATS & IxL Vulnerability Examples	40
2.7	How to apply CENELEC TS 50701	41
2.7.1	Life Cycle	42
2.7.2	Zone and conduit identification	43
2.7.3	Cybersecurity Management Plan	47
2.7.4	Detailed Risk	49
2.7.5	Implementation and handover	52
2.7.6	Legacy Systems	54
2.8	Conclusions	57
3	Proposed Security Solution for monitoring critical conduits	59
3.1	Testbed and use case scenario development	59
3.2	About CAN	60
3.2.1	CAN bus	60
3.2.2	CAN security	61
3.3	CAN application in Railway	62
3.3.1	IEC 61375 Standard	62
3.4	CAN and SocketCAN	63
3.4.1	How to monitor and analyse traffic	65
3.4.2	Markov chains	65

3.5	Software Tool description	66
3.6	Software Tool Validation	69
3.7	Conclusions	71
4	Conclusion	73
	References	75

Acronyms

APTA American Public Transportation Association.

ATO Automatic train operation.

ATP Automatic Train Protection.

ATS Automatic Train Supervision.

CDP Cisco Discovery Protocol.

CENELEC European Electrotechnical Committee for Standardization.

CISA Cybersecurity & Infrastructure Security Administration.

CRA Cyber Resilience Act.

CRM Customer relationship management.

CRS Cybersecurity Requirements Specification.

CSP cloud service provider.

DC Data confidentiality.

DDoS Distributed Denial of Service.

DMZ Demilitarized Zone.

DoS Denial of Service.

EFTA European Free Trade Association.

EIS Enterprise information system.

EN European Normative.

ENISA European Union Agency for Cybersecurity.

ERA European Union Agency for Railways.

ERP Enterprise resource planning.

EU European Union.

FTA Fault Tree Analysis.

IAC Identification and authentication control.

IACS industrial automation and control system.

ICS Industrial control systems.

IoT Internet of things.

IT Information Technology.

IxL Interlocking system.

KMS Knowledge management system.

LOS Line-of-sight.

Main Line principal rail links between big towns and cities.

MSP Managed service providers.

MSSP Managed security service provider.

MVB Multi-function Vehicle Bus.

NIDS Network Intrusion Detection System.

NMS Network Monitoring System.

OCC Operations Control Centre.

OT Operational Technology.

PLC Programable Logic Controller.

RA Resource availability.

RAMS Reliability, Availability, Maintainability & Safety.

RDF Restricted data flow.

SCADA Supervisory Control and Data Acquisition.

SCM Supply chain management.

SDLC Systems Development Life Cycle.

SecRAC Security Related Application Conditions.

SI System integrity.

SIEM Security Incident and Event Management System.

SIL Safety Integrity Level.

SL Security Level.

SL-A Achieved Security Level.

SL-T Targeted Security Level.

SMS safety management system.

SPT Spanning tree protocol.

SRAC Safety Related Application Conditions.

SuC System under consideration.

TETRA TERrestrial TRunked RAdio.

TO Tecnologia Operacional.

TRE Timely response to events.

TS50701 CENELEC Technical Specification CLC/TS 50701 - Railway applications - Cybersecurity.

TSA Transportation Security Administration.

UC Use control.

List of Figures

1.1	Gantt chart	3
2.1	Railway - prime threats [2]	9
2.2	Legacy Stand-alone System, Closed (Mainly Physical and Administrative) [33]	18
2.3	Interconnected System (Partially Integrated) [33]	19
2.4	Purdue Zone Model for Operational Technology (OT) [38]	23
2.5	Model Zone Chart for Transit Systems [35]	25
2.6	Connecting security zones of different security levels [35]	26
2.7	Safety-Critical Testing [35]	27
2.8	Fault tree analysis of train collisions [39]	28
2.9	Overall Derailment Attack Tree [34]	31
2.10	Contingency Planning process [11]	34
2.11	Relationship between cybersecurity and safety [47]	35
2.12	Safety and Quality evidence, and the valid regulations [48]	35
2.13	Safety Case and Cyber security Case interaction [48]	36
2.14	Railway infrastructure communications and network environment [50]	38
2.15	The different meanings of the CIA triad in Information Technology (IT) and OTs	38
2.16	Low cybersecurity awareness [53]	40
2.17	Default Password vulnerability [52]	41
2.18	Obtaining an administrator password on HP/H3C and Huawei devices via SNMP [52]	41
2.19	Railway asset model [18]	44
2.20	Railway physical architecture model [18]	45
2.21	Generic high level railway zone model [18]	46
2.22	Defence in depth with example of measures [18]	48
2.23	Sample of CENELEC Technical Specification CLC/TS 50701 - Railway applications - Cybersecurity (TS50701) Table 6 System Security Requirements and Foundational Classes [18]	51
2.24	Detailed risk assessment flowchart [18]	51
2.25	Vulnerability and outage time during system update (maintenance phase) [18]	54
2.26	Vulnerability and outage time during system update with observation phases [18]	54
3.1	The Layered ISO 11898 Standard Architecture [60]	63

3.2	Typical CAN communication layers. With SocketCAN (left) or conventional (right). [64]	64
3.3	SocketCAN test set-up	65
3.4	Diagram representing a two-state Markov process [71]	66
3.5	Software tool flow diagram	68
3.6	Railway V Cycle V-and-V Activities [76]	69

List of Tables

2.1	Threats to Transit Sector [11]	8
2.2	Zone Importance [35]	21
2.3	DHS Zone Model [35]	23
3.1	Tool Test cases	70

Chapter 1

Introduction

1.1 Context

As today's world gets more interconnected, and with every system getting more technological, the railway industry is also evolving. With the interdependence of systems, a railway infrastructure that until a few years ago was considered safe because it was not connected to the exterior, is now seen as a potential target. This is due to its magnitude and importance to a region or a country. As a result of this new cyber landscape, agencies, integrators, and operators had the need to develop cybersecurity standards, specifications, and guidelines specifically applied to the railway ecosystem.

Typically, a railway infrastructure is made up of several subsystems, the most critical ones, according to the documentation provided in [2], are Interlocking system (IxL) and the Control Center or Automatic Train Supervision (ATS). The IxL controls all the signalling and track moving parts and prevents trains from using the same track. The ATS, is where train routing and traffic management decisions are taken, nowadays with a high level of automation. It is also where all the movement of trains is recorded. Besides these two systems, there are also a few subsystems, such as passenger announcing systems, to power line control systems, etc., that make the railway ecosystems quite complex.

1.2 Dissertation Objectives

The objectives of this dissertation are to present a study of the railway cybersecurity technical specification TS50701, which is applicable to the member states of the European Union and was issued by European Union Agency for Cybersecurity (ENISA), and which in a short time will become European Normative (EN). Similar relevant norms applicable in the United States of America, namely the Transportation Security Administration security directives, and American Public Transportation Association technical guidelines will also be analysed in this document and compared with the European norm. Considering the complexity of

TS50701, it will also be described how to apply this European technical specification. The purpose of this detailed explanation is that it could then be used in future work, saving time in the analysis of TS50701.

With the knowledge of what is currently recommended for new systems and what could be an opportunity of studding and developing a control to be implemented on legacy systems, this presents an opportunity to design a test bed for testing attack detection solutions.

1.3 Work schedule

The work schedule for the complete dissertation was as follows:

- Analyses of which cybersecurity norms and guidelines are mostly used - two weeks
- Analyses of European governance related with cyber-security applied to railway infrastructure in the European union member states - two weeks
- Analysis of cyberthreat landscape and known railway cyber attacks - two weeks
- Description of the applicable U.S.A. Security Directives, Norms and recommended guidelines - two weeks
- Analysis of railway safety norms - two weeks
- Analysis of first European Railway Cybersecurity Technical Specification CENELEC TS 50707 and what the steps for a practical application in a new project and in a legacy system - two weeks
- Identification of the critical conduits in the railway infrastructure to replicate in the test bed - two weeks
- Intermediate dissertation Documentation - two weeks

Due to professional reasons, there was one semester in which I was unable to perform any work related to the dissertation. Therefore, after restarting the work, the remaining work schedule was as follows:

- Bureaucratic and logistic effort to contact railway supplier/operator to get permission for gathering data - six weeks
- Search for alternatives to the data supplied by railway supplier/operator - two weeks
- Analysis of which protocols are involved in railway - two weeks
- Search for message generator for CAN bus and architecture of the test-bed - two weeks

- Proposal of the security architecture and which solutions to develop - two weeks
- Implementation of the security architecture - two weeks
- Test plan development and execution - two weeks
- Documentation - two weeks

Figure 1.1 presents the project schedule for the complete dissertation work.

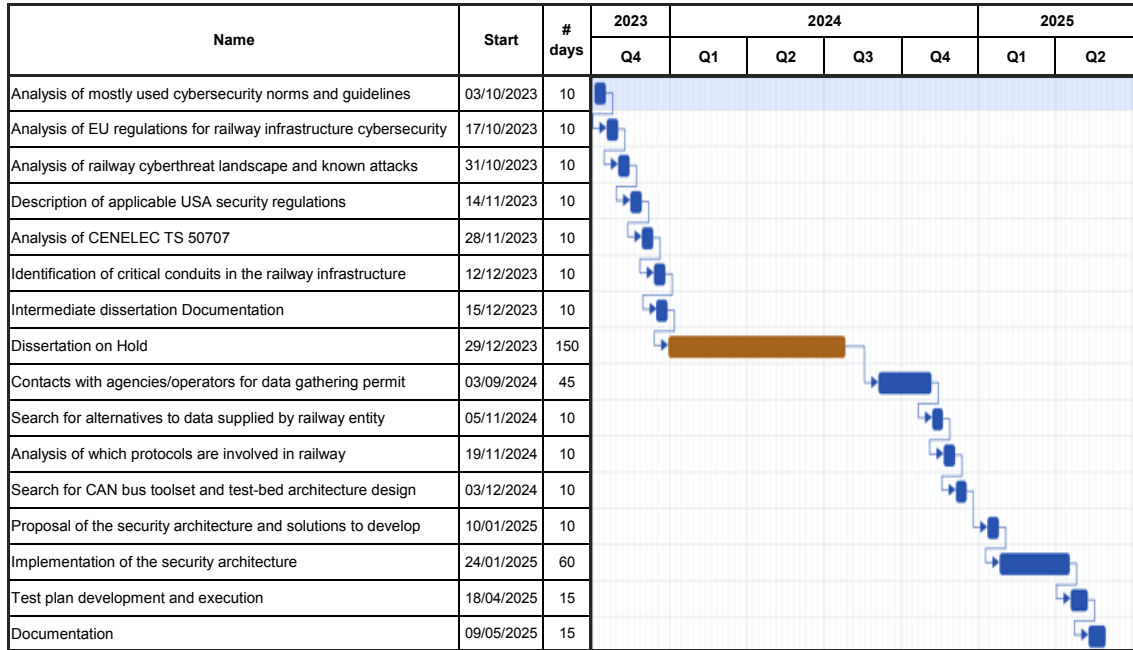


Figure 1.1: Gantt chart

1.4 Document Structure

The document is organized into four chapters. Chapter 1 is divided into four sections. The context in which the railway framework is presented. The objectives of the dissertation, where the goal of this dissertation is presented. The work schedule, depicting all the major tasks to be accomplished, and its time frame together with the project schedule.

Chapter 2, is divided into eight sections. The Introduction, where an approach to Railway Cybersecurity and its major concerns is given. The Cyber Threat Landscape, where an overview of the cyber threat landscape is made and the main threats are presented. The Railway Cyber attacks, where the main railway cyber attacks of Ransomware, data leakage, and DDoS are presented as they were identified as the most prevalent in the cyber threat landscape. The Governance framework, where the governance framework is presented, the first part presents the applicable legislation of the European Commission, then the European Electrotechnical Committee for Standardization, which is the editor of the

European Electrotechnical Committee for Standardization (CENELEC) TS 50701, then an overview of the governance applicable in the United States, where the Transportation Security Administration (TSA) security directives and the American Public Transportation Association (APTA) Recommended Practices are presented, detailing each one. The duality of the Safety and Security is presented and how its approval is achieved in a real project. The Cyber Risk Scenario - IXL ATS SYSTEMS, where is presented the cyber risk scenario for interlocking system and Automatic Train supervision system that are two of the most critical ones in the railway infrastructure and their vulnerabilities. The ATS IxL Vulnerability Examples, where are presented several Interlocking and Automatic Train Supervision vulnerabilities examples. And finally, the How to apply CENELEC TS 50701, which goes through all the major required steps to implement this technical specification.

In chapter 3, the elaboration of the practical part of this dissertation is described in detail. All steps, from the constraints to contact railway operators and suppliers, as well as the final solution of using SocketCan to simulate a railway communication path. In this chapter are also presented the initial requirements for the design of a Python software tool that monitors and identifies abnormal behaviour in communication conduit, the test cases, and the results.

Chapter 4 presents the general conclusions of this dissertation. It states the difficulties found throughout the complete research process for the state-of-the-art, the contact with railway operators, and the design of the software tool to monitor and detect issues in a railway conduit. In addition, the author discusses cybersecurity awareness in the railway industry.

Chapter 2

Context of Railway Cyber-Security

2.1 Introduction

The railway industry is currently taking a huge step towards digitalization. But these systems across Europe, are far from harmonized in terms of technology. This is an industry where the life expectancy of operational equipment is sometimes longer than 30 years. As an example, today, in a state-of-the-art railway system, most of the processing functions for interlocking and signalling are run in the cloud [3]. This ensures the highest level of redundancy, availability, and punctuality. On the other hand, in some countries there are still legacy systems running equipment with technologies from the late 1980s, suffering with obsolescence and where security definitely was not even a topic.

The Railway infrastructure is a critical OT system, with some characteristics, such as being expected to work 24x7, 365 days a year. If something does not work as planned and the OT system is compromised, it can cause a train accident or interrupt traffic, the losses can be very high, from the point of view of business and for the safety of passengers, staff and ultimately human life. So, it becomes a critical target for cyberwarfare from terror groups and foe nations. Even minor disruptions in critical rail systems can result in temporary product shortages that can cause significant damage to national security. Prolonged disruptions in commodity flow could lead to widespread supply chain disruptions, with ripple effects across the economy. Disruptions and delays can affect industries that depend on commodities transported by railroads, which becomes a matter of national defence [4].

Railway systems are now seen as a potential target for cybercriminals. Compared to IT systems, OT systems are usually more vulnerable than IT systems, in part due to a lack of cybersecurity awareness in OT personnel, in part because they were not designed with cybersecurity in mind (long life cycles of 30 years, presence of legacy systems) and because they are less controlled and spread across a larger geographical area. A railway main line system can have several hundreds of kilometres. For example, the Japanese bullet train, Shinkansen, is spread over 515 km [5], involving a large number of different devices with a wide diversity of

supply chains [6].

An incident in this type of systems can also have a great impact on the public opinion due to the large number of passengers. For example, a mass-transit railway system as the London Tube handles up to five million passenger journeys a day, serving 272 stations [7].

Bearing in mind what was previously described in terms of criticality, threats, vulnerabilities, and lack of consistency across countries, the European Union railway suppliers and operators had the urgent need to try to change this course. The task of producing a technical specification that could put into place what are currently the best practices in the cyber security, guided for OT systems, with the focus on the railway ecosystem was given to the European Committee for Electrotechnical Standardization. This organization has just recently released the technical specification CENELEC TS 50701, which had its first release approved in 2021 and the latest release is from 2023-08-11. This Technical Specification applies to communications, signalling and processing domain, to rolling stock and to fixed installations domains. It provides references to models and concepts from which requirements and recommendations can be derived and suitable to ensure that the residual risk of security threats is identified, supervised, and managed to an acceptable level by the duty holder of the railway system [8].

CENELEC TS 50701 takes into consideration relevant safety related aspects (EN 50126 [9]) and takes inspiration from different sources (IEC 62443-3-3 [10], CSM-RA), adapting them to the railway context. Covers numerous key topics such as cybersecurity overview of the railway system during its life cycle, risk assessment, security design, cybersecurity assurance and system acceptance, vulnerability management, and security patch management [8]. The application of this technical specification will be described in chapter 2.7 of this document.

2.2 Cyber threat landscape

Today we can see railway lines fully automated, taking advantage of the latest technologies in terms of Ethernet, Wifi, LTE, Internet of things (IoT) and cloud automation services. Although with all this technology, there are still big differences between railway operators and their cyber defence awareness and infrastructure. In some cases, they can have the state-of-the-art in terms of interlocking, train control, and Control Centre. However, there are still a large number of systems that are operating with relay tables and relay interlockings. This diverse landscape proves to be challenging for railway operators that have to deal with the cybersecurity aspect.

In state-of-the-art systems, we can consider that the attack surface can be quite large due to the number of interconnected systems. Some of these are even connected to the Internet (e.g. online passenger information). Although legacy systems may not be as exposed to external threats due to their lower complexity, one of the major challenges is the availability of security patches that leave them vulnerable to inside threats.

A typical railway system IT infrastructure is made up of three layers, namely: operational system, enterprise information systems, and subscribed systems. Today, these layers are all interconnected and depend on one another for smooth operation [11]. The operational integrity of the transit agency depends on the integrity of each layer and might exchange or utilize information contained in other layers [11]. Malicious actors can target and exploit specific system layers within the railway system IT infrastructure. The layers mentioned earlier include the following:

- Operational systems or OT, integrate Supervisory Control and Data Acquisition (SCADA), train movement, monitoring and signalling of transportation equipment and services.
- Enterprise information systems consist of applications systems for internal and external data exchange and management.
- Subscribed systems, formed by managed systems outside the transportation agency, such as agency website, service provider for timetable information, cloud storage, online ticketing systems, etc. [11].

Cyberattacks towards transportation infrastructure can use several vectors. It can be a single act or a combination of discrete steps threaded together. Those acts can be performed in a complex way by exploiting vulnerable software or the simple use of social engineering to gain access to confidential information. Attacks that reach some level of success almost never take the same attack vector in a consecutive or follow-up assault. One of the reasons for it is the share of information between stakeholders of agencies, the attack needs to be adapted in response to the level of success on the targeted organization. Detected cyberattacks are usually mitigated through some form of countermeasure. This forces the initiating elements to evolve their attack, to avoid the countermeasures. One of the strategies used today by attackers is to hide in the system, supply chain attack, to evade detection and quarantine [12]. This can be done by gaining control of the software that is implemented in the first place to detect this malicious code or malware. It can be so sophisticated that it is even capable of updating, increasing its life and being undetected [11].

Cyberthreat actors apply disruptive and destructive attacks, particularly ransomware attacks. Normally, the consequences of an attack to the organisations if the ransom is not paid are threaten that they will destroy, sell, or leak exfiltrate data or authentication information.

Cyber-physical threats can also endanger people or property; supply chain risks; fraud; vulnerabilities associated with the integration of operational technologies OT and the Internet of Things (IoT); and cyber-enabled information operations that could discredit a transit organization or cause panic [11].

Although many cyberattacks are perpetrated by external actors, railway systems, as any other IT/OT, is vulnerable to internal attacks. These types of attacks have a higher success rate and greater potential for damage due to the level of access and knowledge an inside actor has. As depicted in Table 2.1, the threats to the

value chain of the railway system sector are immense.

VALUE CHAIN PROCESS	STATE CYBERTHREAT ACTORS	CYBERCRIMINAL GROUPS	HACKTIVIST GROUPS	INSIDERS
Planning and Scheduling	<ul style="list-style-type: none"> • Theft of intellectual property • Targeted surveillance and monitoring 	<ul style="list-style-type: none"> • Ransomware attacks to disrupt processes for financial gain • Theft of employee PII for sale or extortion 	<ul style="list-style-type: none"> • Disclosures and embarrassment • Theft of travel plans and data • Disruption of expansion • Reputational damage 	<ul style="list-style-type: none"> • Theft of intellectual property • Human error • Insider trading • Data monetization
Pricing and Ticket Sales	<ul style="list-style-type: none"> • Theft of client PII for espionage • Loss or corruption of critical client information • Loyalty or partner network data theft 	<ul style="list-style-type: none"> • Ransomware attacks to disrupt processes for financial gain • Theft of client PII for use or resale • Credit card skimming 	<ul style="list-style-type: none"> • Denial of service attack • Website defacement • Reputational damage 	<ul style="list-style-type: none"> • Disruption or misuse of systems • Human error • Insider trading • Data monetization • Theft of funds
Station Operations (Wi-Fi, maintenance, etc.)	<ul style="list-style-type: none"> • Social disruptions • Interception of public Wi-Fi • Defacement of announcement boards 	<ul style="list-style-type: none"> • Ransomware attacks to disrupt processes for financial gain • Interception of public Wi-Fi 	<ul style="list-style-type: none"> • Disruption of operations through cyber- and physical attacks • Defacement of announcement boards • Reputational damage 	<ul style="list-style-type: none"> • Human error • Disruption of processes • Theft of data or funds • Defacement of announcement boards • Reputational damage
Transit Operations	<ul style="list-style-type: none"> • Theft of system maintenance data • Cyberhijacking • Geolocation data disruptions • Sensor disruptions 	<ul style="list-style-type: none"> • Ransomware attacks to disrupt processes for financial gain 	<ul style="list-style-type: none"> • Disruption of travel • Panic-mongering • Reputational damage 	<ul style="list-style-type: none"> • Disruption of processes • Theft of assets • Human error
Assets and Logistics	<ul style="list-style-type: none"> • Impact on route availability • Social disruption 	<ul style="list-style-type: none"> • Ransomware attacks to disrupt processes for financial gain 		

Table 2.1: Threats to Transit Sector [11]

In 2020 ransomware and data-related threats were the two major threats aimed at the railway sector as show in Figure 2.1 . These are followed closely by Distributed Denial of Service (DDoS) attacks. Ransomware and threats related to data are generally done in conjunction, as ransomware is usually followed by ex-filtration or data leakage [2]. The majority of attackers have chosen the IT system as their main target (passenger information, ticketing, mobile apps, and others), with the impact causing unavailability of the services. Some of the cases include ransomware attacks targeting Skånetrafiken (2021) and Ferrovie dello Stato Italiane (2022), which resulted in customers not being able to buy tickets following infections to IT systems, making them unavailable [2].

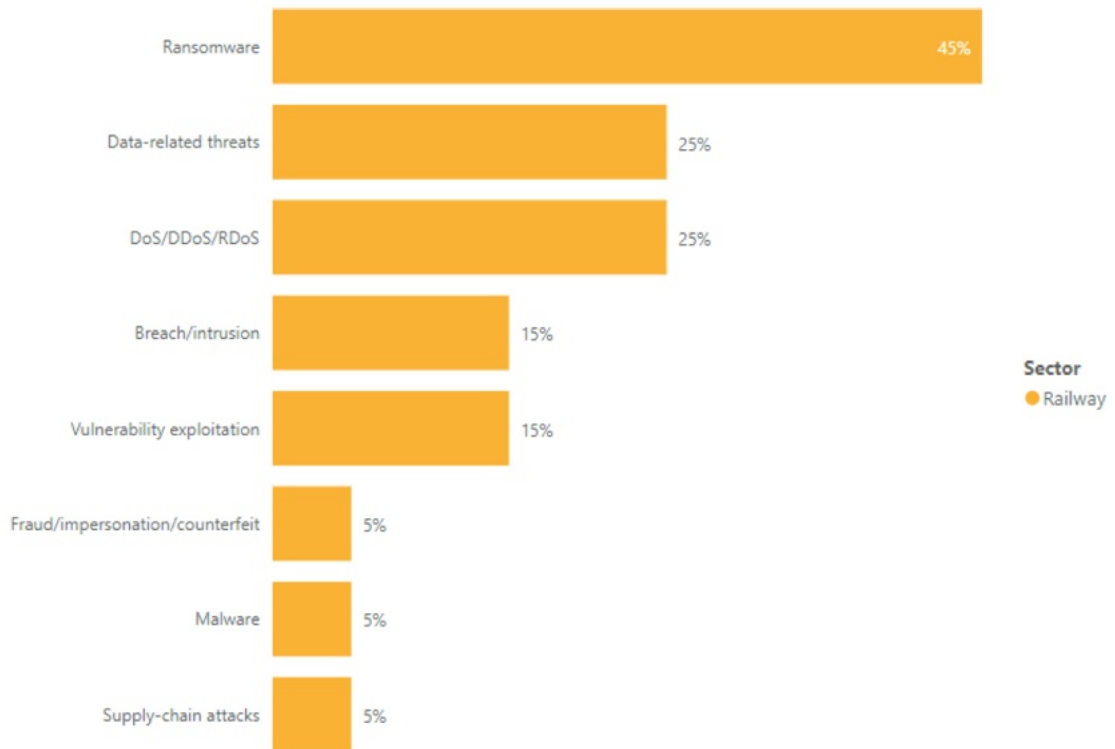


Figure 2.1: Railway - prime threats [2]

2.3 Railway Cyber attacks

Many transit systems are providers of critical infrastructure and, as such, could become targets for politically and financially motivated cyberthreat activity. In fact, geopolitical motivated threat actors have targeted transportation systems as part of larger attempts to discredit or block a country or region [11]. In recent times, the railway infrastructure has been the target of several attacks that impacted passenger information and ticketing systems. In 2016, the San Francisco Public Transportation network ticketing system experienced an attack during Thanksgiving (“ransomware” type attack), which provided free tickets for several days. In 2017, a passenger information system in Germany was targeted by Wannacry ransomware [13].

Between 2015 and 2016, the UK railway network was targeted at least four times by “exploratory attacks”, in which attackers successfully accessed a wide information management system that controls railway traffic signalling [13].

Between 2019 and 2021, the Iranian railway system experienced multiple cyber attacks by an Iranian opposition group known as Indra. It caused widespread chaos with hundreds of trains being delayed or cancelled. On the day of the train attack, an announcement appeared on electronic timetable boards at railroad stations across Iran saying: “Long delays due to cyberattacks.” The message itself was the work of hackers and, in a sardonic twist, it advised confused travellers to seek more information by calling 64411, the office number of Iran’s supreme leader, Ayatollah Ali Khamenei [14]. A day later, the Iranian Transportation Min-

istry's computer system was also hacked, severely disrupting operations. According to the same source, hackers were found to have engaged in intelligence gathering prior to their attack. An identical break-in tool was used for both hacks, disabling the computers by locking them and wiping their contents. The tool is called the Meteor Wiper [15]. This malware consists of 3 stages:

1. Defence Evasion (adding files/folders to exclusion lists).
2. Corruption of Master Boot Records.
3. Payload execution that corrupts and wipes files/folders on the victim's system.

Several cyberattack activities have been reported on many railways in several countries during the ongoing war between Russia and Ukraine.

A sophisticated ransomware attack targeting the Italian railway system disrupted ticketing and reservation services, causing widespread delays and cancellations. The threat actors demanded a significant ransom to restore operations. The attack exploited a vulnerability in the railway reservation system, which had gone unnoticed due to outdated monitoring tools. This allowed attackers to infiltrate the system undetected and deploy a ransomware. Furthermore, the railway's incident response plan proved inadequate, hindering efforts to contain the breach [16].

In Belarus, threat actors have allegedly breached computers that control country trains and brought some to a halt, part of what they say is an effort to disrupt Russian soldiers moving into Ukraine. They have compromised the railway system's routing and switching devices and rendered them inoperable by encrypting data stored on them [17].

According to the documentation provided in [2], the known cases in which OT systems were impacted were when entire networks were affected or when safety-critical IT systems were not available. Other types of cyber attacks on railway operators also include major data-leak attacks. These were the cases of OmniTRAX, MTA, Norfolk Southern Railroads and Lokaltog A/S, where personnel and medical records were stolen. The case of OmniTRAX represents the first publicly known case of a double-extortion ransomware attack against a US freight rail operator. The data was stolen with the threat of being publicly exposed, and at the same time, a ransomware attack blocked access to the same data.

Another interesting attack was that of the Danish train operator DSB's network to its ICT service providers after an alleged DDoS attack. The incident reportedly affected the accessibility of a key safety-critical IT system, thereby disrupting DSB operations for several hours that day [2].

2.4 Governance framework

The critical role that railway systems play in modern society requires strong cybersecurity practices from both operators and manufacturers. Regulations were established to ensure even operators that might be less inclined to implement best practices on their own to comply. In the European Union, the European Commission sets the direction, delegating implementation to member states. These states incorporate best practices, including recommendations from ENISA and the CENELEC 50701 Technical Specification. In the United States, Cybersecurity & Infrastructure Security Administration (CISA) plays a leading role, working alongside TSA to achieve similar goals.

2.4.1 Railway Cybersecurity Regulation in the European Union

The national and European governance are now “waking up” for this new reality and demanding, through legislation, the application of standards like [18] and [19] by railway product manufacturers, suppliers and cybersecurity control operators.

In 2008 the European Parliament approved the directive for European critical infrastructure in the energy and transport sectors, that Directive focuses exclusively on the protection of such infrastructure [20]. In 2022, the directive was repealed, due to evaluation it was recognized that because of the increasingly interconnected and cross-border nature of operations using critical infrastructure, protective measures relating to individual assets alone are insufficient to prevent all disruptions from taking place. Therefore, it is necessary to shift the approach towards ensuring that risks are better accounted for, that the role and duties of critical entities as providers of services essential to the functioning of the internal market are better defined and coherent, and that Union rules are adopted to enhance the resilience of critical entities. These critical entities should be in a position to reinforce their ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate, and recover from incidents that have the potential to disrupt the provision of essential services [21].

2.4.1.1 European Network and Information Agency

The European Network and Information Agency ENISA, was created by the European Union in 2004. It is responsible to advise and assist the European Union in all topics related with cyber security, as well as to build a bridge between all stakeholders (private and public), by encouraging cooperation and best practices related with cyber security. ENISA also promotes risk assessment and management methods to improve the response capacity to the latest cyber threats. By regulation (EU) 2019/881 [22], it was mandated to be responsible for the development of the European cybersecurity certification framework for products, processes, and services (including railway) that will be valid throughout the European Union. The member states are then responsible for moving the European

legislation to their national legislation.

2.4.1.2 European Union Framework

In terms of the regulatory framework applied to railway, there are three distinct major fields of competences:

1. **Railway safety**, which is related to the overall functioning of the system, which in turn consists of subsystems (infrastructure, rolling stock, control-command / signalling, operations, etc.), where the risks are mainly technical and environmental [13].
2. **Operating safety** is the ability of the components (doors, brakes, etc.) of a sub-system to meet one or more functions required under given conditions. It is used to establish demonstrations of the safety of technical subsystems [13].
3. **Cybersecurity** is a set of technologies, processes, and practices that aims to protect networks, computers, and data against attacks, damage, and unauthorised access. In an OT context, this is applied to cyber and physical safety [13].

This is a highly regulated sector, with safety authorities to enforce the rules, verify controls, and give authorisations. In the geographical space of the European Union, each member state was responsible for transposing Directive 2004/49/EC of the European Parliament and of the Council on safety on the railways of the Community which, in its first article, stipulates on every member state, the obligatory establishment of a railway safety authority [13]. The European technical regulation is above all an interoperability regulation, and includes railway safety issues for regulators and operators.

In an effort to improve interoperability, two European directives and a regulation were issued in 16 of June of 2019, to empower the role of European Union Agency for Railways (ERA). This entity is responsible for granting European authorisations for safety certificates, rolling stock, infrastructure, and signalling together with each national agency. For each new train or infrastructure, it must be authorized by the competent safety authority, and this regulatory compliance is mandatory. A comprehensive analysis of railway risks is performed for each system, enabling the demonstration of compliance with the mandated safety standards. Therefore, a train or infrastructure that meets the standards enforced by the regulatory framework will be considered safe to function [13].

However, it is important to mention that the railway rules and guidelines change from country to country. Requirements imposed by one Member State that are different from, or even in conflict with, those imposed by another Member State may substantially affect such cross-border activities. Furthermore, the possibility of inadequate design or implementation of cybersecurity requirements in one Member State is likely to have repercussions at the level of cybersecurity of other Member States, in particular given the intensity of cross-border exchanges [23].

An example of the diversity on railway guidelines, is a train that needs to go from Madrid to Berlin, will need to be able to use four distinct voltages, six signalling systems, and two rail gauges. The process of harmonization involves significant investments, lengthy implementation periods, and complex coordination efforts. To date, these efforts have primarily targeted European corridors used for high-speed rail and freight transportation between key terminals [13].

In simplified terms, the railway ecosystem can be broken into two primary domains: the technical objects, which encompass rolling stock, infrastructure, and signalling, and as the second domain, the organizational entities. These organizations are supported by human factors that are indispensable for their operational efficiency. Any new technical "object", in case it is a train or an infrastructure, must be authorised by the competent safety authority. For obtaining this authorisation, any organisation/manufacturer/integrator/operator which is applying for it, must demonstrate by means of a safety dossier that the object in question complies with the European regulations (called Technical specifications of Interoperability - TSI). This regulatory compliance is mandatory. It must be associated with an analysis of the railway risks, to prove the safety of the system. So an "object" that meets the standards requested by the regulatory framework will be considered safe to operate [13].

In the same way that the technical objects have to be authorised to function, each operator must also be authorised to get into service. For that, it must be inspected in terms of a safety management system (SMS), which will demonstrate its competence to identify and manage risk (management of documentation, maintenance, skills managements) and also the dissemination of a safety culture throughout the undertaking and the management of the organisational and human factor [13].

Risk analysis provides a shared understanding between authorized entities and safety authorities, enabling the identification of potential hazards and the implementation of appropriate safeguards. However, risk analysis does not address cybersecurity concerns directly, nor does it establish connections with agencies and organizations responsible for cybersecurity matters.

The European Commission Implementation Regulation European Union (EU) No. 402/2013 on the common safety method for risk assessment and evaluation, applicable to the railway sector, specifies that the risk should be evaluated using one or more of the following risk acceptance principles [24]:

- **Application of codes of practice**, following the prescribed regulatory specifications and standards is essential to maintain a satisfactory level of safety [13].
- **Comparison with similar parts of the railway system**, the operational history of the system has demonstrated its ability to ensure an adequate level of safety [13].
- **Explicit risk estimation**, it is frequently used for complex or innovative changes and where none of the two previous options can be used [13].

2.4.1.3 European Commission Regulation 2016/1148 (NIS 2 Directive)

Facing the number of cyber-related threats and the increase in the number and sophistication of IT attacks on critical infrastructure, such incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy of the Union, the EU commission has legislated on this matter in the Directive (EU) 2016/1148 [25]. It is essential that all Member States have minimum capabilities and a strategy that ensures a high level of security of the network and information systems on their territory. In addition, security and notification requirements should apply to operators of essential services and to digital service providers to promote a culture of risk management and ensure that the most serious incidents are reported.

Railway service providers are also stated as essential, so they are required to secure their most sensitive information systems by complying with the security rules. In the event of an incident to the security of the information system, they must immediately notify their national authority. One of the goals with this legislation is to raise the cyber security awareness level, in this case in the railway environment, and mitigate the impact when an attack occurs. Nevertheless, it also recognized in the legislation text that "Member States have very different levels of preparedness, which has led to fragmented approaches across the Union" [25], so there is still a long path to follow to bring all the member states to a good cyber security level. This directive was repealed in December 2022 by (EU) 2022/2555 [23]. It sets out minimum rules regarding the functioning of a coordinated regulatory framework, by laying down mechanisms for effective cooperation among the responsible authorities in each Member State. It also updates the list of sectors and activities subject to cybersecurity obligations by providing effective remedies and enforcement measures, which are key to the effective enforcement of those obligations.

2.4.1.4 European Commission Regulation 2024/2847 (Cyber Resilience Act)

Following the NIS 2 referenced in Section 2.4.1.3 that affects railway operators, now software and hardware manufacturers will have to comply with EU Cyber Resilience Act (CRA) [26]. The CRA introduces mandatory cybersecurity requirements for manufacturers and retailers, governing the planning, design, development, and maintenance of such products. These obligations must be met at all stages of the value chain. The act also requires manufacturers to provide care during the lifecycle of their products. Some critical products of particular relevance for cybersecurity will also need to undergo a third-party assessment by an authorized body before being sold on the EU market [27].

An example of products that must comply with this regulation is network equipment, such as routers and switches, access control readers, and biometric readers.

The economic operators and Member States will have 36 months to adapt to the new requirements starting from December 2024 when this legislation was formally adopted [26]. Similarly to the NIS 2 Directive, the manufacturers have also reporting obligations, when the manufacturer becomes aware of any actively ex-

exploited vulnerability contained in the product with digital elements, it shall notify simultaneously to the CSIRT designated as coordinator and to ENISA. Unless relevant information has already been provided, a vulnerability notification, without undue delay, and in any event within 72 hours of the manufacturer becoming aware of actively exploited. This shall provide general information, as available, about the product with the digital elements concerned, the general nature of the exploit and the vulnerability concerned, as well as any corrective or mitigation measures taken to mitigate the vulnerability [26].

2.4.1.5 CENELEC

In terms of European standards, the European Electrotechnical Committee for Standardization is one of three European Standardization Organizations (together with CEN and ETSI), CENELEC has been officially recognized by the European Union and by the European Free Trade Association (EFTA) as being responsible for developing and defining voluntary standards at European level [28].

The CENELEC TS 50701 “Railway Applications – Cybersecurity” [18] is the first document that specifically addresses the railway environment, including rolling stock, signalling, and infrastructure in the geographical space of the European Union. Provides references to models and concepts from which requirements and recommendations can be derived and that are suitable to ensure that the residual risk from security threats is identified, supervised, and managed to an acceptable level by the railway system duty holder [8].

2.4.2 Railway Cybersecurity Regulation applied in the United States

In the United States the agency that establishes cyber security requirements at the top level is CISA, this agency belongs to the Department of Homeland Security. CISA does not make cyber security regulation for essential organizations, it only defines the high-level requirements, and then for each sector it relies on the regulatory body, to design specific requirements, in the case of the railway sector, it is TSA [29].

TSA is responsible for harmonizing the cyber security requirements across the U.S.A. market, the harmonization is enforced by the TSA directives, namely, at the date of writing it is TSA Security Directive 1580/21-01, released on Dec. 31, 2021 [30] and 1580/82-2022-01 released on Oct. 24, 2022 [4].

2.4.2.1 TSA Security Directives 1580/21-01 and 1580/82-2022-01

The TSA Security Directive 1580/21-01 [30] has four critical actions, which require all freight railroad carriers to designate a Cybersecurity Coordinator to:

- Be responsible for the implementation of cybersecurity practices.
- Manage incidents, be the point-of-contact with the agencies 24x7d and report incidents.
- Develop a cybersecurity response plan.
- Perform a cybersecurity vulnerability assessment.

The TSA Security Directive 1580/82-2022-01 [4], requires railroad owners / operators to implement several cybersecurity measures to prevent or mitigate the impact of a cyber attack. Namely, to put into place a TSA cybersecurity implementation plan, that should include network segmentation policies and controls, to ensure that the systems continue to operate even under attack. It should determine zone boundaries, and in which cases, the Information Technology and Operational Technology system services data is crossing from one zone to the other. This boundary crossing can only occur when strictly necessary for business or operational purposes. It should detail which measures are put in place to secure and defend each zone. It demands the deployment of access control measures to the areas of Critical Cyber Systems. It should implement Multi-factor Authentication, that supplements password authentication to provide risk mitigation. If these measures are not implemented, it needs to justify what controls are being taken to compensate.

The Security Directive 1580/82-2022-01 [4] also dictates the implementation of monitoring and detection policies, which should detect and correct anomalies that affect the systems. These policies must also include capabilities to detect and defend against phishing and spam, known or suspicious web domains, mail content such as macros, and harmful scripts. From an auditing perspective, the plan should ensure that the controls are capable of detecting any access to unauthorized domain, or any communication between OT systems and any external system. The system should continuously log potential intrusions and anomalous behaviour related to OT systems, retaining these logs for a sufficient period to enable effective investigations, if necessary (albeit such processes may become increasingly complex as the number of endpoints, devices and even the amount of persisted data increases [31], eventually calling for domain-specific forensics methodologies [32]). It must ensure that security patches are applied promptly using a risk-based approach.

Finally, it requires setting up a Cybersecurity Assessment Program, and submit an annual plan to TSA describing all the implemented measures, and how they are maintained to identify and resolve network and system vulnerabilities. The plan should include, an architectural design review that must be conducted every two years. To be compliant, the documentation should focus on all the topics mentioned above, plus hardware and software asset inventory. The inventory should also contain firewall rules, network diagrams, switches, and router configurations. It may be required a snapshot, with packet capture of network traffic not exceeding 24h, "East-West" traffic between OT system, and "North-South" traffic between OT and IT [4]. After the effective date of this security directive [4], system owners have only 120 days to submit all the documentation. If there is any

change that affects the security conditions, it is required to submit an amendment to the initial Cybersecurity Implementation Plan.

These TSAs impose more strict reporting measures than the European regulation. Although European operators must fulfil similar technical requirements from the cybersecurity perspective, the European legislation does not require the submission of the documentation to the regulatory authorities without previous request. It also does not require the submission of the configurations of network and security devices, nor logs. Normally, this information is only analysed by the national authorities in the case of a security incident, or by request of the railway operator, as stated in the NIS 2 Directive [23]. According to the same directive, the railway qualifies as an operator of essential services, so it has reporting obligations. Railway operators should submit an incident notification without undue delay and in any event within 72 hours of becoming aware of the significant incident [23]. It is the railway operator's responsibility to take a proactive approach to cyber threats and to make the best effort to comply with CENELEC TS 50701 [18].

2.4.2.2 American Public Transportation Association Recommended Practices

As the legislation for Railway cybersecurity is imposed in the United States by the TSA directives [30] and [4]. In the European Union, there is no defined standard, until now only technical recommendations and guidelines. These are given by [18]. In a similar analogy, for the United States, the recommended guidelines for technical details on implementation are given by the recommendations of the APTA-American Public Transportation Association. The purpose of these recommendations is to share TSA best practices and to establish a minimum requirement for security control within the transportation industry [33]. Within these guidelines, four are notable, the APTA SS-CCS-RP-001-10 [33], APTA SS-CCS-003-15 [34], APTA SS-CCS-RP-002-13 [35] and the APTA SS-ECS-RP-001-14 [11].

2.4.2.3 APTA SS-CCS-RP-001-10 Elements, Organization and Risk Assessment / Management

The APTA SS-CCS-RP-001-10 [33] "Securing Control and Communications Systems in Transit Environments Part I: Elements, Organization and Risk Assessment/Management", addresses the importance of cybersecurity in the railway IT/OT environment for railway agency or operator. It depicts the various subsystems that build a typical railway control and communication system. It also clearly identifies the necessary steps that establish the stages in conducting a risk assessment and managing risk in an enterprise environment. One big difference from CENELEC TS 50701, is that although APTA SS-CCS-RP-001-10 is not so profound in the technical aspects, it gives a more clear vision in terms of a management and enterprise perspective. It shows the need to communicate with the board of directors, explains what the steps inside an organization are to get budget approval to implement the control measures, and how to present it to the board.

It begins by describing the purpose of a typical transit control and communications system and its complexity. It states that the equipment monitored by a transit control center may include a large number of functions, and it segregates the system into two major types:

- Legacy or closed - These are non-computer-type systems or stand-alone systems (see Figure 2.2) that may or may not be processor-based but are not accessible externally by any means, including laptop, network and peripheral devices. These systems require physical and administrative security.
- Advanced technology - These are computer-based systems that may have remote connectivity. They may be stand-alone systems or have some level of integration with other systems in the control center and may include connections to other systems or agencies outside the control center (see Figure 2.3). These systems require physical, administrative, and cyber security.

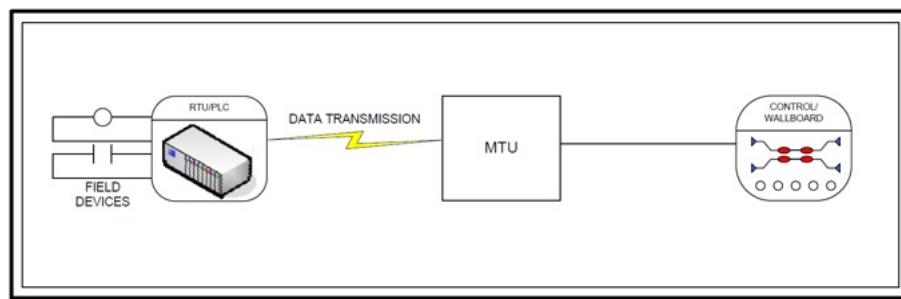


Figure 2.2: Legacy Stand-alone System, Closed (Mainly Physical and Administrative) [33]

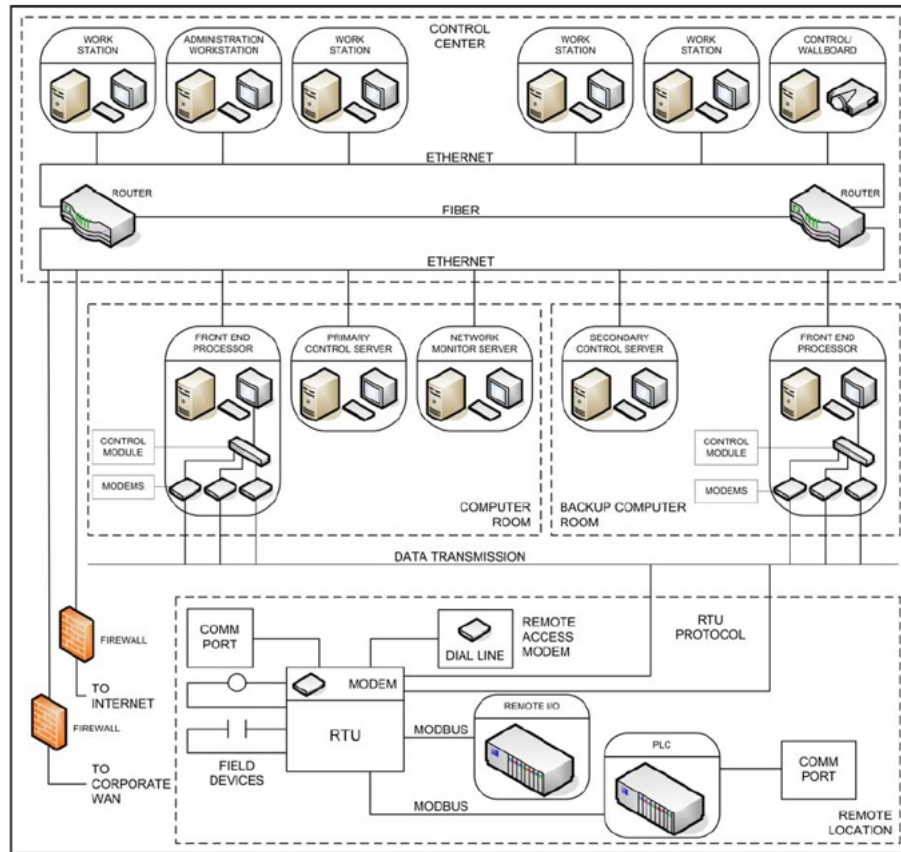


Figure 2.3: Interconnected System (Partially Integrated) [33]

There is clearly an effort to cover both legacy and newer technologies. Although, compared with TS 50701 [18], in the European guideline there is a complete annex only for legacy systems, in the APTA guidelines the focus is not very detailed, it is clearly more focused on major system upgrades or new systems and not the legacy ones.

The documentation provided in [33] details the operational requirements of transit environments and why control systems are essential for centralized supervision, as they can control numerous network devices and subsystems. Although some control systems are specialized for specific tasks, such as train control or vehicle tracking, others offer integrated solutions that encompass multiple functions from signalling to train Integrated Traffic Management to optimize train traffic flow.

Several systems are described in [33], starting with the Train Control systems, which provide Automatic Train Supervision ATS, and may include control capabilities in the control center. Train control systems may also provide Automatic Train Protection ATP and Automatic Train Operation ATO for train safety and control of train movements, directing train operations on the main line and in the train yards. SCADA systems as power substations, traction power, control of emergency HAVAC systems are also covered.

The next core area is data transmission systems, with a focus on wireless communications and the various types of technologies used. These can go from WLAN

or Wi-Fi (IEEE 802.11) to ZigBee technologies (IEEE 802.15.4), and others. It explains the use of each technology, depending on the purpose and what protocols and safeguards should be used in a correct wireless technology in the industrial environment. The reason for this focus is due to the large number of wireless networks that can be found in the transit system and how it becomes such a critical point.

Another system described is the fare collection system; since these are frequently linked with financial systems, such as credit card companies, these are strictly governed by financial standards and regulations (including PCI and CFMS, etc.). This fare systems should be on a segregated network (even though sometimes they are not), and require appropriate security controls to avoid or mitigate attacks like the one described above in Thanksgiving attack.

After the several systems have been described, it is detailed how to organize a control system security program, with all 4 phases:

- **Phase 1:** Awareness of security plan, establishment of a security team. The purpose of this section is to ensure that management understands the need for security in the environment of transit control systems. This step aims to ensure that the appropriate people in the transit agency are aware of the consequences if a security program is weak or non-existent [33].
- **Phase 2:** Risk assessment and funding of the security plan. The risk assessment will be the focal point of the security program, as it identifies all systems, equipment, data paths, computer operating systems, and the physical location of all equipment (so cyber and physical aspects of security should be reviewed). The loss of functionality will then be examined to determine the consequences that will occur to the agency, measured in either loss of money, deterioration of service revenue, loss of life, or physical safety of the public or agency personal or equipment. The outcome of the risk assessment will be used in the development of the security plan countermeasures [33].
- **Phase 3:** Development of the security plan and security countermeasures. The development of the security plan will be detailed and requires time to explore the control and communications system infrastructure, policies, and procedures, and to develop adequate security measures to address the recommendations resulting from the risk assessment. The plan will include physical and cybersecurity measures for all systems and equipment including existing (legacy) equipment, new system procurement, equipment maintenance and support, it is at this stage where all the stakeholders are clearly identified and its responsibilities, as well as policies and procedures.
- **Phase 4:** Implementation of security plan measures and maintenance plan.

This ends part I of the recommended guideline, and it is followed by part II.

2.4.2.4 APTA SS-CCS-RP-002-13 Defining a Security Zone Architecture for Rail Transit and Protecting Critical Zones

In the "Securing Control and Communications Systems in Transit Environments Part II: Defining a Security Zone Architecture for Rail Transit and Protecting Critical Zones" [35], it is assumed that the railway operator has conducted the risk assessment of part I. Now it explains the Defence-in-Depth approach that will be established for the control and communication system, defining security zone classifications and a minimum set of security controls for the most critical zones.

As described earlier, the railway control and communication systems and subsystems are quite complex, with equipment that moves along the railroad tracks. Its control systems can be located buried under or alongside the rail lines, throughout the routes in wayside bungalows, stations, road crossings, signal towers, tunnels, maintenance yards, power stations, refuelling depots, equipment storage yards/parking lots, storage depots, local control rooms and operations control rooms [35].

As not all systems and zones have the same importance, they must be categorized from Most Public to Most Safety Critical. These can span from the communication with business partners and vendors, for scheduling purposes, up to the field signalling and interlocking that are responsible for safety to of the transit. See Table 2.2

Importance	Zone	Example System
<div style="display: flex; align-items: center; justify-content: center;"> <div style="writing-mode: vertical-rl; transform: rotate(180deg);">Most Safety Critical</div> <div style="margin: 0 10px;">↑</div> <div style="writing-mode: vertical-rl; transform: rotate(180deg);">Most Public</div> </div>	Safety- Critical Security Zone (SCSZ)	Field signaling and interlocking
	Fire, Life-Safety Security Zone (FLSZ)	Fire detection/suppression
	Operationally Critical Security Zone	Traction power SCADA
	Enterprise Zone	Fare systems, turnstiles, accounting systems, schedule systems
	External Zone	Communications with the Internet, business partners, vendors and others

Table 2.2: Zone Importance [35]

As nowadays these systems are more interconnected, via networking standards like Ethernet, as in principal rail links between big towns and cities (Main Line) operations. Due to the long distances, there is the tendency for the operators to use the same communication conduits, and this reuse may create vectors for cyber-attacks. The use of radio broadcasting signals in clear text is also a vulnerability that can be used as an attack vector [35]. As an example radio broadcasts from freight trains in the US can be listened online in some websites [36].

The number and type of security controls to be implemented often depend on the nature of the systems. This is the case for real-time and time-sensitive domains, such as the communication between the interlocking (IxL) system in the field, and the regulation system operating in the Control Center, which controls the train movement by opening and closing of the track signals. Due to their criticality, these systems are not expected to have any downtime or performance degradation in terms of deterministic behaviour as such, the use of specific exe-

cution environments [37], anti-virus, whitelisting mechanisms, firewalls, or other cyber-defence mechanisms, may cause disruptions by introducing lag in the communications, and in that sense, disturb operational characteristics. As such, these must be carefully evaluated. For control systems the two items integrity and availability of the CIA triad are of vital importance, so that calculations can be made, so that trains can be stopped or started and so that crossing gates go up and down appropriately, the confidentiality has less importance compared with the other two.

In the Cybersecurity approach of the document, it is defined what should be protected, and how to prioritize it. For rail, the most critical systems to protect are those that involve the highest risk to life and property: such as control and communication systems that let the train or train operator start, control the speed of or stop the train [35].

APTA defines 4 key parts for protection:

- **Prevention:** Keep anyone or anything from tampering with the system [35].
- **Tamper detection:** Detect when an unauthorized change has occurred or is occurring [35].
- **Auditable:** If someone tamper with the system, determine who, what, where, when and how [35].
- **Tamper detection and auditability** ensure appropriate personnel are notified of unauthorized or abnormal activity and can respond in a timely manner to take action as required [35].

The Defence-in-Depth methodology approach is the recommended strategy for securing communications and control systems for the railway sector. The methodology recommends a balance between protection capability, cost, performance, and operational considerations. It requires that first the agency should identify zones and boundaries, defining its controls that protect information and transactions as they move across zone boundaries. It should not only be applied a defence-in-depth, but combined with Detection-in-Depth, that is, a way to detect that a malicious actor has access to the railway infrastructure. As a consequence, detection methods should be implemented, the basic rule of least privilege tells us to first block all traffic, and then create permission for known and necessary inbound and outbound connections.

The documentation provided in [35], also states that a compliance and audit program must be created to ensure that all controls are in place as designed. This should be reviewed periodically, to assess its effectiveness and if there is the need to implement more controls or change the existing ones.

The next step is to define the risk zones, to put in place what have been previously described. APTA adopts the Department of Homeland Security model for the manufacturing industries. This model is very similar to the Purdue model [38] see Figure 2.4, but in this case, instead of 5 levels, only 4 are defined see Table 2.3.



Figure 2.4: Purdue Zone Model for OT [38]

Zone	Description	Security Priority	Ref. Number
External Zone	The area of connectivity to the Internet, peer locations, and backup or remote offsite facilities. This is not a demilitarized zone (DMZ), but it is the point of connectivity that is usually considered untrusted.	Lowest	N/A
Corporate Zone	The area of connectivity for corporate communications. Email servers, Domain Name System (DNS) servers, and IT business system infrastructure components are typical resources in this zone.	Medium	1
Manufacturing/ Data Zone	The area of connectivity where a vast majority of monitoring and control takes place. It is a critical area for continuity and management of a control network. Operational support and engineering management devices are located in this zone alongside data acquisition servers and historians. This zone is central to the operation of both the end devices and the business requirements of the Corporate Zone.	High	2
Control/Cell Zone	The area of connectivity to devices such as programmable logic controllers (PLCs), HMI and basic input/output devices such as actuators and sensors.	Very High	3
Safety Zone	The area that controls directly and often automatically the devices that control the safety level of an end device, such as safety instrumented system.	Extremely High	4

Table 2.3: DHS Zone Model [35]

As described in APTA-SS-CCS-RP-002-13 [35], the main differences between a manufacturing site and a railway system are:

- **distance** - A rail system covers a wide distance, and each segment of the rail system has to communicate with its adjacent segments and with the operations control center.
- **communication** - several types of wired and wireless communication, with maintenance crews, engineers, done along great distances and in all kinds of weather, where Line-of-sight (LOS) communication can be difficult due to nature (snow, plant growth, downed trees) and in an electrically noisy environment that is difficult to shield.

- **power** - Transit systems often have independent traction power stations to supply electricity. Power is sourced from local utilities and distributed through catenaries or third rails. Auxiliary power is necessary for various systems, including lighting, communications, and signalling. A notable difference from standard commercial systems is the use of a floating ground electrical configuration.
- **people** - The primary objective of a transportation system is to transport people safely. Unlike manufacturing environments with limited and controlled human access, transportation systems must prioritize the safety of a large number of passengers. Although a manufacturing plant has people to operate and secure the plant, transportation systems can be a much more compelling target due to the vast number of people who use it and the immediate impact of an attack on passengers.
- **access to property** - Compared to a manufacturing site, the railway system is in the public domain, even the toughest efforts to enforce access control, it is impossible to keep single-minded individuals away from the assets of the transportation system [35].

As described, security zones can extend to several physical locations, so the agency must have a way to implement security across these zones and control physical access and permissions to critical systems. In Figure 2.5 we get a perspective of the allocations in terms of several security zones, Enterprise Network, Operationally critical, Life safety, and safety critical.

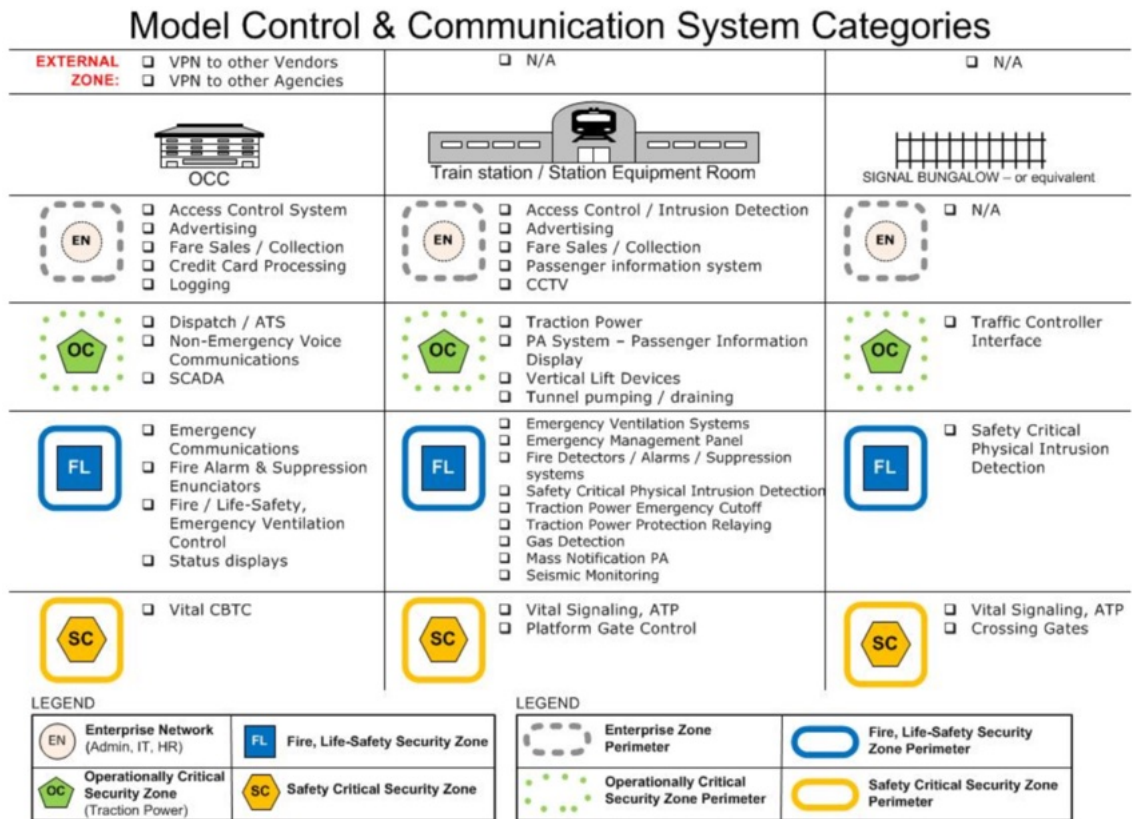


Figure 2.5: Model Zone Chart for Transit Systems [35]

There should always be a balance between putting too much into the more secure zones and at the same time not turning it into an opportunity for an attack. This means that you should not only secure the most critical areas, meanwhile leaving other zones more prone to attacks. Although all zones should be secure, they should not be mixed. Only the most critical systems should be in the most critical zone. Putting something into a more secure zone should not be done lightly, only when necessary to achieve an acceptable level of risk. The functions and services of one zone should not be combined with one another zone without proper segregation. It may create covert channels that an attacker can use to control an agency's systems, sometimes business decisions do not consider the risk and cost of mixing functions.

In the guideline, the system security and minimum controls for Safety Critical Zones are described, with a detailed description and examples of what type of control should be applied in each zone and how to interconnect different zones. In Figure 2.6 an example is given on how these recommendations are presented.

Ref # B	Version 1.0	Aud. TA	When Now	TITLE: Connecting security zones of different security levels
Reference: SP 800-53 Primary:				CONTROL: All network-routable interfaces connecting the SCSZ or FLSZ with a less-critical security zone should use an isolation device (defined below) to ensure security separation.
Reason for control <p>The Defense-in-Depth strategy used in this <i>Recommended Practice</i> requires routable (TCP/IP based) network connections to have a device to allow authorized traffic and to prohibit unauthorized traffic between the SCSZ and FLSZ and other less-critical zones.</p>				
Discussion <p>An isolation device may be a hardware-based firewall to filter traffic at TCP/IP stack layers 2, 3 and 4 (corresponding to link layer, IP layer and TCP layer). If technology is available, filtering at the Application Layer is also desirable (see Appendix B for more information)</p>				
Measures of effectiveness <ul style="list-style-type: none"> Unauthorized network traffic is recognized and stopped at the Isolation Device 				
Examples <ul style="list-style-type: none"> Acceptable: <ul style="list-style-type: none"> Hardware-based firewall as described above. Not acceptable: <ul style="list-style-type: none"> Using a dual-homed personal computer to connect to a SCSZ or FLSZ network and also a lesser security zone. 				

Figure 2.6: Connecting security zones of different security levels [35]

This guideline also focuses management responsibility on training programs, that are commonly forgotten and are essential for the cybersecurity program to be effective. Configuration management and patch management are also depicted. Focuses on firmware and software that may need to be modified or patched for both functionality and vulnerability, requiring an annual audit to assess it. The transit agency must coordinate with the vendor so that updates can be applied without compromising safety and security. Certified vendor patches should be supplied for both proprietary and Commercial off the Shelf firmware and software, which are part of the vendor's equipment [35].

The guideline ends with a table that gives security controls applicable within the safety critical security zone electronic security perimeter. It calls attention to the fact that before implementing any cybersecurity controls, a thorough analysis must be performed to ensure that the controls cannot adversely impact the functions implemented in that perimeter.

Two examples on how to apply the security controls into zones are presented, and defines each electronic security perimeter and the control for each border. Figure 2.7 is one of the examples shown, it illustrates the application of safety critical security zone requirements to a generic signalling bungalow using a block signalling approach. Note that firewalls (isolation devices) protect the routable network connections.

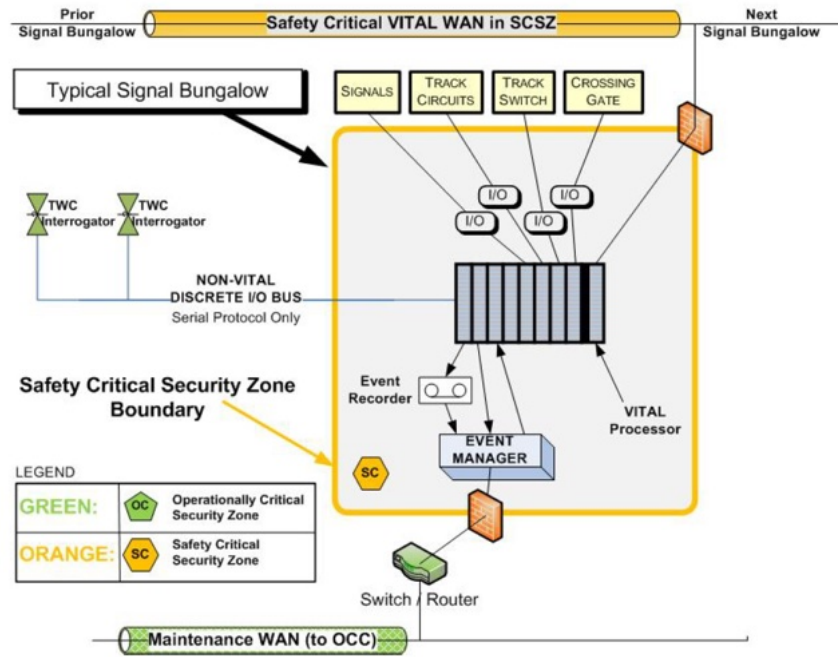


Figure 2.7: Safety-Critical Testing [35]

2.4.2.5 APTA SS-CCS-003-15 - Attack Modelling for Rail Transit

The third part of the document presents the attack modelling method to analyse security in critical zones of the railway system. It makes use of attack trees used as a graphical representation of how the system can be exploited, voluntarily or not. This approach is very similar to the one already used in the railway ecosystem, the fault tree, but the fault trees do not include actions of harmful intent [34].

Fault Tree Analysis (FTA) is a systematic method that is used to identify potential failures within a system and their potential consequences. It involves breaking down a complex system into simpler components and analysing how these components can fail to lead to a specific undesirable event, often referred to as a "top event" [39].

FTA can be qualitative or quantitative. In a qualitative FTA, the focus is on identifying potential failure modes and their relationships. In a quantitative FTA, probabilities are assigned to basic events to estimate the likelihood of the top event occurring [39].

The primary objectives of FTA are to:

- **Identify potential failure combinations:** Determine all the ways in which basic events can combine to cause the top event.
- **Estimate event probabilities:** Calculate the probability or frequency of the event that occurs the most.
- **Prioritize improvement areas:** Identify system components or processes that, if improved, would significantly reduce the risk of the top event.

FTA utilizes logic gates to represent the relationships between events. Common logic gates include:

- **AND gate:** The top event occurs only if all input events occur.
- **OR gate:** The top event occurs if any input event occurs.
- **PRIORITY AND gate:** The top event occurs only if all input events occur in a specific sequence.
- **EXOR gate:** The top event occurs if exactly one input event occurs.
- **INHIBIT gate:** The top event occurs only if a specific input event occurs and additional conditions are met.

By visually representing the failure modes of the systems and their logical connections, FTA provides a powerful tool for risk assessment and decision-making [39]. Figure 2.8 shows an example of a fault tree analysis.

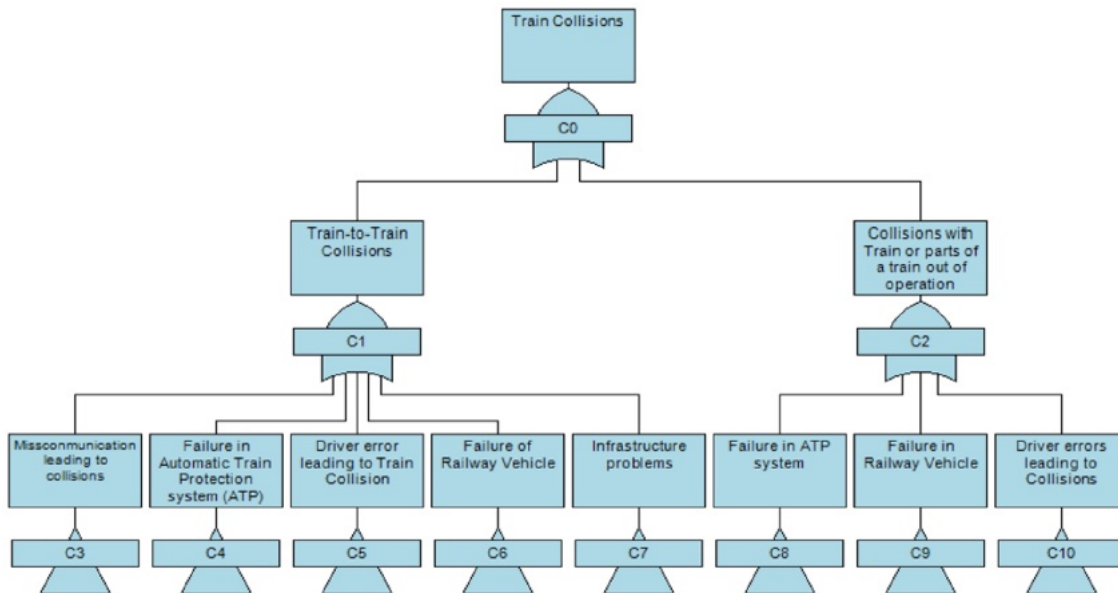


Figure 2.8: Fault tree analysis of train collisions [39]

In the same way as the fault trees, the explosion or derailment as the ultimate consequence that we are trying to prevent goes on top of the tree. For cybersecurity concerns, the attack trees may also include Denial of Service, as it impacts the normal flow of the railway traffic, or any data breach as a consequence to be avoided sitting on top of the attack tree.

The need to use attack trees is to mitigate security concerns in the design of new communication and control systems. To ensure that all parties are viewing security considerations in the same way, as well as to ensure that it used the same method to examine the risk associated with different threats. This technical recommendation foresees that the system integrator will do the attack modeling with the help of vendors, while the agency engineers will oversee it. This modus operandi is recommended due to the complexity of this technique. It is advised

to use the attack modelling in the preliminary design stage, and in the final stage, to evaluate alternative architectures and, respectively, when vendor's products have been chosen. Due to the financial costs and impacts of this technique, it should be established a trigger of when to use it, based on the size and scope of the project, if the support of a vendor is required due to the complexity, and also based on the magnitude of the cybersecurity question to be answered.

What should we model? Also related to financial impact, it should be taken into consideration where to apply it. Only sections of a new design or concept that need a thorough analysis to answer the security question posed should be modelled. It should be emphasized that the attack modelling should be precise, it will try to present an answer to a particular security question in a well-defined event that should be located on the top of the tree [11]. So, it should be contained to the smallest area that accommodates the issue.

To start modelling the attack tree, two other critical details should be defined, the team that will be involved, and the necessary tools. For the team, the agency recommends an attack tree modelling expert that should be at the same time the team leader, a railway operator representative. For the necessary tools, depending on how complex the modelling will be, it could be necessary to use an attack modelling software, APTA recommends the SecurITree® [40] by Amenaza Technologies Limited and Isograph+ or open-source applications such as ADTool [41] and Poseidon Community Edition. Documenting network software similar to MS Visio®. Expected deliverables may include a management summary, committee minutes, important high-level attack tree scenarios, and attack tree files. It should be taken into account that the results should be presented in a way that management will understand the impact on operational activities and facilitate executive decision making.

Attack modelling should be decomposed into several phases.

1. Characterize the system that we need to model; this should be composed of an asset list of all hardware and software within the scope, including a network diagram to completely describe how the assets in the area that are being modelled are interconnected. The trust boundaries should also be defined; those are an imaginary logical or physical perimeter that circumvent the area that is being modelled. Finally, what are the entry and exit points of the defined boundary.
2. In the second phase, it should describe the normal sequence of operations, start/shutdown, normal operation, maintenance/update.
3. Identify threats to the system; for this, there should be three perspectives an authorized user that makes an accidental mistake, a malicious insider, and a malicious outsider.
4. With all this information, the next phase is to build the attack trees. The guideline demands that there should be one for each of the following scenarios:
 - Accidental misuse by an authorized user.

- Malicious insider and outsider.
- Collusion between malicious insider and outsider.
- Physical and cyber possibilities.

When building attack trees, it is a good practice for the team to question the original assumptions bearing in mind what can be seen in the tree. For example, if an assumption was made that “all our employees are perfectly loyal”, it is worth going through a “what-if” scenario, and asking “What if this assumption is wrong? What would happen to my attack tree?” and examining the consequences [34]. The probabilities of the events described in the attack tree should also be reviewed to possibly eliminate the most improbable. Once the tree is drawn, the attack modelling team should make a decision on the type of evaluation to be implemented: to work with attack scenarios qualitatively (without assigning relative probabilities) with the short method, or to proceed with full (and more lengthy) analysis using risk/probability features of attack tree software. In Figure 2.9 is an example of an attack tree for a derailment in the interlocking that may result from the following actions:

- Tamper with rail itself (loosen section, cut rail, remove section, etc.).
- Tamper the signal light to always read green.
- Tamper with switch.
- Break into signal bungalow, install jumpers.
- Install an unsafe application file on the vital Programmable Logic Controller (PLC) (master scenario under study).

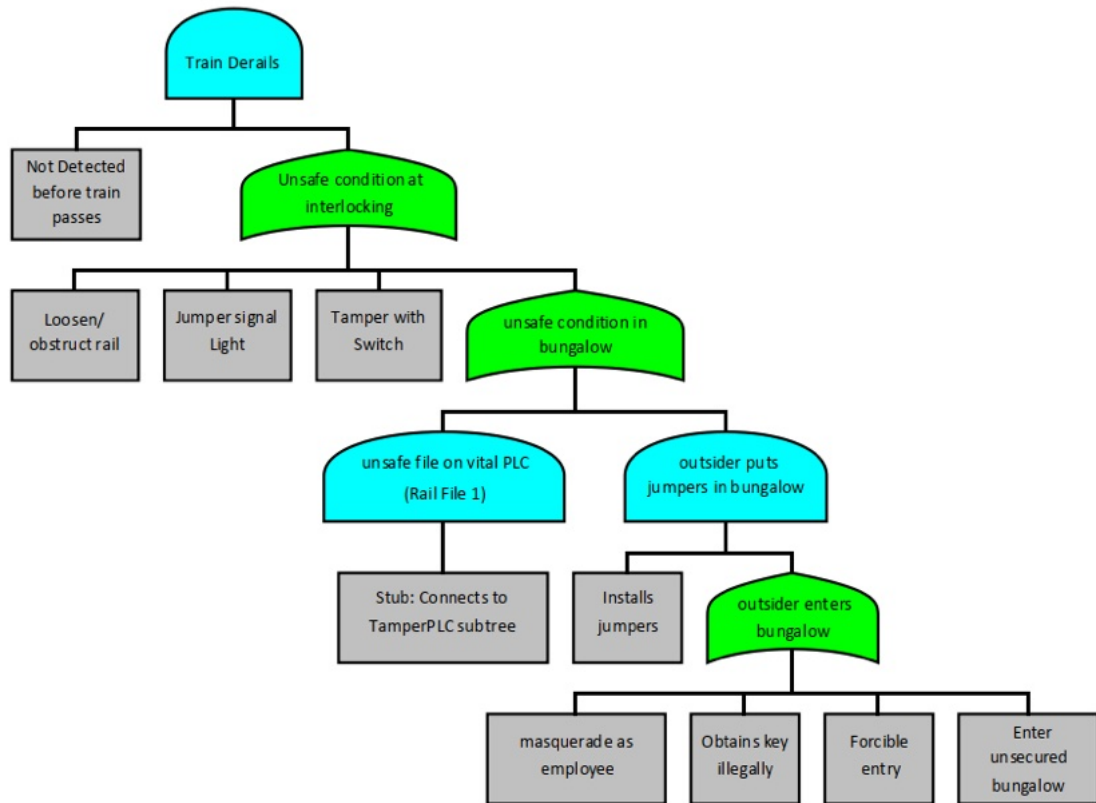


Figure 2.9: Overall Derailment Attack Tree [34]

2.4.2.6 APTA SS-ECS-RP-001-14 - Cybersecurity Considerations for Public Transit

This recommended practice document starts by describing the national security of the United States, and what are the administration's main cybersecurity goals to improve resilience and reduce cyberthreat. These goals should be achieved with the 4 priorities in mind:

1. Standards, policies, and procedures.
2. Information system technology and infrastructure.
3. Awareness, training, and education.
4. Information security risk management integration.

The presentation of the priorities is followed by a characterization of the cyber-threat landscape. The CIA triad is described and where the OT ecosystem differs from the IT one in a Cybersecurity approach. It is also explained why integrity and availability are the main priorities and confidentiality is relied upon as not so critical. What are the main threats to the railway system, and because these are critical infrastructures, they are prone to attacks motivated by politics and financial interest. It is also stated that geopolitically motivated threat actors have targeted transportation systems as part of larger attempts to discredit or block a country or region [11].

To help understanding the several systems that form the railway environment, and the ones which it could possibly interact, a detailed description of each one is presented, namely:

- **Operational systems** - Transit agencies rely on operational technology OT systems —Industrial control systems (ICS) —to manage essential services such as train and traffic control, passenger access, and more. Traditionally isolated ("air-gapped") on dedicated networks, these OT/ICS systems are now increasingly connected to enterprise IT systems due to advances in IT infrastructure, digital transformation initiatives, and evolving business needs.
- **Enterprise information systems** - An agency's Enterprise information system (EIS) encompasses its entire IT platform, addressing all information and technology needs. The EIS integrates the organization's core functions and can be broadly divided into three subcategories.
 - Infrastructure systems - are the core backbone of enterprise information technology and include networks, compute and storage, operating systems, and hypervisor technical services [11].
 - Application systems - primarily consist of user-interfaced software. Application systems are often considered at the highest risk for cyberattacks, particularly networking-capable applications such as email and web browser applications [11].
 - Business enterprise systems - are specialized applications that are specifically responsible for managing the agency's confidential information and daily business functions. Such systems include Enterprise resource planning (ERP), Customer relationship management (CRM), Knowledge management system (KMS) and Supply chain management (SCM) [11].
- **Cloud service** - public transportation agencies, are using cloud service provider (CSP) to varying degrees, as it has become cost prohibitive in some cases to provide some technology services by internal IT teams. Many applications and service providers are now offering cloud-only solutions [11].
- **Managed service providers (MSP)s** - can offer a range of services, including cybersecurity monitoring, threat detection and response, financial transaction processing, maintenance of support system, payroll management, customer and employee data handling, and other essential operational functions. Transit agencies must ensure that third-party vendors are compliant and meet specific information security requirements in order to provide or perform critical services [11].
- **Passenger information systems** - are automated systems that provide users with information on the nature and state of a transportation service through visual, voice, or other means. The information can be static or real-time. Real-time information is provided to passengers in several ways, including platform-level signage, mobile phone applications, integration with existing third-party map applications, transit applications, and automated public address systems [11].

- **Fare collection systems** - are the service created by integrating various technology components that automate the ticketing and ticket validation systems of a public transportation network. Fare collection systems now support integrated ticketing, which allows a person to make a journey that involves transfers within or between different transport modes with a single ticket valid for the entire journey [11].
- **Transit communication systems** - are technologies that pass information from one user to another in a usable form via wire, wireless, radio, the internet, or other links. Communications technologies like TERrestrial Trunked RAdio (TETRA) facilitate the interaction among drivers, dispatchers, emergency responders, and other personnel involved in transit and transportation operations.
- **Physical security systems** - protect people, property, and physical assets from actions and events that could cause damage or loss. This includes physical deterrence, detection of intruders and responding to those threats [11].

Taking into consideration what has been described by the recommended practice so far, it is now shown how it integrates with the NIST Cyber Security Framework and its four pillars of identify, protect, detect, respond, and recover. As reinforcement of [33], the risk management process is once again reviewed based on the NIST key concepts and principles established in the NIST 800-30, "Guide for Conducting Risk Assessments" [42] and NIST 800-39 [43], "Managing Information Security Risk". Compared with [33], this is more an update of what was already previously covered by [33] as it was issued in 2010. APTA SS-ECS-RP-001-14 shows a new focus on system contingency and resilience with the several plans that make up the Contingency Planning Process, the 7 phases can be seen in Figure 2.10. In addition, a focus on the Systems Development Life Cycle (SDLC), where security by design, that which is to integrate cybersecurity from the beginning of the project into the SDLC, to cover each of the stages from the beginning till the end of the IT system. In this way, major delays and costs associated with the requirement of including cybersecurity in the software are avoided.

Using the SDLC process, railway operators manage their OT systems more efficiently. There are a variety of SDLC, but generally cover five dominant phases: initiation, development/acquisition, implementation, operations / maintenance, and disposal. As the main objectives are to maintain information security, ensure confidentiality, maintain integrity, and availability in each phase of SDLC. Using the security activities described within each phase developed by NIST SP 800-100 [44], railway operators will achieve a broad understanding of which activities imply SDLC to secure their infrastructure.

It is also recommended in the documentation provided by [11] to incorporate a Managed security service provider (MSSP) [45], this is an outsourced asset. It will speed up the process, since the railway operator will not need to hire security personnel and will not spend time on their training and retention, as well as MSSPs provide monitoring and management of security devices and systems, and use high-availability security operation centers (either from their own facilities or from other data center providers) to provide 24/7 security services.



Figure 2.10: Contingency Planning process [11]

Compared with TS50701, the APTA SS-ECS-RP-001-14 [11] is more based on the NIST framework, TS50701 is an autonomous document that does not push you to look into other publications. The documentation provided in TS50701 also presents a deeper detail of the risk assessment phases, well detailed with flow diagrams, and input and output documents of each phase, as it is also completely customized for the railway ecosystem, in opposition to the NIST perspective, which is suited for a more generic view of the ICS systems, which of course includes the railway systems.

2.5 Difference between Safety and Security in Railway

Safety is deeply embedded in the railway industry, even more nowadays as railway classified as safety-critical, due to severity of a the possible impact if a failure occurs. The approach to this kind of industry is "safety above all" as stated in [46], so to be certified for public use, the system and its subsystem must achieve a minimum Safety Integrity Level (SIL) [18]. In a very simplistic way, Safety integrity levels can go from 1 to 4, and it is related to the probability of a failure to occur in the system; in a system SIL-1 this will mean that the probability or an error to occur in the system is much higher, so the risk tolerance must also be greater, therefore the safety critical system must have a SIL level higher than 1. Compared to a system that has a SIL-4, for instance, the signalling system that controls train movement and track alignment, it must be highly reliable and have a very low risk tolerance, because if there is a green light when there is a train ahead, there will be a collision and the potential for severity of the incident is very high. Figure 2.11 presents a high-level representation of how safety and cybersecurity norms are related.

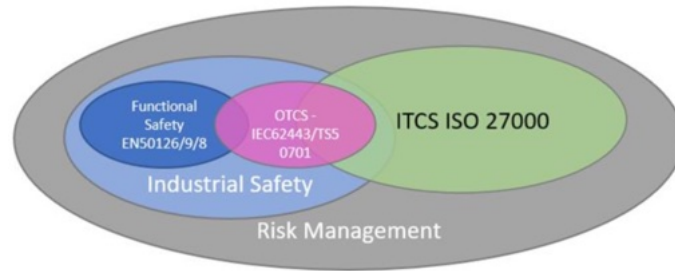


Figure 2.11: Relationship between cybersecurity and safety [47]

As described in the documentation provide by [48], in the European Union the safety certification of railway systems is based on several standards, among others CENELEC standards EN 50126-1/2 (2017), EN 50128 (2011), EN 50129 (2018) and EN 50159 (2010). The main goal of this approval is to guarantee the safety of the system; however, cyber security is also addressed. Although the target in EN 50126-1/2 (2017) and EN 50128 (2011) is on safety and quality, EN 50129 (2018) and EN 50159 (2010) also include requirements related to cyber security in the context of Operational Technology [48]. As shown in Figure 2.12, the EN directives for safety management and Cybersecurity management respectively.

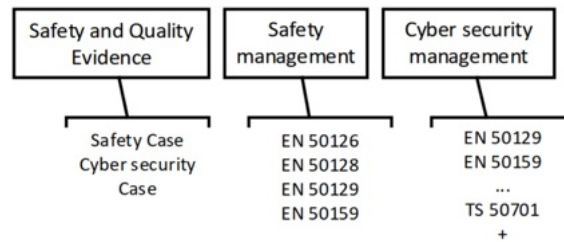


Figure 2.12: Safety and Quality evidence, and the valid regulations [48]

The Safety Case is a document in which quality and safety evidence is stated, is required by EN 50129 (2018), and shows that the safety management process intends to minimize the residual risk of systematic safety-related faults and security threats so far as safety is concerned. It also requires that, if the impact of IT-security on functional safety is reasonably foreseeable and cannot be excluded by simple arguments, it should also be managed during risk assessment. As railway systems are interconnected through network systems, EN 50129 (2018) demands that it be documented in a Safety Case what kinds of networks are used and what controls are implemented in the signalling system to ensure secure communication.

In EN 50159 (2010), requirements are defined for the signalling infrastructure network, where three categories of networks are established, from closed networks to untrusted ones; for this last one, cyber threats are also considered. The cyber threats demanded to be considered are only intentional, and attacks on confidentiality and measures to prevent system overloading (Denial of Service) are not covered [48].

As previously described, the cybersecurity aspects impact the safety cases used for operational certification of the railway system, but as the differences between

the life cycle of safety, which is almost static during the life time of the railway infrastructure, and the cyber security aspects life cycle, which can be very short due to everyday evolving cyber threats. Therefore, for this reason, the European Union and CENELEC introduced the TS50701. The purpose of this technical specification is stated as follows: "when a railway system is compliant with TS50701, it can be demonstrated that this system is in the state of the art in terms of cybersecurity, that it meets its targeted Security Level and that its security is maintained during its operation and maintenance" [18].

TS50701 introduces the concept of Security Level (SL). In general, the security levels (SLs) are defined for the zones and conduits in EN IEC 62443-3-3:20191 Annex A, generically in relation to the threat type against whom they are to offer protection.

Where SL 0, no security protection is required, SL 4 protection against intentional violation using sophisticated means with extended resources, industrial automation and control system (IACS)-specific skills and high motivation[18]. So, TS50701 provides guidance on how cyber security could be managed in the context of the EN 50126-1 (2017) Reliability, Availability, Maintainability & Safety (RAMS)-life cycles. The target goal of TS50701 is to be compatible and consistent with EN 50126-1 when applied to the System Under Consideration, as well as to isolate the safety approval and cyber security acceptance as much as possible, due to differences in the life-cycle [48].

The TS50701 performs this separation by allocating specific cyber security activities with synchronization and the corresponding deliverables throughout the life-cycle phases of EN 50126-1 (2017). Of course, certification activities require the synchronization between the stakeholders' system engineering, Safety, RAM, Verification-and-Validation, and Testing-and-Commissioning activities. TS50701 proposes to define only a limited number of coordinated cyber security objectives to be implemented in the cyber security case. As can be seen in Figure 2.13 the synchronization between the safety and cyber security cases as proposed by the TS 50701.

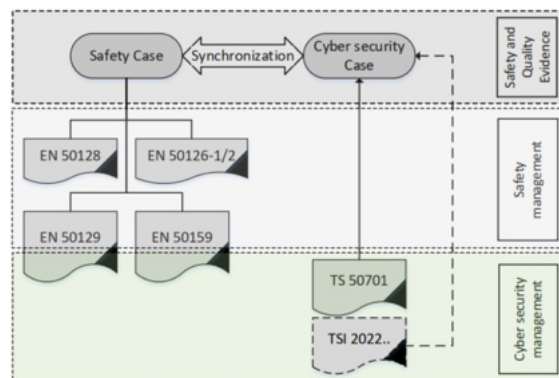


Figure 2.13: Safety Case and Cyber security Case interaction [48]

The achievement of the cyber-security requirements is stated in the cyber security case. So, security controls are demonstrated in Security Related Application Conditions (SecRAC), with the same meaning as Safety Related Application Conditions (SRAC) already used for Safety Related Application Conditions. If by any

chance the cyber conditions evolve, it should be demonstrated that the cyber security goal is still valid. As already mentioned, safety approval rarely changes and should be avoided due to the related costs of the process to achieve approval. This is very long and time consuming, and turns out to have a negative financial impact on the railway operator or supplier that requires the change after system approval. That is the opposite in the cyber perspective, which is constantly evolving, therefore the goal is that essential safety documentation can be maintained as the cyber security process adapts to changing threat scenarios [48].

In the handover phase, which is the time that the integrator delivers the system to the railway operator ready to be explored, if the system integrator sees that the cyber security case needs an update, the operator will validate it when it has been successfully proven. During the rest of the system life cycle, TS50701, also presents recommendations for patch and vulnerability management; all of which should be performed in coordination with safety management.

By separating the cyber-security case from the safety case, one will also decrease the synchronization points between the safety and security process. Some of the challenges that this approach may raise in the synchronization process are the different time windows and duration of the safety approval process compared to cyber security assurance. Coordination between safety and cyber-security can be quite difficult for larger projects. Risk assessment activities and safety analysis must work closely with a common objective from the requirement phase, to define a proper security architecture, and should attempt to have the least amount of changes avoiding the re-issue of new safety cases [48].

2.6 Cyber Risk Scenario - IxL & ATS SYSTEMS

Railway system are nowadays getting more complex, Figure 2.14 shows us the great number of different systems that belong to the railway ecosystem. These systems are roughly divided into three categories, safety and security, passenger experience, and operations. All of these systems are interconnected, using a wide range of physical means and protocols.

Railway IxL systems are the systems responsible for controlling the exclusive access of a train to a route, which is a sequence of track elements exclusively assigned for train movement through a station or a junction [49].

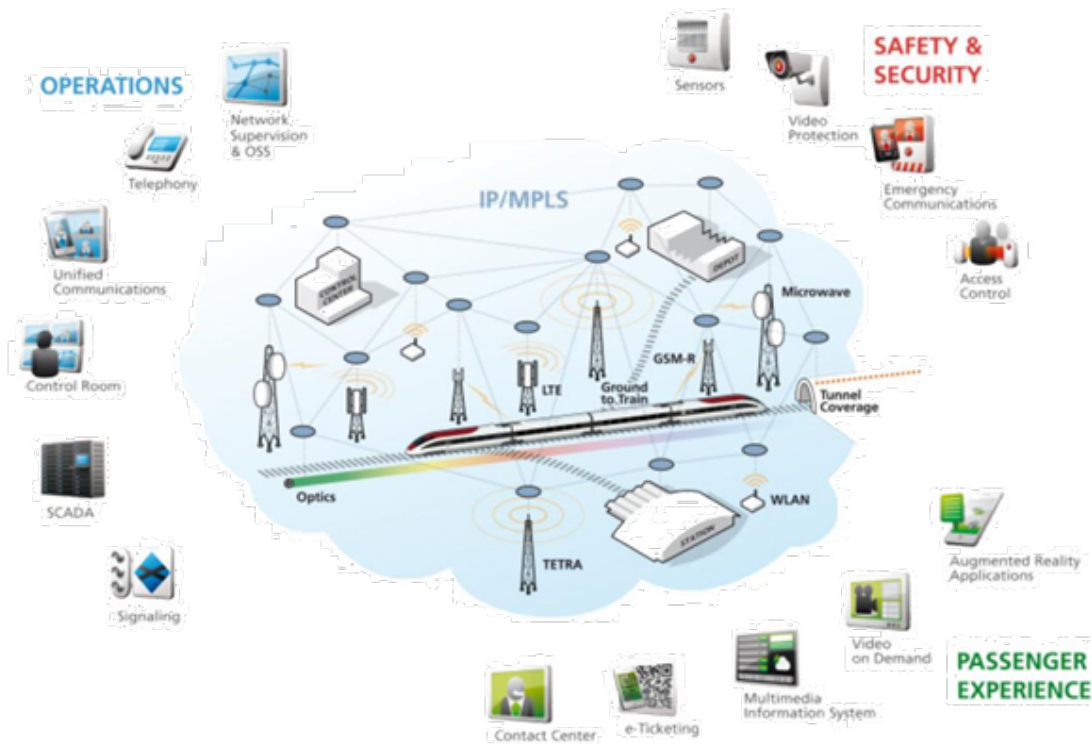


Figure 2.14: Railway infrastructure communications and network environment [50]

ATS or Operations Control Center, often acts on signals generated by the IxL system to monitor and adjust the performance of individual trains, to ensure smooth railway service, and is where railway control operators take decisions and control all railway traffic [49].

Securing OT presents different challenges than securing pure IT systems. As shown in Figure 2.15, while IT security focuses on confidentiality to prevent stealing confidential information, OTs are more concerned with data integrity and avoiding unplanned system outages that can disrupt production availability and profitability. Compared to classical OTs, the transportation sector places even greater importance on the concept of resilience, since the availability of each sub-system is a paramount priority [49].

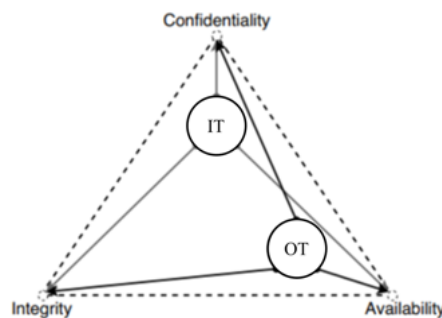


Figure 2.15: The different meanings of the CIA triad in IT and OTs

2.6.1 IxL Main vulnerabilities

The major vulnerabilities of Interlocking systems are the following:

- As the railway infrastructure is spread over a wide geographical area, where critical nodes of railway systems and networks require maximum availability, and in the countryside, where physical protection and maintenance cost time and money [51].
- Track-side equipment updates, in particular, can have an important financial impact due to the number of systems, the way they are spread throughout a large geographical area, equipment being used 24x7 with short maintenance windows, and highly skilled personnel to perform the software update, all of which leads to a great financial impact [51]. Updating legacy or obsolete systems with life cycles calculated in decades is difficult or even impossible.
- Lack of know-how due to obsolescence and loss of technical skills to perform patches and updates on OT equipment. As technology ages, people who used to take care of maintenance and updates will also age, which leads to a point where you lack qualified personnel to perform the necessary tasks to ensure an adequate security level [51].
- Other risk factors are the non-existence of devices to monitor and analyze network traffic for potential exploratory actions or attacks, and the widespread use, even nowadays, of plain text communications, without any kind of authentication control method [52].
- Reinforcing the security of systems can disturb data flows and systems (e.g., cryptography, system segregation). These can strongly impact system performance or availability if any issues arise (e.g. expiry of a certificate) [51]. Exchange of a board with a different MAC address.

2.6.2 ATS Vulnerabilities

Some vulnerabilities in Automatic train supervision systems are:

- Lack of consensus on how to design control centers, many different Operations Control Centre (OCC) configurations have been designed following possibly incompatible standards, this may be an issue at the time of requiring that the OCC's follow the same standards throughout the European Union in terms of operation and cyber security [49].
- Servers and operator workstations with outdated operating systems, without recent patches. Network equipment not properly configured, with protective measures turned off (e.g., sticky MAC, to avoid ARP spoofing, Cisco Discovery Protocol (CDP), Spanning tree protocol (STP)) and also missing the latest security patches updates [52].

- Default passwords on operator workstations, root operator, and network equipment (SNMP, Telnet, SSH, Web)[9].
- Incorrect network segregation, both to provide passenger access and to communicate telemetry data with track-side devices [52]. Poor network segregation and packet filtering between what comes from the field and what arrives to the Control Center LAN.
- Lack of authentication to access the transport network, no VPN or encrypted tunnel that would prevent a rogue IxL with an IP address from a legitimate IxL from connecting to the OCC network and perform network reconnaissance / mapping and other related types of actions.
- Workstations usually have specialized software, sometimes with built-in security, but are impossible to patch or upgrade [52], some with USB ports available to operators for reporting tasks, allowing them to enter the system.
- Railway operators report low cybersecurity awareness and cultural differences, especially among safety and operations personnel [51]. Railway Supervision application developers with weak cybersecurity awareness focused only on functionality and availability.
- On the other hand, applications where security is not carefully balanced and require the user to always input their credentials for simple tasks that have no major impact. Or when the password complexity is too high, this may lead people to leave their credentials on sight.

2.6.3 ATS & IxL Vulnerability Examples

The following are three explicit examples of issues encountered in railway systems that pose a high vulnerability to threat actors. In Figure 2.16, it is clear the low cybersecurity awareness of the operations control centre operator, where the username and password are explicit in the computer screen, and this was broadcast in a national tv program [53].

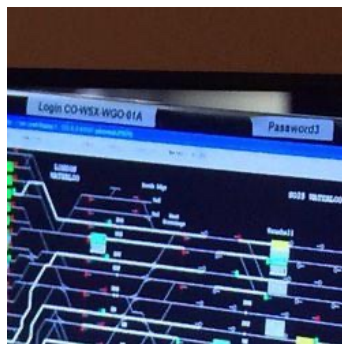


Figure 2.16: Low cybersecurity awareness [53]

Another vulnerability example of low cybersecurity awareness, now from the supply chain, in Figure 2.17 one of the equipment manual, the supplier clearly

states what are the possible administration passwords to be used [52].

```

Dear customer,

Due to recent software updates and deviating
from the information in the user manual there
are two possible combinations of the default
administrator password:

User name: admin
Password: funkwerk

or

User name: admin
Password: admin

```

Figure 2.17: Default Password vulnerability [52]

The third vulnerability is shown in Figure 2.18 and demonstrates how easy it could be to obtain the administrator password from a network device via SNMP using a tool available in a Kali Linux distribution [52].

```

root@kali:~# snmpwalk -Cc -v 2c -c [redacted] 1.3.6.1.4.1.2011.10.2.12.1.1.1
iso.3.6.1.4.1.2011.10.2.12.1.1.1.1.5.97.100.109.105.110 = STRING: "admin"
iso.3.6.1.4.1.2011.10.2.12.1.1.1.1.3.104.51.99 = STRING: "h3c"
iso.3.6.1.4.1.2011.10.2.12.1.1.1.2.5.97.100.109.105.110 = STRING: "admin"
iso.3.6.1.4.1.2011.10.2.12.1.1.1.2.3.104.51.99 = STRING: "password"
iso.3.6.1.4.1.2011.10.2.12.1.1.1.3.5.97.100.109.105.110 = INTEGER: 7
iso.3.6.1.4.1.2011.10.2.12.1.1.1.3.3.104.51.99 = INTEGER: 0
iso.3.6.1.4.1.2011.10.2.12.1.1.1.4.5.97.100.109.105.110 = INTEGER: 3
iso.3.6.1.4.1.2011.10.2.12.1.1.1.4.3.104.51.99 = INTEGER: 1

```

Figure 2.18: Obtaining an administrator password on HP/H3C and Huawei devices via SNMP [52]

Bearing in mind what has been said and shown so far, how should we respond to it? What guidelines can and should be used? CENELEC TS 50701 provides some clarity in this regard.

2.7 How to apply CENELEC TS 50701

To mitigate the vulnerabilities described previously, what today equipment suppliers and railway operators are entitled to follow are the requirements and recommendations to address cybersecurity within the railway sector on the CLC/TS 50701. The purpose of this technical specification is that, when a railway system is compliant with it, it could be demonstrated that the system is at the state-of-the-art in terms of a cybersecurity approach and meets its target. Of course, there can be some factors that could make it impossible to achieve the completeness of all the requirements on it, namely, time and the project budget. But cybersecurity is an exercise of managing risk and a trade-off between effort, budget, and risk tolerance.

This technical specification is directly based on IEC/EN 62443 series, which in turn are based on EN ISO/IEC 27001 and EN ISO 27002. Its goals are to fill the gap for a narrower specification and a consistent approach to the railway system. Previously, system suppliers and railway operators followed a much broader and generic standard IEC/EN 62443, which was applied to industrial networks. What will be described in the next Subsection is a guide on how to apply this technical specification CLC/TS 50701.

The main goal of railway cybersecurity is to protect the essential functions of the railway system, even if they are threatened by malicious attackers. Since modification of data or processes can force systems to malfunction, lack of cybersecurity can lead to operational interruptions, damage to assets, or even worse, to injuries and death [18].

2.7.1 Life Cycle

This technical specification considers 13 different phases on the Security-related activities within a railway application life-cycle, and they are directly derived from the standard EN 50126-1. These are:

1. Prerequisites – When the Railway operator’s security program is established, and Legal and regulatory framework is identified.
2. Concept – Where System under consideration (SuC) is identified, what are the security-related controls and defined a High-Level zone model. What security standards are applicable, and one of the key points of the technical specification, the definition of the purpose and scope. At this stage, there must be alignment with the railway operator / asset owner and stakeholder’s security goals. The outcome of this phase is the project cybersecurity management plan.
3. System definition and operational context – it should be defined the System boundaries, it is made a Logical and physical network plan review, defining the zones and conduits of the network.
4. Risk analysis and evaluation – At this stage, a risk assessment should be made to identify possible threats, physical and organizational countermeasures, or assumptions for zones and conduits. It should also be considered the business continuity aspects (incl. incidence response and recovery) for the system under consideration.
5. Specification of system requirements – In this phase, the SuC-specific refinement of normative requirements should be performed.
6. Architecture and attribution of system requirements – At this stage, the risk assessment should be updated if necessary, it should be taken into account the security-related application conditions, which are explained in Table 6 of the documentation supplied by [18], where an extensive table of security requirements is presented, and its application to the railway environment.
7. Design and implementation – With all the necessary information, it is now time to conclude the design of the solution, it should be prevented and avoided the conflicts between the component cybersecurity functionality and functional architecture.
8. Manufacture or Procurement – All the necessary material and services are acquired in this phase.

9. Integration – In this phase, network plans should be reviewed considering the new acquired equipment, and an inventory of all systems and applications should be made. It is also now that the qualification of security components and functions from test integration results, penetration testing, and vulnerability scanning should be made.
10. System Validation – In this phase, it should be assessed by examination and provision of objective evidence that SuC in combination with its security-related application conditions complies with the Cybersecurity Requirements Specification, the output of this phase is the Updated System Integrator cybersecurity case.
11. System acceptance – Finally, we reach system acceptance, now the security handover occurs between System Integrator and railway operator.
12. Operation, maintenance and performance monitoring – This is the longest phase in the life cycle of the SuC, within it, is required to perform the maintenance of the logical and physical network plan and also the list of IT systems and installed applications. Perform patch and/or configuration management, data backup and auditing procedures to enable data recovery.
13. Decommissioning – Finally the decommissioning phase, the disposal of components, taking security criteria into account, ensuring that all confidential data and information should be completely erased, and erasure verified during system decommissioning and disposal.

2.7.2 Zone and conduit identification

After the concept phase, the next step in approaching CLC/TS 50701, is to define a railway asset model. Usually in the railway ecosystem, the assets are divided in four physical groups and different criticality levels (e.g. signalling, command and control, auxiliary, etc.). In Figure 2.19 the four different physical groups, and on each of them, each asset is represented by a colour to indicate their function classes. Assets from different colours and physical groups can be interconnected (e.g. between a Traffic management system and an interlocking).

The Railway operators can identify the assets as a subset of this model in Figure 2.19. In addition to the assets shown, there are also network devices that should be considered as assets to be protected from cybersecurity. The output of this exercise will be used as an input to define our SuC.

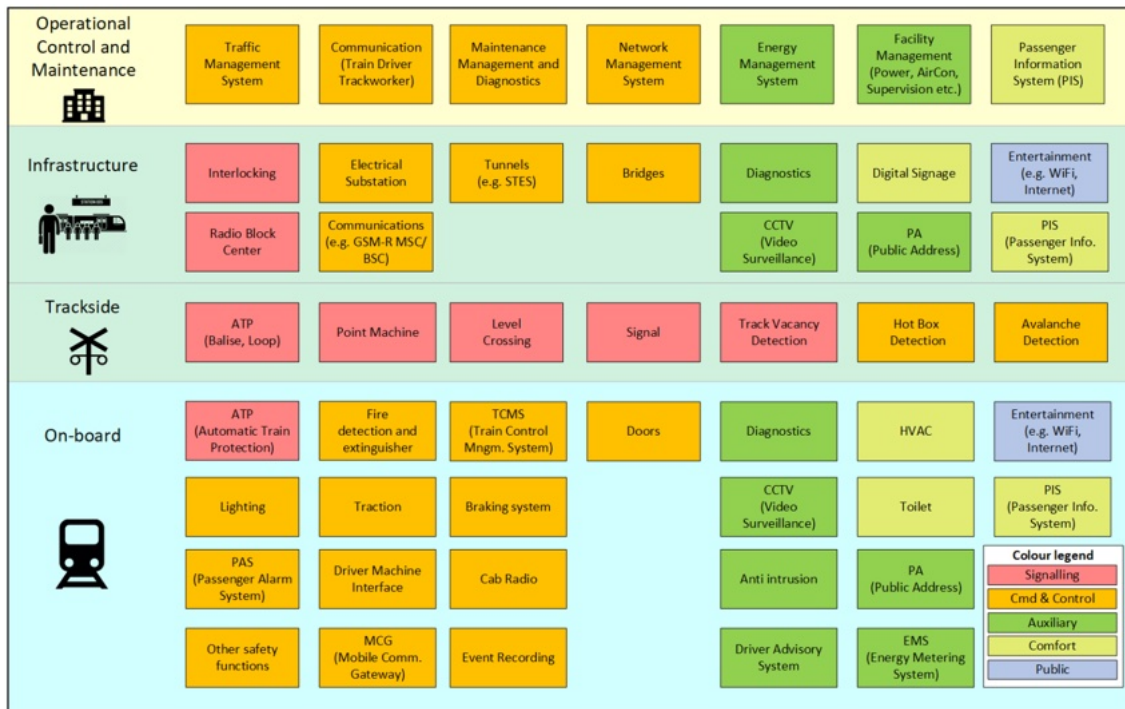


Figure 2.19: Railway asset model [18]

The next point to take into consideration is the Railway physical architecture model, from a cybersecurity perspective, the distributed locations of the different components and subsystems as well as their physical security features are to be considered, especially in risk analysis. For example, assets located along the track are more prone to direct physical attack than assets in a control centre. On the other hand, a traffic management system that may have interfaces to the enterprise world (ERP systems, mail servers, and other office systems) as shown in Figure 2.20, may be more exploitable by a Denial of Service (DoS) attack or other threats in the IT domain [18].

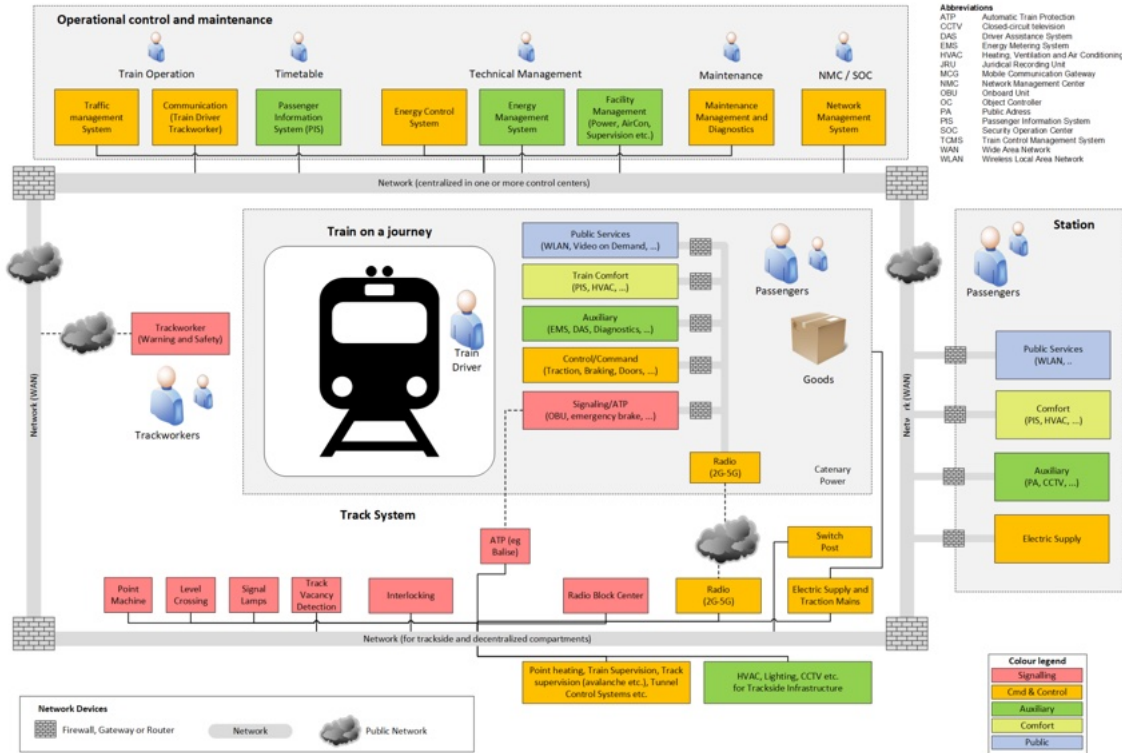


Figure 2.20: Railway physical architecture model [18]

Railway operators and system integrator can identify the network-oriented connections between the components of the SuC in the Railway physical architecture model.

Bearing in mind the physical location and the network approach, we can now go to the High-level railway zone model. This model will be used as input for the activities of SuC identification, initial risk assessment and SuC zoning (identification of zones). In the zone definition, it should be taken into consideration to keep a particular service running in case of an incident in another zone, in other words, segregation of networks and a clear sense of boundaries.

The combination of zones, conduits (communication paths), subsystems and zone priorities result in a generic zoning model. Figure 2.21 shows a railway zoning reference according to the design principles of IEC/TS 62443-1-1:2019, the zoning principles of EN IEC 62443-3-2:2020 and the risk-based approach.

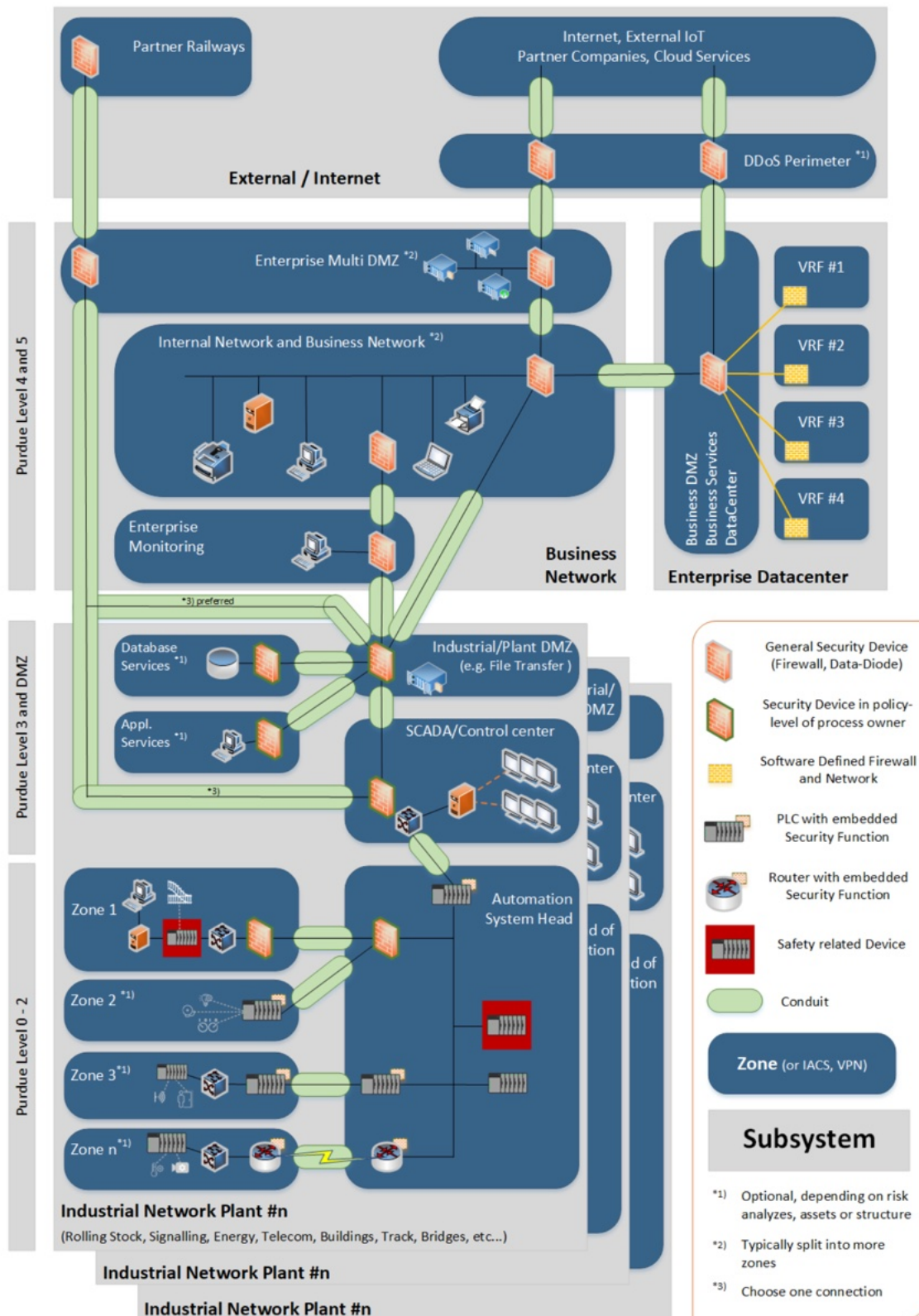


Figure 2.21: Generic high level railway zone model [18]

When evaluating the zone model, the two things that should be part of the concept are:

- Communication and human interactions in high criticality zones should be monitored, logged and stored.
- Security devices between zones with different criticality that protect the zone with the highest criticality should be managed by the responsible organization of the higher criticality zone.

As a best practice there are only three type of conduits necessary to connect zones, depending on the SL of the zones:

- Conduit implementing a transparent gateway (connecting zones of same security level).
- Filter conduit as firewall appliance (allowing a zone of lower or equal security level to communicate with a zone of a higher security level).
- Unidirectional conduit as data diode or network tap (allowing output from a higher security level zone to others).

2.7.3 Cybersecurity Management Plan

For the development of the management plan, the asset owner should define their context, the goal is to have a clear view of the threats we will face and their sources, the legal requirements, and what the boundaries of the system are. It should be used a methodology to identify, evaluate, and manage, for this a risk assessment framework like ISO 27005 can be used.

2.7.3.1 Risk assessment and criticality Definition

After the zone definition, a risk assessment should be performed to identify the criticality of each zone and conduit, which should lead to the definition of the cybersecurity requirements specification as the central outcome of this activity [18]. During the system life cycle, there may be a need to reevaluate risk when new countermeasures are implemented or if new threats or vulnerabilities are disclosed. This risk assessment cannot override any mandatory requirements for security protection, like national legislation.

The integration of products already designed and certified according to the cybersecurity requirements can be a good approach to ensure flexibility, saving effort not having to evaluate a complete solution, and at the same time more budget cost-effective.

The first step is to identify the threat landscape, it should be based on recognized and accepted threats library or reports, and built with a high-level approach, providing an overview of the threats applicable to the railway sector. As a reference, it can be used the following:

- ENISA Threat Landscape Yearly report.

- ISO/IEC 27005.
- NIST SP 800-30.

It is recommended to use a defence in depth approach, which is one of the guiding principles to provide appropriate security for the essential functions of all systems. An example of controls that can be applied is shown in Figure 2.22. When applying these, the integrity and availability are to be considered with the highest priority, this stands out as one of the major differences between the OT and IT worlds.

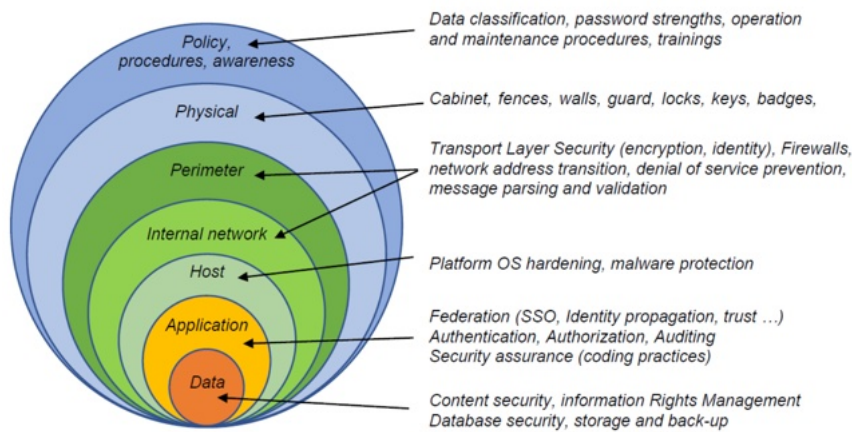


Figure 2.22: Defence in depth with example of measures [18]

It should be identified what are essential functions of SuC, these key functions needed for the operation of the railway application are normally related to safety availability and control, knowing them is essential to protect SuC. Also avoids imposing security requirements that could limit or even compromise them.

To enable a consistent approach for threat risk assessment between asset owners, it is important to define an impact assessment reference between all stakeholders. For the railway environment, it should be used at least a criteria impact to Human health and safety, Operational availability, and financial impact. When estimating the likelihood of a threat, it should be considered :

- The exposure of the asset.
- Its physical location.
- And the effort and sophistication needed to succeed on an attack.

The likelihood could be estimated from scales based on the exposure and vulnerability of the asset. The resulting likelihood L is calculated from Exposure and Vulnerability by:

$$L = EXP + VUL - 1$$

With all these data, we are ready to perform a risk evaluation, it could be determined in a matrix where the likelihood and the impact of the threat are related. The risk acceptance criteria has to be approved by the asset owner to avoid conflicts in the future.

On the basis of the output of the initial risk assessment, the system under consideration should be breakdown, and the assets shall be assigned to consistent security zones connected by conduits. This means all assets in the same zone and all data sent by the same conduit share the same or similar cybersecurity requirements.

The output documentation of this phase should be:

- Threat Landscape.
- Risk Matrix.
- Risk Evaluation.

2.7.4 Detailed Risk

In the event that the outcome from the initial risk assessment is that all risks are sufficiently mitigated without any additional countermeasures, because there is a very strong physical and organisational protection, the detailed risk assessment could be skipped [18]. If this is not the case a detailed risk assessment needs to be performed.

Generally, the risk assessment is proactive, and it will not wait for an incident to trigger it, therefore, there maybe a need to update it when compensating controls are evaluated or there is a new vulnerability. This risk assessment should be updated during most of the life-cycle and not only in the design phase of the cybersecurity project. If zones or conduits share the same risk perspective, then the assessment needs to be performed only to one zone or conduit, but the results must be applied consistently.

The baseline of the process is the output from the initial risk assessment, the zones and conduits are identified there. It is acknowledged that the easiest application of the process is if only one principle is applied for each zone or conduit, and it would be covered by a code of practice (approved strategy for a given case) or a reference system (system used as a reference to replicate the used solution), but in the railway environment there can be complex systems that would require more than one principle. When it is not possible to apply a code of practice or a reference system, it will be necessary to determine the cybersecurity target security level Targeted Security Level (SL-T).

In general, the security levels (SLs) are defined for zones and conduits in EN IEC 62443-3-3:2019 Annex A, generically in relation to the threat type against whom they are to offer protection:

- SL 0 No security protection necessary.

- SL 1 Protection against casual or coincidental violation.
- SL 2 Protection against intentional violation using simple means with few resources, generic skills and a low degree of motivation.
- SL 3 Protection against intentional violation using sophisticated means with moderate resources, IACS-specific skills and a moderate motivation.
- SL 4 Protection against intentional violation using sophisticated means with extended resources, IACS-specific skills and high motivation.

The EN IEC 62443-3-3 presents a relation between the controls according with the SL-T, that is interpreted as qualitative means of risk reduction bearing in mind the needed risk reduction.

The process begins with a target security level starting point, which is acquired based on experience or attacker profile, it should be determined the security level to each one of the seven foundational requirements, namely:

1. Identification and authentication control (IAC)
2. Use control (UC)
3. System integrity (SI)
4. Data confidentiality (DC)
5. Restricted data flow (RDF)
6. Timely response to events (TRE)
7. Resource availability (RA)

The security level of each one of the requirements will be combined into a security level vector:

$$\text{Security Level Vector} = (\text{IAC}, \text{UC}, \text{SI}, \text{DC}, \text{RDF}, \text{TRE}, \text{RA})$$

With the requirement Security Level Vector now in place, we can proceed to choose the control for each requirement taking in consideration its Security level. For example, if we have the Security Level Vector where the value of the IAC is equal to 4. Now checking the already mentioned Table 6 of [18] were a sample of it is shown in Figure 2.23, we get that multi-factor authentication should be applied for all networks, also relevant is the column Railway notes, that gives detailed information applied to the railway environment.

The initial controls are chosen from a list presented in the EN IEC 62443-3-3, and the risk is evaluated. If its value is not acceptable, more controls should be added until we reach an acceptable target security level, which determines the security requirements. This exercise should be performed on all zones and conduits in our system under consideration.

In Figure 2.24 it presents the general process for a detailed risk assessment, adapting ZCR 5 from EN IEC 62443-3-2 for the railway environment.

Req	SL	Title	Railway notes (informative)	Relevant design principles	Stakeholder	Type
FR 1	Identification and authentication control (IAC)					
SR 1.1 RE(3)	4	Multifactor authentication for all networks	The feasible multifactor authentication solutions outside the IT system in railways are generally external and could comprise a badge or a physical recognition of presence for the human user e.g. by a phone call. This could equally apply to regularly planned maintenance activities.	6 - Authenticate requests 12 - Proportionality principle	Op Sys	Tech

Figure 2.23: Sample of TS50701 Table 6 System Security Requirements and Foundational Classes [18]

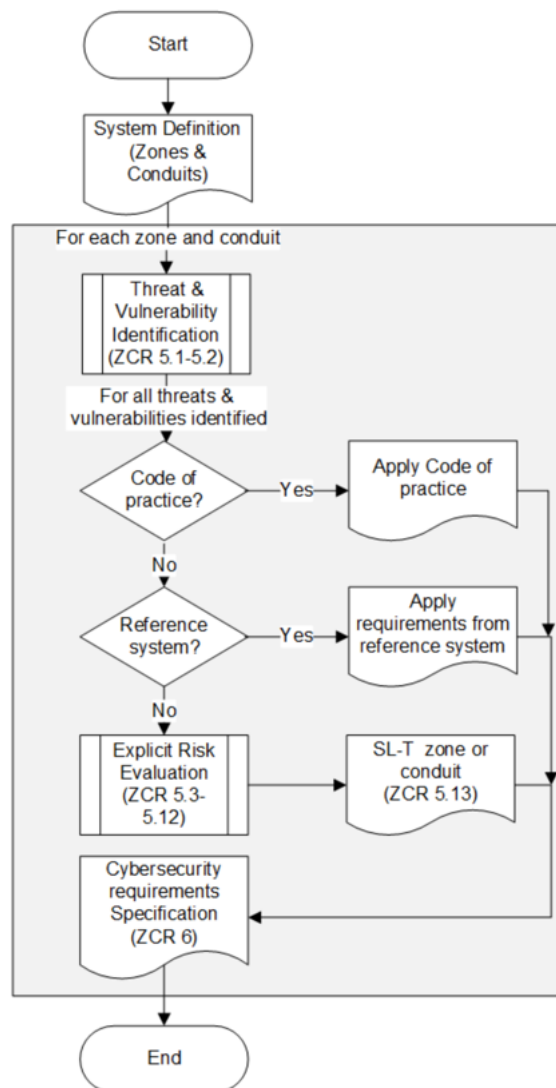


Figure 2.24: Detailed risk assessment flowchart [18]

2.7.5 Implementation and handover

With the cybersecurity requirements specification concluded, where we have defined all the necessary controls to be applied, it is now time to move onto the implementation, verification, acceptance and handover phases.

After all controls are implemented, we should now validate and assess what is the Achieved Security Level (SL-A) of the system. If SL-A reaches the expected SL-T according to the cybersecurity requirements specification, or if it does not, then compensatory counter measures are implemented or we will need to go back to the design phase. With all this information, we will build a cybersecurity case, which delivers the evidence that the system as implemented operates with the expected security confidence level.

For this stage, the input will be the cybersecurity requirements and the cybersecurity assurance procedures. The assurance procedures are a test protocol, that allows us to have a well defined and systematic approach for inspection and testing the implemented system. They should be performed based on the targeted security level (SL- T) as follows:

- Security requirements testing
 - Verification of implemented Cybersecurity Requirements Specification (CRS).
- Threat mitigation testing
 - Verification of countermeasures implemented to mitigate threats and assessing the resilience of these implemented countermeasures.
- Vulnerability Testing
 - Vulnerability scanning identifies systems and system attributes and attempts to detect known vulnerabilities.
- Penetration testing
 - The pen testing should be the final step of the of the tests, similar to the system test on a railway system. Its goal is to demonstrate the resilience against the identified risks and threats. It must be performed by independent testers, from another department or organization.
- If any test fails, then a design review should be performed, it will result in either an additional countermeasure or returning to the design stage. If all tests are successfully completed, the cybersecurity case should be updated with these results, and we can move forward to the system acceptance.

The system acceptance should be performed by a different entity from those undertaking any roles in the project, to guarantee independence of the process, and it should result in a Cybersecurity Assessment Report, which shall make a conclusion about its readiness for operation. The system can now be handed over.

2.7.5.1 Operation, maintenance, and disposal

With the SuC handed over, it should be ensured that the cybersecurity of the system is maintained throughout its life cycle.

A necessary precondition to ensure the secure operation, maintenance and disposal of the system, is that the asset owner shall have implemented an OT security program, where all the parts concerning the railway application should be in scope of it. In that program, a vulnerability management process and security patch management shall be defined. This vulnerability management goal is to detect, classify, prioritize and remediate vulnerabilities. On the other hand, for the security patch management, the product supplier should inform the asset owner when a security patch should be applied. At the time of installation (remember that we are dealing with a critical system) if the application of this patch requires a reboot, this should only be performed by an operator or engineer manually with the acceptance of the operator. If the application of a security patch impacts safety functions, it shall also be coordinated with safety management as well.

On systems like the ones running in the OCC with redundancy, for the estimation of the system outage time and periods with reduced availability of the system (running in non-redundant mode), which should be considered for the estimation of the availability of the system, two different approaches are contemplated. Figure 2.25 shows an overview for these time-frames due to a security update on a 1:1 active/passive, we can see the following states of the system:

- Operational State: System is operational or out of service.
- Availability State: System runs with redundancy, without redundancy, or is out of service.
- Security State: System is vulnerable (before patching the active system), or secure, or out of service.

For systems with additional Safety requirements, the updates have to be evaluated additionally against the Safety Certification Case. An additional observation phase after update might be defined, this can be a single day operating with the newly update node, and compare its behaviour with the primary node. This observation depends on the ability of the system. Today, a large number of railway operators have testing environments with virtual reference system, a digital twin for this purpose. Figure 2.26 shows a system with the introduction of additional observation phases as they might be required for systems with additional requirements.

For the decommissioning phase, Data and information should be completely erased, and erasure verified during system decommissioning and disposal [18].

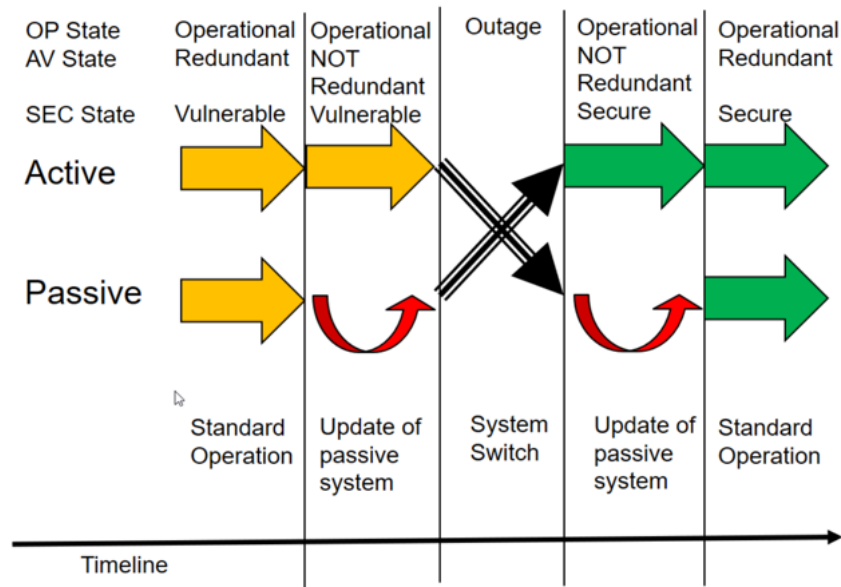


Figure 2.25: Vulnerability and outage time during system update (maintenance phase) [18]

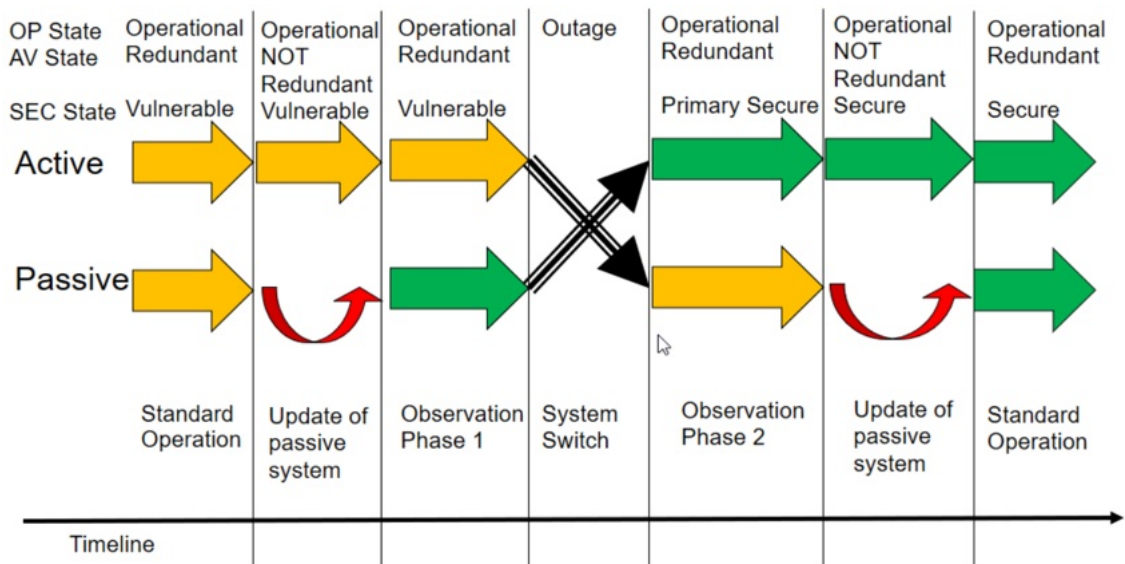


Figure 2.26: Vulnerability and outage time during system update with observation phases [18]

2.7.6 Legacy Systems

In the case of a legacy system that cannot achieve a security level according with IEC 62443, there are still base measures that can be taken to achieve a basic security level, even though it can only prevent some cyber-attacks.

2.7.6.1 Basic security risks and mitigation

As basic security risks, it can be considered denial of service attacks and vulnerability exploits, these attacks can be achieved when the attacker gets physical or logical network access to the operational network. Attaching attack devices to the physical network can be impeded by physical security of the installation, in the event that an attacker could break in the physical perimeter, the detection of these devices can be achieved by regular inspections of the installation and by network monitoring.

Track-side installation or installations in other open areas (e.g. on-board installations on trains) should be secured by metal cases according to resistance class 3 of EN 1627. If the specific installation allows access to the operational network, additional sensors to detect excessive motion or vibration should be considered as means to initiate a visual inspection.

Seals can be used to reveal modifications and tampering of installations. They can reduce the need for detailed inspection unless the seal is broken.

On the other hand, to compromise the network via a logical access, as it requires access to the network, it can be mitigated by network segmentation and closed network design. If this separation is not possible, the operational network should be separated from the non-operational network by a data diode (in the case of data only flowing one way), or by the implementation of a Demilitarized Zone (DMZ) when bi-directional communication is needed.

In case of impersonation attacks, like a man-in-the-middle, where data from and to the attacked device can be altered, since a legacy device might not strongly authenticate the sender of the request, it cannot distinguish between a permitted message and a specifically crafted and forged message. As these types of attacks require access to the network (physical or logical), the previously discussed measures can be taken. As compromising an existing device via remote network access typically involves several network activities, a network monitoring system, intrusion detection system and honeypots can be implemented to detect abnormal network activities. Domain-specific security probes can also provide effective detection capabilities for such scenarios, as is the case of the Shadow Security Unit [54] [55], which was implemented for similar OT contexts, such as SCADA systems.

A Network Monitoring System (NMS) should be installed in conjunction with managed switches. It should be configured to monitor all network devices and to create alerts when unknown devices appear on the network or when the configuration of network devices changes. If a Security Incident and Event Management System (SIEM) is used, the alerts should be forwarded to a SIEM [56] or an event correlation system [57].

If redundant communication channels are used in the operational network, this can be used to further enhance the detection rate of a Network Intrusion Detection System (NIDS). If an attacker influences only one of the two channels, NIDS can detect this attack instantly.

If legacy equipment is not capable of encryption (TLS/SSL), security gateways can provide this functionality between two zones. Data diodes, which are based on unidirectional gateways (whose function is constrain data flows in a single direction), can also be used to protect telemetry streams in such scenarios [58].

In legacy systems the principle of defence in depth approach should be used, and it is meant to ensure that countermeasures are still in place even if a security breach has occurred.

2.7.6.2 Zoning

The boundaries of each zone should be protected in the same way as described earlier, by security gateways, firewalls and eventually data diodes.

For zone definition, the Purdue model can be used:

Level 0: All sensors (e.g. axle counters, track circuits, odometers) and actuators (e.g. point machines, signals, brakes) that provide the basic input and output of the control system.

Level 1: Local Control: All elements that receive input from sensors or provide output to actuators, elements that process data and elements that send or received data to or from an area control element.

Level 2: Area Control: All elements that are required for area control or train control functions.

Level 3: Overall Control: All elements that are needed for central control and business logic (as planning and disposition).

Level 4+5: The Enterprise/Office network of the asset owner

2.7.6.3 Training staff

Besides all the technical equipment that can be used, it should not be forgotten that the weakest link is the user. Advanced attacks need escalation of privileges and interaction with legitimate users e.g. phishing attacks. Personnel should be regularly trained. Awareness of cybersecurity risks should be kept at a high level.

2.7.6.4 Asset inventory

It should be ensured that systems are known in depth and it can be analysed where which versions are in use. A list with each equipment, with its characteristics, part number, serial number, operating system, latest patch, etc., should always be kept up to date. If an organization doesn't know their assets, they don't know what to secure.

2.8 Conclusions

By the analysis of the several railway cyber-security standards, technical specifications, guidelines and scientific papers for the European Union member states and USA, we can conclude that the railway ecosystem still have a long path do to reach a harmonization of the implemented cyber-security controls and policies. It is clear that safety is paramount in railway, we can see it by the amount of standards that must be met in Section 2.5 for safety. Industry has only recently started to implement controls and put cybersecurity plans into place. In part due to the cyber threat landscape and, on the other hand, forced by the legislation. Especially the one with respect to essential service providers that, in addition to requiring that any cyber event with impact should be reported, but also that the provider needs to prove that it has taken all the means to implement the "minimum" cyber-security controls, to try to mitigate known vulnerabilities and attacks, as stated in Section 2.4.1. The task of implementing these controls becomes even harder to do on legacy systems, as focused in Section 2.7.6.

Despite the cyber-security norms in the USA and EU try to achieve a common goal, which is to secure the system, it can be noticed that in the US ones, there is a bigger sense of business enterprise environment, because it focused more on how to present results to the management board, in terms of impact into business and operation, with the goal as well to get budget approved to perform assessments, risk management, and implement controls, than compared with the European TS 50701. In contrast, the European TS 50701, is much more focused on the railway ecosystem, as it presents more examples of controls to be implemented in this business, and it is more detailed and focused on helping integrators and operators in a practical level on what should be done on each phase. The European TS 50701 is also more "aware" regarding the process certification of a system, as it tries to distinguish between the SRAC and SecRAC, how they are different in terms of life-cycle, due to the cyber-threats being evolving every day. Both APTA and CENELEC guidelines are quite long, but there is an effort to try to reach the complete life-cycle of the systems, one remark that should also be made, that is, APTA guidelines, hardly focus on the legacy systems and the way of reaching a comfortable level of measure and controls TS 50701 clearly states that despite some railway systems could not comply with a security level, it still has a complete annex on how to approach these systems and what could be done. Bearing in mind these legacy systems, that already use Ethernet to communicate, but lack any monitoring or protection system in terms of cybersecurity, in the work that is presented in Section 3 of this dissertation, the goal is to develop a detection tool, focused on critical conduits as stated in TS50701 to perform traffic monitoring and analysis, to try to identify anomalies in the information being exchanged between the two endpoints, and in that way to identify potential malfunctions or attempts to tamper the system.

Chapter 3

Proposed Security Solution for monitoring critical conduits

This chapter documents the development process for the security anomaly detection tool proposed in the scope of this thesis, also covering other aspects such as the testbed used for validation or the specific use security case scenario to be considered. Regarding the testbed, this chapter documents not only the efforts undertaken to acquire the necessary means for its integration, but also the mitigation actions that had to be taken in order to deal with a series of problems faced during development.

Equally addressed are the requirements for the security tool, which ultimately drove its development but also helped define the uses cases supporting functional validation. Moreover, other development-specific aspects are also covered in this chapter.

3.1 Testbed and use case scenario development

The goal of the testbed was to simulate a railway conduit between two critical items, allowing to analyse traffic. The main idea is to establish a nominal state based on captures undertaken during normal operation (to be used as baseline), allowing to detect and identify malicious data modification attacks, by means of a tool specifically developed for this purpose. This tool could have the ability to monitor conduits on legacy systems, where security was not a priority.

For the testbed implementation, several possibilities have been foreseen. The first and more desirable one was to have access to real hardware used in railway infrastructures, to assemble a testbed to emulate a high fidelity environment. A second alternative was to resort to a large dataset of IP traffic from one critical conduit of a railway subsystem, as depicted in TS 50701. Working with this dataset, there would be the possibility to assemble a testbed to simulate the referred conduit.

Several attempts were made to contact entities such as railway operators (In-

fraestruturas de Portugal), as well as railway integrators, Siemens Mobility and Thales, to have access to a railway conduits for traffic monitoring, or at least to get an IP traffic dataset from a critical conduit. Unfortunately, none of the entities was open to cooperation. This situation reinforces the idea that cyber security awareness is still very low among railway infrastructure players, not being considered a critical aspect. The other issue is due to the use of proprietary protocols, which cannot be analyzed and scrutinized without permission from manufacturers.

As none of the previously described options were possible, the path followed was to identify a communication protocol that was used on railways, and source a simulator for it. After several possibilities, the CAN (Controller Area Network) protocol was chosen. Despite the adoption of this mitigation strategy, the fundamental rationale for the tool to be developed remained the same: it should be able to monitor the traffic in the bus, analyze it and learn the nominal operation behavior, in order to be able to identify any abnormal state or communication pattern.

3.2 About CAN

The CAN bus was developed in 1985 by BOSCH¹, for the automotive industry to simplify in-vehicle networks [59]. It is a multi-master, message broadcast system that specifies a maximum signaling rate of 1 megabit per second (bps). Unlike a traditional network such as USB or Ethernet, CAN does not send large blocks of data point-to-point from node A to node B under the supervision of a central bus master. In a CAN network, many short messages, such as temperature or RPM, are broadcasted throughout the network, ensuring data consistency at every node of the system [60]. This design facilitates efficient data sharing among system components, but also introduces a security risk, as any node can potentially inject harmful messages into the network.

Although originally developed for automotive applications, CAN is used in various industries, including automotive, aerospace, industrial automation, and medical devices, due to several key benefits that have driven its widespread use. It is cost-effective and straightforward to implement, while its architecture supports the seamless expansion and integration of new components. Its message-based communication and error detection mechanisms enhance network reliability and robustness. Additionally, the CAN bus excels in real-time communication, making it well-suited for time-critical applications like engine control.

3.2.1 CAN bus

The CAN bus consists of two wires: CAN high (CANH) and CAN low (CANL). It utilizes differential signalling, meaning that when a signal is transmitted, the voltage on one wire increases while the other decreases by the same amount.

¹Robert Bosch GmbH, www.bosch.com

The system relies on a single twisted pair of wires, helping to counteract electromagnetic interference, which might otherwise introduce noise into the transmitted signal. Differential signalling is commonly used in environments where noise resistance and fault tolerance are essential.

CAN packets are classified into two types: Standard and Extended. Standard packets consist of four key components:

- **Arbitration ID:** An 11-bit identifier that determines message priority when multiple nodes compete for bus access. If two packets are transmitted simultaneously, the one with the lower arbitration ID takes precedence.
- **Identifier Extension (IDE):** A bit that is always set to 0 in standard CAN packets.
- **Data Length Code (DLC):** Specifies the amount of data contained in the packet, ranging from 0 to 8 bytes.
- **Data:** The actual payload, with standard CAN supporting up to 8 bytes. Some systems enforce an 8-byte size by padding shorter packets.

While Extended Packets resemble standard packets, they can be linked to generate longer IDs, allowing IDs to be stored in a larger address space.

With respect to speed, there are two types of CAN bus: low and high-speed. Low-Speed CAN, which is also referred to as fault-tolerant CAN or ISO 11898–3, supports data rates of up to 125 kbps. It is primarily used in non-critical applications such as body control modules, door locks, and window controls, where high-speed data transmission is not essential. A key advantage of Low-Speed CAN is its ability to remain operational even if one wire in the bus fails.

High-Speed CAN, detailed under ISO 11898–2, can achieve data transfer speeds of up to 1 Mbps. It is ideal for time-sensitive applications such as engine management systems and electronic braking systems, where rapid communication is crucial. However, unlike Low-Speed CAN, it does not offer fault tolerance.

CAN FD (Flexible Data-Rate), developed by Bosch in 2012, enhances traditional high-speed CAN networks by increasing data transfer rates up to 5 Mbps while remaining backward compatible with standard CAN devices. Its key advantage is the ability to transmit larger payloads more efficiently, making it well-suited for modern vehicles with complex electronic systems.

3.2.2 CAN security

As modern vehicles become increasingly reliant on Electronic Control Units (ECUs) for critical functions and vehicle-to-everything (V2X) communication expands, the security of CAN bus networks is more crucial than ever. Cyberattacks on the CAN bus pose serious risks, including loss of control, theft, and potential physical harm, highlighting the urgent need for robust cybersecurity measures.

Unfortunately, there are several security problems with CAN, namely:

- **Lack of Authentication and Encryption** – CAN messages are neither verified for authenticity nor encrypted, making them susceptible to spoofing and eavesdropping.
- **Broadcast Communication** – Since all nodes can receive messages, any compromised node can inject malicious data into the network.
- **Limited ECU Processing Power** – Electronic Control Units (ECUs) have minimal computing resources, making them vulnerable to denial-of-service (DoS) attacks that flood the system with traffic.
- **Physical Access Risks** – Attackers with access to the OBD-II port can directly connect to the CAN bus, allowing them to manipulate vehicle functions.

Due to these vulnerabilities, CAN bus systems require enhanced security measures such as intrusion detection, message authentication, and access control to mitigate potential threats.

3.3 CAN application in Railway

CAN was first created for automotive use, so its most common application is in-vehicle electronic networking. However, as other industries have realized the dependability and advantages of CAN over the past 20 years, they have adopted the bus for a wide variety of applications. Railway applications such as street-cars, trams, undergrounds, light railways, and long-distance trains incorporate CAN [59].

Multi-function Vehicle Bus (MVB) is the vehicle bus standardized in IEC 61375 (presented in Section 3.3.1) to interconnect rail vehicles. In locomotives, this provides the standard communication interface for various on-board equipment such as radio, diagnostic systems, brakes, power electronics modules, power line, motor control, and the cockpit. In coaches, it interfaces with door controls, HVAC, passenger information systems, lighting units, etc. [61]. The application of the CAN protocol on the railway is standardized by IEC 61375 presented in Section 3.3.1.

3.3.1 IEC 61375 Standard

IEC 61375 defines hardware and software protocols, automatic reconfiguration, and network services such as topology and subsystem interfaces [61]. It applies to the architecture of data communication systems in trains, i.e. it covers the architecture of a communication system for the data communication between vehicles of the said trains, the data communication within the vehicles, and the data communication from train to the ground. The applicability of IEC 61375 to

train network technologies allows interoperability of individual vehicles within trains in international traffic. The data communication systems inside vehicles are given as recommended solutions to cope with the said Train Communication Network [62].

3.4 CAN and SocketCAN

The CAN communications protocol, ISO-11898: 2003, describes how information is passed between devices on a network and conforms to the Open Systems Interconnection (OSI) model, which is defined in terms of layers. Actual communication between devices connected by the physical medium is defined by the physical layer of the model. The ISO 11898 architecture defines the two lowest layers of the seven-layer OSI/ISO model as the data-link layer and the physical layer as shown in Figure 3.1 [60].

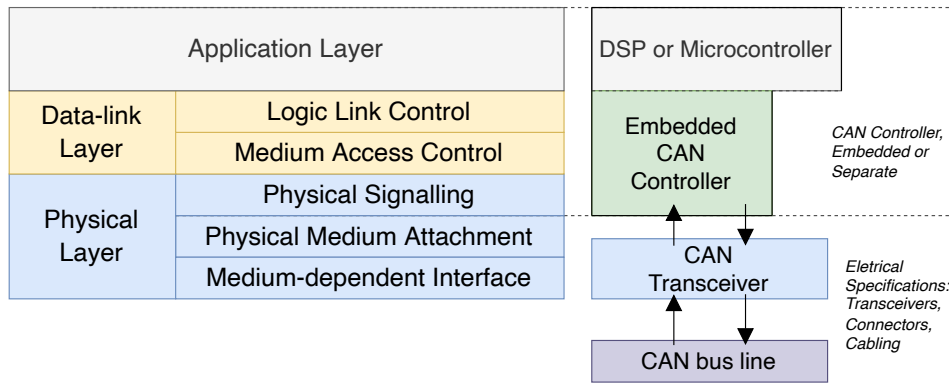


Figure 3.1: The Layered ISO 11898 Standard Architecture [60]

In Figure 3.1, the application layer establishes the communication link to an upper-level application specific protocol such as the vendor-independent CANopen™ protocol. This protocol is supported by the international users and manufacturers group, CAN in Automation (CiA) ².

As already mentioned, due to the fact that it was not possible to get access to the communication dataset, it was decided to use a SocketCan simulator.

SocketCAN, previously known as the Low Level CAN Framework (LLCF), is an open-source framework within the Linux kernel. Contributed by Volkswagen Research, it provides a set of CAN drivers and a networking stack.

SocketCAN leverages the concept of network devices, enabling:

- Multi-application access: Multiple applications can simultaneously use a single CAN device.
- Multi-network support: A single application can interact with multiple CAN networks concurrently.

²CAN in Automation, www.can-cia.org

Linux SocketCAN offers open-source drivers and a network stack for CAN (Controller Area Network) communication within the Linux operating system. It uses a familiar socket interface, similar to the Berkeley socket API, allowing applications to easily interact with the CAN bus. Supporting various CAN controllers, SocketCAN adheres to the ISO 11898 CAN protocol standard. This allows CAN bus communication using the same socket-based approach as with the internet, as shown in Figure 3.2 [63].

Key components of SocketCAN include:

- Network device drivers: These drivers facilitate communication with various CAN controllers.
- CAN protocol family implementation: This provides the necessary framework for CAN protocol-level operations within the Linux kernel.

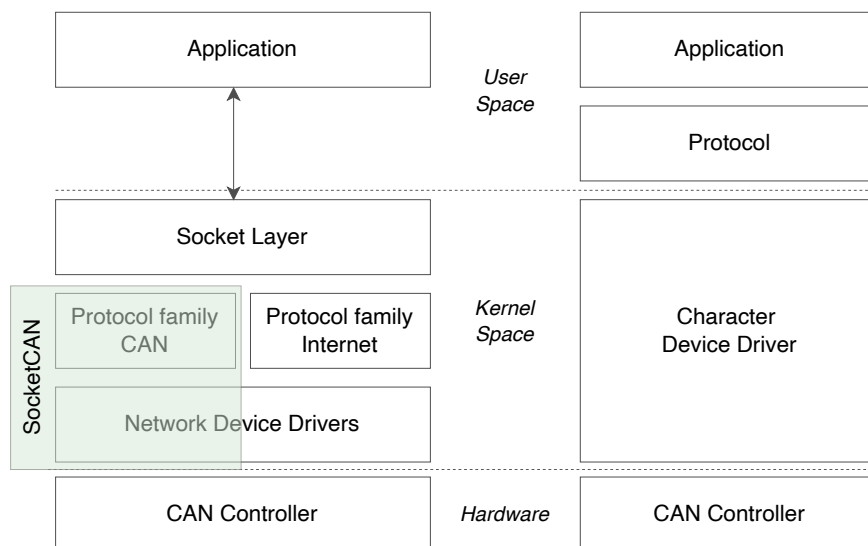


Figure 3.2: Typical CAN communication layers. With SocketCAN (left) or conventional (right). [64]

SocketCAN made it possible to virtualize the CAN bus, with one application generating speed indication messages by simulating a speed sensor and another one acting as a speedometer, displaying the speed to the user. The displayed speed would change according to the messages that were being generated and sent through SocketCAN in real time, the complete set-up diagram is shown in Figure 3.3.

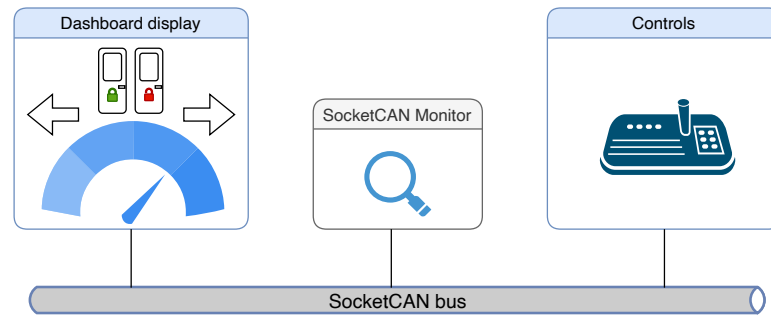


Figure 3.3: SocketCAN test set-up

3.4.1 How to monitor and analyse traffic

Now that we have devices that generate and acquire traffic messages, there was the need to monitor those messages that were exchanged. For it, the first approach was to use the `CANDump` tool, which allows you to print all data that are being received by a CAN interface. This tool is part of the `CAN-utils`³ package, and it is very similar to the well-known `TCPDump`⁴ tool. In this way, it was possible to monitor all traffic on the bus. To improve the message filtering, the `CANSniffer` tool was used, which allows to filter and see the message content in a more structured way. With this last tool, it was possible to identify which messages contained the speed information, as well as the messages of the direction change indicators. Another tool used in the message analysis was `CANPlayer`, used to replay the messages collected by `CANDmp` and `CANSniffer`. Just as a reference, `Wireshark` can also be used to monitor the `SkocketCan` bus.

After the initial approach of understanding the messages that were being exchanged and how to replicate them, it was now time to develop a component that would be able to filter the selected messages and process them. For this purpose, a software tool was developed in Python⁵ language, which allows the filtering and storage of the messages for further analysis.

The purpose of analysing the traffic was to learn the normal behaviour of the devices and to identify when a message was not part of the normal traffic behaviour. The selected approach was to use a Markov chain, next explained in 3.4.2.

3.4.2 Markov chains

Deterministic Finite Automata [65] or even Deterministic Probabilistic Automata (DPA) [66] have been suggested in the past as possible mechanisms to model Cyber-Physical Systems behaviour, at network and/or process level. Following a similar rationale, Cruz et al. [54] and, later on, Graveto et al. [55] suggested the adoption of Markov Chains for the same purpose, with other related mechanisms such as Discrete Time-Based Markov Chains (DTMCs) having been suggested by

³<https://manpages.debian.org/testing/can-utils/index.html>

⁴`TCPDUMP`, www.tcpdump.org

⁵www.python.org

other authors [67] [68].

A Markov chain is a mathematical model that represents a system shifting between different possible states. The core principle of a Markov chain is that the likelihood of transitioning to the next state is solely based on the current state, ignoring the history of how the system reached its current position. By creating numerous potential sequences of states using Markov chains, stochastic simulations can mimic the behaviour of real-world systems. By generating a large number of possible state sequences through Markov chains, stochastic simulations can approximate the behaviour of systems, helping to predict outcomes and assess risks [69][70]. Figure 3.4 is a diagram representing a two-state Markov process, the numbers are the probability of changing from one state "A" to another state "E" and the probability of staying in the same state.

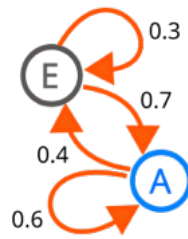


Figure 3.4: Diagram representing a two-state Markov process [71]

For the purposes of this thesis, it was decided to experiment with a Markov chain-based modelling approach, which was deemed adequate to model the specific behaviour/control patterns in CAN-based railway vehicular systems. This effort will be described in the next sections.

3.5 Software Tool description

The software tool was essentially focused on analysing the speed and its behaviour. The requirements for the software tool were:

- Learn the normal traffic of a conduit.
- Identify when a speed value is not expected, as an example of a change from 20 km/h to 22 km/h without the values in between.
- Identify when even the value is the one expected, but it changed too fast or too slow compared with the normal learned behaviour.
- Identify even when that value is in the learned pattern, but its probability is very low.

As stated above, the tool conceived to analyse the traffic was developed using the Python language. This tool performs the following tasks:

1. Monitors and captures the traffic from the SocketCan bus for a defined set of time and stores it in a file.
2. Reads the previously stored file and generates the Markov model of the captured values, which includes defining the current and the previous state speed and timestamp values, storing the values, and measuring the probability of the current value inside of all acquired messages. Calculate the time-difference between these specific values, and store the maximum and the minimum time-difference. The initial Python code used was based on [72], but modified to store message values as well as its time stamp. The calculation of the Markov model was also modified to include the maximum and minimum time difference between the occurrence of the pair current and previous messages.
3. After having the Markov model calculated, it monitors the bus, analyses each speed message against the model, and determines if the current and the previous values exist as a pair in the calculated model.
4. Checks whether the probability of this value to appear is lower than the expected value, even though it exists in the pattern.
5. If any previously described parameters do not match the learned ones, it will trigger a message.
6. Checks the time difference between the pair of messages against the stored ones and if that pair of messages took the time between the minimum and the maximum expected.
7. If the cadence between two speed messages is higher than the stored maximum value, the software tool will trigger a warning. This indicates that the values are being manipulated or that speed sensor malfunctioning.
8. If the cadence between two speed messages is lower than the stored minimum value, the software tool will trigger a warning. This indicates that the values are being manipulated or that speed sensor malfunctioning.
9. When the speed is greater than 4 km/h, if the open-door message is detected, the software tool will also trigger a warning.

For the development of the Python code, the following libraries were used:

- **python-can** - this library provides Controller Area Network support for Python, providing common abstractions to different hardware devices, and a suite of utilities for sending and receiving messages on a CAN bus [73]. This library was used to access the Socket Can.
- **asyncio** - is a library to write concurrent code using the `async / await` syntax [74]. This library was used to fetch the generated Markov model asynchronously, while messages were received through the socket, allowing these two tasks to run independently [74].

- **time** - this library provides various time-related functions [75]. This library was used to set the duration of the message capture, which was then used to build the initial Markov model.

In the developed tool, it was necessary to filter the speed values when the vehicle was at rest. This is because the message generator produced random values and because of its great granularity, sometimes it was possible that the pair of previous and current values did not exist. This behaviour would trigger the warnings that these messages are not in accordance with the expected Markov model, or if they were, their probability of occurrence was very low. To avoid this, all messages with values less than 4 km/h were ignored.

The analysis of the values described above can fulfil two purposes. The first is to detect whether the values are being manipulated with malicious intent by an external actor. Or, on the other hand, that the system is starting to malfunction, and this analysis can be very useful to detect failures in the system in an early state, even before the human operator or the maintenance team gets noticed of it.

Figure 3.5 shows the flow diagram of the software tool developed.

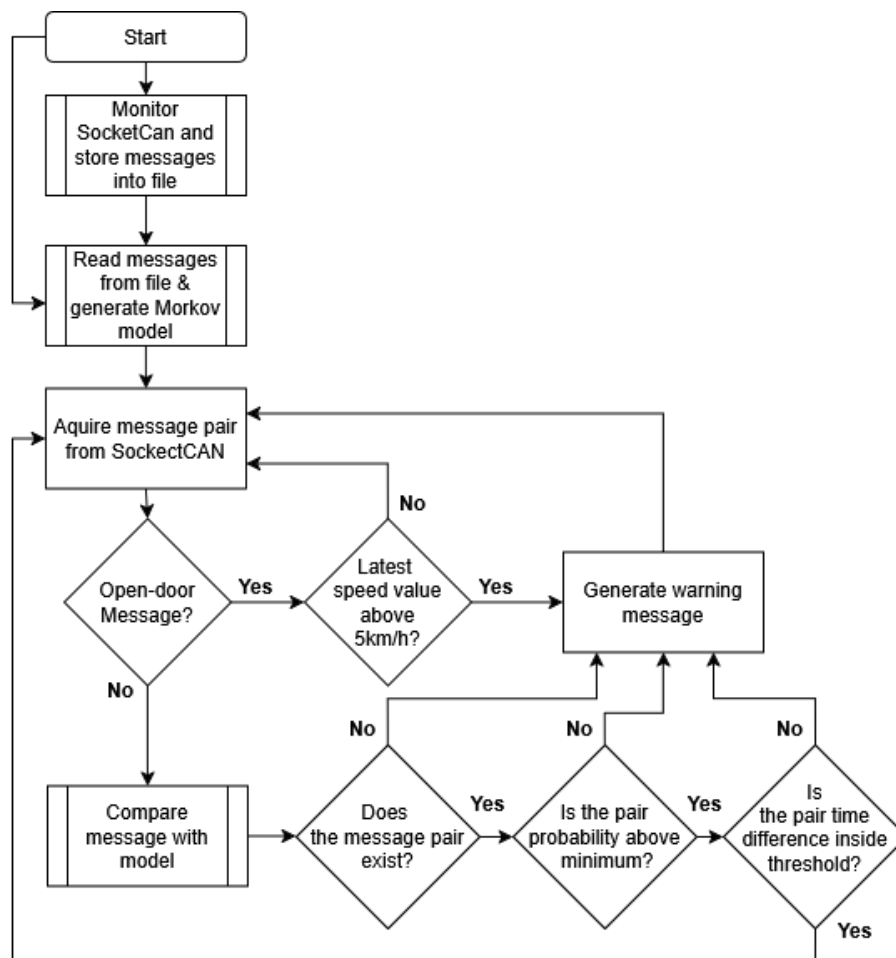


Figure 3.5: Software tool flow diagram

3.6 Software Tool Validation

The development of the software tool was subject to a simplified version of the Verification & Validation as applied in the railway industry, as shown in 3.6. There was a phase for gathering requirements and data, a first draft of the software tool for analysis, and discussion with tutor teachers. With the result of the review, the necessary changes should be applied, and the corrections should be implemented. Then, elaborate a verification document and perform the tests.

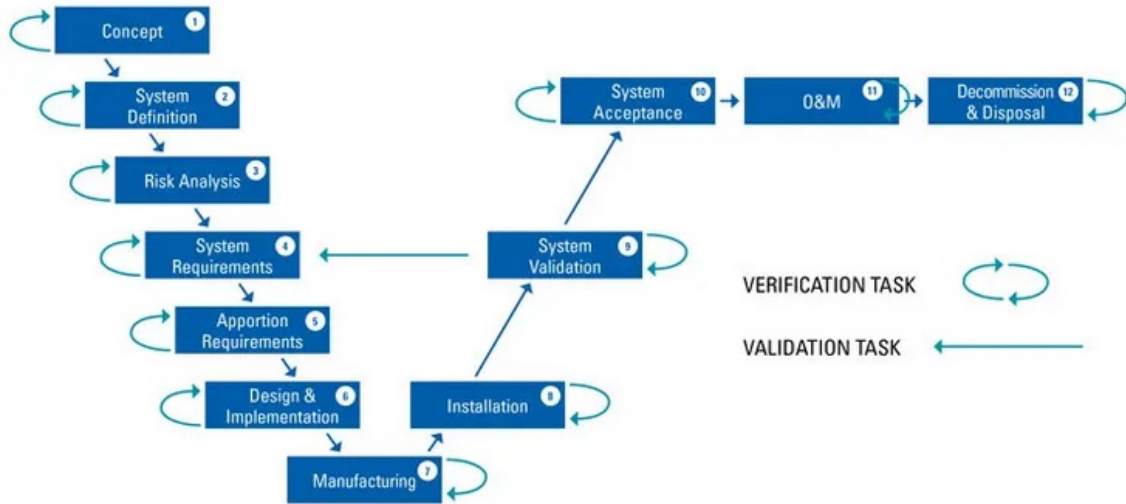


Figure 3.6: Railway V Cycle V-and-V Activities [76]

The software tool will be tested following the test cases in Table 3.1. For the development of the test cases, a back-box testing approach was followed, which tests the software against the specification of its external behaviour without knowledge of its internal implementation details.

To acquire data for the Markov model, the first step was to do the value acquisition for 1 hour, using the message simulator, and using its controls to increase and decrease the speed values simulating the normal operation of the system. In parallel, the traffic is also logged with CANDump. The recorded log from CANDump will then be modified in a way to include the various abnormal conditions that need to be identified by the software tool. The software tool is then replayed using CANPlayer. The speed values and the door messages will be monitored directly in the speedometer, which also includes an icon with the door status. The warning messages are displayed in the console output of the Python IDE.

Table 3.1: Tool Test cases

ID	Test case description	Test Steps	Test data	Expected Result	Actual Result	Status
1	With a speed message with values lower than 4 km/h, the system should not trigger any warning if the message pair is in the calculated model.	1.Replay message log with modified speed values.	Speed test existing in the Calculate model "244#00000001B9" and "244#00000001B7"	No warning is triggered.	No warning was triggered.	Pass
2	With a speed lower than 4 km/h, the system should not trigger any warning if there is an open-door message.	1.Replay message log with modified speed values. 2.At the same time activate the door-open message. 3.Door-open icon should be illuminated	Sent the open door message "19B#00000E000000" with speed under 5 km/h.	No warning is triggered. Door-Open icon ON	No warning was triggered.	Pass
3	With a speed lower than 4 km/h, the system should not trigger any warning if there is a closed-door message.	1.Replay message log with modified speed values. 2.At the same time activate the door-closed message. 3.Door-open icon should be deactivated.	Sent the open door message "19B#00000F000000" with speed under 5 km/h.	No warning is triggered.	No warning was triggered. Door-open icon off	Pass
4	With a speed message with values higher than 4 km/h, the system should trigger a warning if the message pair is not in the calculated model.	1.Replay message log with modified speed values that higher than 4 km/h and are not in the calculated model.	Message value "0000000943" in the replay	Warning is triggered with message "Message pair not in model"	Message displayed "Mar-25 13:12:57 - Message not in Markov model next state 0000000943 kmh ->23"	Pass
5	With a speed higher than 4 km/h, the system should trigger a warning if there is an open-door message.	1.Replay message log. 2.When speed is higher than 4 km/h activate activate the door-open message.	Sent the open door message "19B#00000E000000"	Warning is triggered with message "Door message"	Message displayed "02-Mar-25 13:14:04 - Door alarm, vehicle in motion"	Pass
6	With a speed higher than 4 km/h, the system should trigger a warning if there is an closed-door message.	1.Replay message log. 2.When speed is higher than 4 km/h activate activate the door-open message.	Sent the open door message "19B#00000E000000"	Warning is triggered with message "Door message"	Message displayed "Door alarm, vehicle in motion, speed->00000b000000"	Pass
7	With a speed higher than 4 km/h, the system should trigger a warning if the message pair probability is lower than the predefined value.	1.Replay message log that has a crafted message pair that only exists once.	Created single occurrence of message pair 0000000a1f and 0000000a0a	Warning should be triggered with message "Low probability message"	Message displayed "12-Mar-25 05:26:58 - Probability too low->0.00869565 for current message 0000000a1f kmh->25 and previous message 0000000a0a kmh->25"	Pass

Table 3.1 continued from previous page

ID	Test case description	Test Steps	Test data	Expected Result	Actual Result	Status
8	With a speed higher than 4 km/h, the system should trigger a warning if the interval between the previous value and the current value is higher than the maximum one in the model.	1.Replay message log that has a crafted message pair with time difference higher than the maximum recorded.	Set message pair "244#000000020D" and "244#000000021F" with 72ms of difference while its maximum in the model was 59ms	Warning is triggered with message "Message time difference too big"	Message displayed "12-Mar-25 08:53:41 - Warning time difference too big, current timestamp dif-> 0.07272648811340, stored timestamp_diff-> 0.05998100"	Pass
9	With a speed higher than 4 km/h, the system should trigger a warning if the interval between the previous value and the current value is lower than minimum the one in the model.	1.Replay message log that has a crafted message pair with time difference lower than the minimum recorded.	Sent message pair "244#000000017F" and "244#00000001FD" with time difference of only 100ms	Warning is triggered with message "Message time difference too small"	Message displayed "02-Mar-25 13:12:56 - Warning time difference too small, current timestamp dif-> 7.8678131103515, stored timestamp_diff-> 0.3737719999999"	Pass
10	The system should trigger a warning if the message value is not in the learned values in the model.	1.While message log is being replayed, send speed message with CANSend values that does no exist.	Crafted speed message with value 0000000943 that is not part of the model	Warning is triggered with message "Message not in the model"	Displayed message "02-Mar-25 13:12:57 - Message not in Markov model next state 0000000943 kmh -> 23"	Pass

3.7 Conclusions

The software tool detected all the abnormal conditions that it was meant to detect. Due to the number of false positives, it was necessary to adjust the probability threshold from when it detected a low probability of occurrence of a message pair. A similar adjustment was necessary for the time difference detection, as SockecCan is not deterministic, so the timestamp can vary by a few milliseconds, that is why it was also required to use a threshold for the time difference detection. This software tool still has the opportunity for improvement, by analyzing other message types that could be relevant for the train operation, like brake information, power information, and others. This would only require that the message filter and Markov model used can be updated to include them. In the final conclusion, the software tool can fulfill the proposed requirements.

Chapter 4

Conclusion

In the first phase of the dissertation, a detailed analysis of the applicable cybersecurity norms, security directives, and guidelines that are followed in the European Union and the United States related to railway cybersecurity was conducted. It also focused on the applicable governance in the EU and explained the dichotomy in the railway ecosystem of safety versus security. Comparing the two geographical regions applicable normatives and guidelines, it can be noticed that the U.S.A. is stricter in terms of mandatory regulation, as they are mandated to apply the Security Directives, it can also be concluded that there is also a greater "enterprise" perspective in terms of organization. On the other hand, the EU ones are more detailed and concise regarding what needs to be implemented. The railway operators considered critical suppliers have now also to follow the NIS2 directive, which on top of the technical requirements focused on TS50701, also has reporting obligations. Railway software and security system suppliers for access control, firewalls, and other related services and equipment, will also be required to comply with the Cyber Resilience Act beginning in 2027. These regulatory obligations pose great challenges for all involved in the industry. It also presents great opportunities for cyber security professionals that are required to analyse, test, implement, and maintain the security policies and controls implemented throughout the system life-cycle. It is also an opportunity for insurance companies to offer products related with cybersecurity, and as well for law and audit firms that need to keep track of all legislation applicable to cybersecurity and provide consulting in this area to railway operators and integrators.

Bearing in mind what is suggested in the guidelines, more specifically in TS50701 for new and legacy systems and following the approach of the Purdue model, in the second part of this dissertation, it was initially intended to develop a software application that could analyse critical conduits, especially in legacy systems, and detect abnormal behaviours in traffic data. The first major step back was the lack of cooperation of railway integrators, and especially railway operators, to support this academic work, despite several attempts to contact several organizations and entities.

Not being able to collect real data from a railway conduit, the author decided to pursue research on the protocols used in the railway industry. In the group of possible used protocols, it was then analysed which ones were publicly available

and for which ones we could have a message traffic generator. After consideration, the CAN protocol was selected as a target. This was instrumental to become acquainted with the difficulties of handling communications traffic for cybersecurity analysis purposes, something that became obvious during the development of the tool described in Section 3.

During the elaboration of this dissertation, there was also the opportunity to write a scientific paper that was presented at the 23rd European Conference on Cyber Warfare and Security, in June of 2024, held in the University of Jyväskylä, Jyväskylä, Finland. This was a great opportunity to present to others part of the work that was already being developed during the dissertation.

The general conclusion is that there is still a long way to go to reach a solid baseline in cybersecurity, but the foundations have been laid to help railway operators and suppliers achieve this goal.

References

- [1] J. Nunes, T. Cruz, and P. Simões, “Railway infrastructure cybersecurity: An overview,” *23rd European Conference on Cyber Warfare and Security*, pp. 331–340, 6 2024, doi: 10.34190/eccws.23.1.2296.
- [2] ENISA, *ENISA THREAT LANDSCAPE: TRANSPORT SECTOR*. ENISA, 2023.
- [3] Siemens, “Infrastructure in the cloud,” <https://www.mobility.siemens.com/global/en/portfolio/rail/automation/infrastructure-in-the-cloud.html>.
- [4] “U.S. department of homeland security- transportation security administration, security directive 1580/82-2022-01 - rail cybersecurity mitigation actions and testing,” 2022, U.S. Department of Homeland Security, 2022.
- [5] TrainSpread, “Japanese trains,” <https://www.trainspread.com/japan/shinkansen/>, 2023, [Online; accessed 14-12-2023].
- [6] N. Kapoor, “Understanding railway cybersecurity - isa - international society of automation, 2022,” <https://gca.isa.org/blog/understanding-railway-cybersecurity>, 2022, [Online; accessed 14-12-2023].
- [7] Mayor of London, “Transportation for london - what we do,” <https://tfl.gov.uk/corporate/about-tfl/what-we-do>, 2023, [Online; accessed 22-01-2023].
- [8] CENELEC, “A major step for railways cybersecurity: the new clc/ts 50701 - cen-cenelec,” <https://www.cencenelec.eu/news-and-events/news/2021/eninthspotlight/2021-06-10-new-clc-ts-50701-railways-cybersecurity>, 2021, [Online; accessed 01-09-2024].
- [9] —, “CENELEC EN 50126 - railway applications - the specification and demonstration of reliability, availability, maintainability and safety (rams),” 2017.
- [10] International Electrotechnical Commission, “IEC 62443-3-3- industrial communication networks – network and system security – part 3-3: System security requirements and security levels,” p. 80, 2013.
- [11] APTA-American Public Transportation Association, “Recommended practice-cybersecurity considerations for public transit,” American Public Transportation Association, Tech. Rep., 2022.

- [12] K. Zetter, "Solar winds," [Online; accessed 14-12-2023]. [Online]. Available: <https://www.wired.com/story/the-untold-story-of-solarwinds-the-boldest-supply-chain-hack-ever/>
- [13] L. Cébalski, S. BA, T. Chatelet, Y. Garnier, and Q. Rivette, "ENR135 - prise en compte des enjeux de cybersécurité au sein de la sécurité ferroviaire," <https://www.securite-ferroviaire.fr/reglementation/prise-en-compte-des-enjeux-de-cybersecurite-au-sein-de-la-securite-ferroviaire>, 2021. [Online]. Available: <https://www.securite-ferroviaire.fr/reglementation/prise-en-compte-des-enjeux-de-cybersecurite-au-sein-de-la-securite-ferroviaire>
- [14] R. Bergman, "Mysterious hacker group suspected in july cyberattack on iranian trains," <https://www.nytimes.com/2021/08/14/world/middleeast/iran-trains-cyberattack.html>, 2021, [Online; accessed 22-09-2024].
- [15] Intel471, "Meteor wiper | intel471," <https://intel471.com/blog/meteor-wiper>, 7 2021, [Online; accessed 22-09-2024].
- [16] P. S. Derby, "Cyber attack: Exploring the impact on the italian railways - pride solutions derby ltd." <https://pridesolutions.co.uk/cyber-attack-exploring-the-impact-on-the-italian-railways/>, 10 2023, [Online; accessed 22-09-2024].
- [17] R. Gallagher, "Belarus hackers allegedly disrupted trains to thwart russia," <https://www.bloomberg.com/news/articles/2022-02-27/belarus-hackers-allegedly-disrupted-trains-to-thwart-russia#xj4y7vzkg>, 2022.
- [18] CENELEC, "CLC/TS 50701 - railway applications - cybersecurity," CENELEC, Tech. Rep., 2021.
- [19] —, "CENELEC EN 50126 - railway applications - the specification and demonstration of reliability, availability, maintainability and safety (rams)," 2017.
- [20] European Parliament, "Council directive 2008/114/EC," 2008, resilience of critical entities.
- [21] —, "Directive (EU) 2022/2557 of the european parliament and of the council of 14 december 2022 on the resilience of critical entities and repealing council directive 2008/114/ec (text with eea relevance)," <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2557&qid=1729500087411>, 12 2022. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2557&qid=1729500087411>
- [22] European Commission, "REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification ," <https://eur-lex.europa.eu/eli/reg/2019/881/oj>, 2019, [Online; accessed 03-1-2024].

-
- [23] —, “NIS 2 directive,” <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32022L2555>, 12 2022.
 - [24] —, “Commission Implementing Regulation (EU) No 402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment,” <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32013R0402#d1e758-8-1>, 2013, [Online; accessed 03-1-2024].
 - [25] —, “DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, concerning measures for a high common level of security of network and information systems across the Union,” <https://eur-lex.europa.eu/eli/dir/2016/1148/oj?locale=en>, 2016, [Online; accessed 03-1-2024].
 - [26] Publications Office of the European Union, “Regulation (eu) 2024/2847 of the european parliament and of the council of 23 october 2024 on horizontal cybersecurity requirements for products with digital elements and amending regulations (eu) no 168/2013 and (eu) no 2019/1020 and directive (eu) 2020/1828 (cyber resilience act) (text with eea relevance),” <http://data.europa.eu/eli/reg/2024/2847/oj>, 11 2025.
 - [27] European Commission, “Cyber resilience act | shaping europe’s digital future,” <https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act>, 1 2025, [Online; accessed 26-01-2025].
 - [28] CENELEC, “About CENELEC,” <https://www.cenelec.eu/about-cenelec/>, 2024, [Online; accessed 03-1-2024].
 - [29] M. Dick, J. Baca, and E. Plemons, “Railway cybersecurity regulations and standards,” <https://www.railwayage.com/cs/railway-cybersecurity-regulations-and-standards/>, 2023, [Online; accessed 03-1-2024].
 - [30] U.S. Transportation Security Administration, “U.S. department of homeland security- transportation security administration, security directive 1580/21-01 - enhancing rail cybersecurity,” 10 2022, <https://www.tsa.gov/sd-and-ea>.
 - [31] J. Henriques, F. Caldeira, T. Cruz, and P. Simões, “Combining K-Means and XGBoost Models for Anomaly Detection Using Log Datasets,” *Electronics*, vol. 9, no. 7, 2020, doi: 10.3390/electronics9071164.
 - [32] K. Barmapsalou, T. Cruz, E. Monteiro, and P. Simoes, “Mobile forensic data analysis: Suspicious pattern detection in mobile evidence,” *IEEE Access*, vol. 6, pp. 59 705–59 727, 2018, doi: 10.1109/ACCESS.2018.2875068.
 - [33] APTA-American Public Transportation Association, “Securing control and communications systems in transit environments - part i: Elements, organization and risk assessment/management,” American Public Transportation Association, Tech. Rep., 2010.
 - [34] —, “Securing control and communications systems in rail transit environments - part iiii: Attack modeling security analysis white pape,” American Public Transportation Association, Tech. Rep., 2015.

- [35] —, “Securing control and communications systems in rail transit environments - part ii: Defining a security zone architecture for rail transit and protecting critical zones,” American Public Transportation Association, Tech. Rep., 2013.
- [36] “Welcome to railroadradio.net!” <http://www.railroadradio.net/>, [Online; accessed 2-12-2023].
- [37] R. Queiroz, T. Cruz, J. Mendes, P. Sousa, and P. Simões, “Container-based virtualization for real-time industrial systems—a systematic review,” *ACM Computing Surveys*, vol. 56, no. 3, Oct. 2023, doi: 10.1145/3617591.
- [38] K. Stouffer, “Guide to operational technology (ot) security,” <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf>, 2023.
- [39] T. H. A. Nguyen, J. Trinckauf, T. A. Luong, and T. T. Truong, “Risk analysis for train collisions using fault tree analysis: Case study of the hanoi urban mass rapid transit,” *Urban Rail Transit*, vol. 8, pp. 246–266, 12 2022.
- [40] A. T. Limited, “Amenaza technologies limited,” <https://www.amenaza.com/>, 2025, [Online; accessed 2-12-2023]. [Online]. Available: <https://www.amenaza.com/>
- [41] Security and Trust of Software Systems Group - University of Luxembourg, “Attack-defense tree tool,” <https://satoss.uni.lu/members/piotr/adtool/>, 2023, [Online; accessed 2-12-2023]. [Online]. Available: <https://satoss.uni.lu/members/piotr/adtool/>
- [42] NIST, “Guide for conducting risk assessments,” <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>, 2012.
- [43] —, “Managing information security risk :,” <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf>, 2011.
- [44] P. Bowen, J. Hash, and M. Wilson, “Information security handbook :,” <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf>, 2006.
- [45] Gartner, “MSSP,” <https://www.gartner.com/en/information-technology/glossary/mssp-managed-security-service-provider>, [Online; accessed 14-12-2023].
- [46] S. Soderi, D. Masti, and Y. Z. Lun, “Railway cyber-security in the era of interconnected systems: a survey,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, pp. 6764–6779, 7 2022.
- [47] H. Parkinson, D. Basher, and G. Bamford, “Railway cyber security and ts50701,” in *Proceedings of the Fifth International Conference on Railway Technology: Research, Development and Maintenance*, vol. 1. Civil-Comp Press, 6 2023, pp. 1–9.

-
- [48] B. Castanier, M. Cepin, D. Bigaud, C. Berenguer, E. H. Okstad, R. Bains, T. Myklebust, and M. G. Jaatun, "Implications of cyber security to safety approval in railway," *Proceedings of the 31th European Safety and Reliability Conference*, 2021.
 - [49] S. Soderi, D. Masti, M. Hämäläinen, and J. Iinatti, "Cybersecurity considerations for communication based train control," *IEEE Access*, vol. 11, pp. 92 312–92 321, 2023.
 - [50] EVOLEO, "Evoleo, "cybersecurity in the railway - safety and security requirements of rail," CYRAIL, Tech. Rep., 2017.
 - [51] ENISA, "Railway cybersecurity - security measures in the railway transport sector," ENISA, Tech. Rep., 2020.
 - [52] S. Gordeychik, "Cyber resilience of railway signaling," *dummy*, 2019.
 - [53] "Oops! train control centre passwords revealed on bbc tv," <https://mobile.twitter.com/gcluley/status/594098708406530048>, 2015, password revealed.
 - [54] T. Cruz, J. Barrigas, J. Proença, A. Graziano, S. Panzieri, L. Lev, and P. Simões, "Improving network security monitoring for industrial control systems," in *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, 2015, pp. 878–881, doi:10.1109/INM.2015.7140399.
 - [55] V. Graveto, L. Rosa, T. Cruz, and P. Simões, "A stealth monitoring mechanism for cyber-physical systems," *International Journal of Critical Infrastructure Protection*, vol. 24, pp. 126–143, 2019, doi: 10.1016/j.ijcip.2018.10.006.
 - [56] L. Rosa, T. Cruz, M. B. de Freitas, P. Quitério, J. Henriques, F. Caldeira, E. Monteiro, and P. Simões, "Intrusion and anomaly detection for the next-generation of industrial automation and control systems," *Future Generation Computer Systems*, vol. 119, pp. 50–67, 2021, doi: 10.1016/j.future.2021.01.033.
 - [57] T. Cruz, J. Proença, P. Simões, M. Aubigny, M. Oedraogo, A. Graziano, and L. Yasakhetu, "Improving cyber-security awareness on industrial control systems: The CockpitCI approach," *Journal of Information Warfare*, vol. 13, no. 4, pp. 27–41, 2014. [Online]. Available: <https://www.jstor.org/stable/26487465>
 - [58] M. B. de Freitas, L. Rosa, T. Cruz, and P. Simões, "SDN-enabled virtual data diode," in *Computer Security. ESORICS 2018 International Workshops, Cyber-ICPS 2018 and SECPRE 2018*, S. K. Katsikas and et al., Eds. Cham: Springer International Publishing, 2019, pp. 102–118, doi: 10.1007/978-3-030-12786-2_7.
 - [59] National Instruments Corp., "Controller Area Network (CAN) Protocol Overview - NI," <https://www.ni.com/en/shop/seamlessly-connect-to-third-party-devices-and-supervisory-system/controller-area-network--can--overview.html?srsId=AfmBOoqTiHHdPr3xmL9ZegqyHv94G2ysupe06ABiPrVDVrDJ8AKNOkAy>, 11 2024, [Online; accessed 13-01-2025].

- [60] S. Corrigan, "Introduction to the Controller Area Network (CAN) application report introduction to the Controller Area Network (CAN)," in *Application Report*, 6 2016.
- [61] K. AB, "Can protocol in railway," <https://kvaser.com/about-us/applications/railway/>, 1 2025, [Online; accessed 13-01-2025].
- [62] International Electrotechnical Commission, "International standard iec 61375-1 - electronic railway equipment–train communication network (tcn)." in *International Standard IEC 61375-1*. International Electrotechnical Commission, 6 2012, p. 105.
- [63] dissecto GmbH, "Socketcan — knowledgebase," <https://munich.dissec.to/kb/chapters/can/can-socketcan.html#socketcan>, 2023, [Online; accessed 06-02-2025].
- [64] M. Emilio, "Embedded linux design: Hardware and drivers, eeweb article," <https://en.wikipedia.org/wiki/SocketCAN>, 10 2024, [Online; accessed 17-01-2025].
- [65] N. Goldenberg and A. Wool, "Accurate modeling of modbus/tcp for intrusion detection in scada systems," *International Journal of Critical Infrastructure Protection*, vol. 6, no. 2, pp. 63–75, 2013. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1874548213000243>
- [66] P. Matoušek, O. Ryšavý, M. Grégr, and V. Havlena, "Flow based monitoring of ics communication in the smart grid," *Journal of Information Security and Applications*, vol. 54, p. 102535, 2020. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2214212619311329>
- [67] M. Caselli, E. Zambon, and F. Kargl, "Sequence-aware intrusion detection in industrial control systems," in *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security*, ser. CPSS '15. New York, NY, USA: Association for Computing Machinery, 2015, p. 13–24. [Online]. Available: <https://doi.org/10.1145/2732198.2732200>
- [68] M. Caselli, E. Zambon, J. Petit, and F. Kargl, "Modeling message sequences for intrusion detection in industrial control systems," in *Critical Infrastructure Protection IX*, M. Rice and S. Sheno, Eds. Cham: Springer International Publishing, 2015, pp. 49–71.
- [69] dida Datenschmiede GmbH, "What is a markov chain?" <https://dida.do/what-is-a-markov-chain>, 1 2025, [Online; accessed 25-01-2025].
- [70] K. Academy, "Origin of markov chains (video) | khan academy," https://www.khanacademy.org/computing/computer-science/informationtheory/moderninfotheory/v/markov_chains, 2025, [Online; accessed 06-02-2025].
- [71] Joxemai4, "File:markovkate 01.svg - wikimedia commons," https://commons.wikimedia.org/wiki/File:Markovkate_01.svg, 5 2013, [Online; accessed 25-01-2025].

-
- [72] S. Dutta, “Markov chain nlp,” <https://www.kaggle.com/code/orion99/markov-chain-nlp>, 2021, [Online; accessed 02-02-2025].
- [73] B. Thorne, “python-can 4.5.0 documentation,” <https://python-can.readthedocs.io/en/stable/>, 2010, [Online; accessed 01-04-2025].
- [74] Y. Selivanov, P. G. Salgado, A. Kumar, Łukasz Langa, and S. Ostrowski, “asyncio — asynchronous i/o — python 3.13.2 documentation,” <https://docs.python.org/3/library/asyncio.html>, 2025, [Online; accessed 01-04-2025].
- [75] Python.org, “time — time access and conversions — python 3.13.2 documentation,” <https://docs.python.org/3/library/time.html>, 2025, [Online; accessed 01-04-2025].
- [76] TÜV, “Independent verification and validation for railway,” <https://www.tuvsud.com/en/industries/infrastructure-and-rail/rail/complete-system-services/independent-verification-and-validation-for-railway>, 2023, [Online; accessed 14-1-2024].