CYbersecurity in the RAILway sector

D2.1 – Safety and Security requirements of Rail transport system in multi-stakeholder environments

Due date of deliverable: June 2017

Leader of this Deliverable: EVOLEO

Reviewed: UIC

Document status		
Revision	Date	Description
001	2017-04-07	Draft of Document
002	2017-06-20	First issue of Document
003	2017-09-04	Second Issue of Document
004	2017-10-09	Content of document closed
005	2017-10-15	Revision of Document

Start date of project: 2016-10-01 Duration: 24 months

REPORT CONTRIBUTION

Name	Company	Details of contribution
L. ALEXE	UIC	Contributions on section 3
H. Pereira, P. Ribeiro	EVOLEO	Contributions on section 2, 5, 6, 7, 8 and 9
Bonneau/Marqués	UIC	Contributions on introduction, section 1, 2, 3, 4, 5, 7 and 9, and Revision

Objectives of the Deliverable

In **D2.1 – Safety and security requirements of rail transport system in multi-stakeholder environments**

This deliverable is the result of efforts made in two tasks of WP2, namely T2.1 Rail systems within the public transport environment and T2.2 Safety and security of the Railways systems.

In T2.1 Rail systems within the public transport environment, we had analyses from a cyber-security and safety point of view the main rail sub-systems (networks, signalling, communication, train control systems ...) as well as the various processes (traffic management, infrastructure management, maintenance, station management, passenger information...), people involved, the interactions with the other operators and the public area in an operational environment, and the dependencies with external stakeholders.

In T2.2 Safety and security of the Railways systems, we researched the security technologies and processes already used in the rail environment to ensure a comprehensive protection of the system and especially availability, integrity and confidentiality of the data. This has also considered technologies available on the IT sector, due to its relevance.

As such, this deliverable focus on two main accomplishments:

1. The identification of the requirements for safety and security in railways, and which functions are acceptable to lose;
2. The inventory of technologies and solutions available and already in place to promote cybersecurity of systems and data.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

With more than 400 billion passenger-kilometres per year (2015) and a steady increase trend, railways represent a key-asset in the overall European transportation scenario, as well as a critical infrastructure which is due to be properly protected.

For the whole railway sector, the paramount goal to be achieved in the coming years is that of further rising its share in the transportation sector expanding its geographical reach, delivering innovative and integrated travel solutions for people and goods while guaranteeing the highest service standards in terms of safety and security.

Railways have been so far generally considered as a 'safe domain' with regard to cybersecurity issues, mainly because they rely on proprietary, segregated networks with specific protocols for management, communication and signalling.

The near future, though, will bring many challenges for the relevant stakeholders. The main challenges are the following:

- Rail Systems are more and more connected and open.
- Rail Technologies are becoming more and more interoperable and harmonized
- Threats (human and technology based) - are adapting quickly to traditional security detection methods

The deployment of ERTMS traffic management system along with its planned evolution and integration within the framework of existing national systems, the future advent of a successor to the GSM-R communication system and the growing need for secure remote maintenance are only a few among the many aspects that will need highly integrated and comprehensive cybersecurity standards and procedures.

The need for a smarter mobility for people and goods will call for a new generation of intelligent transportation services. Customers are constantly seeking for reliable and seamless internet connectivity not only to plan, book and manage their journeys, but also to entertain themselves or work inside the stations and on the trains.

The shift towards inter-modal transports will require management systems capable of connecting previously separated layers and entities, but also of preventing malicious attacks directed to new potential weak spots in the chain.

Moreover, the heterogeneous and geographically-distributed nature of the railway infrastructure could expose many layers of the system to both cyber-physical and physical-cyber-attacks, potentially involving or triggering domino effects within the same or different domains.

In this context, this document gives an overview on safety and security requirements of rail transport system in multi-stakeholder environments. The work was supported by the ongoing UIC project ARGUS which focus on “Availability and Security Challenges of Open Networks aiming of their use in signalling of railways”.

The document starts with a general overview on the rail system, its specificities, the stakeholders, the main rail functions to be protected against cyberattacks and a focus on signalling system which is considered as a main critical IT system within railway system.

Based on questionnaire sent to UIC members within the ARGUS project, a set of requirements for ensuring security of the main assets, functions and processes is detailed and some solutions currently used by some companies to protect the rail system are described.

To complete this analysis focusing on railway systems, an inventory of existing security technologies and processes as well as standards and rail related normative which are available is made.

2. TERMINOLOGY TO BE USED IN THE DOCUMENT

Table 1 - Acronym Description

Acronym	Description
AES	Advanced Encryption Standard
BGP	Border Gateway Protocol
COPS	Common Open Policy Service
CTC	Centralized Train Control
DC	Data Confidentiality
DES	Data Encryption Standard
DMZ	Demilitarized zone
ERA	European Railway Agency
ERTMS	European Rail Traffic Management System
GSM-R	Global System for Mobile Communications - Railway
HIDS	Host detection intrusion system
IAC	Identification and Authentication Control
IDPS	Intrusion Detection and Prevention Systems
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Protection System
LDAP	Lightweight Directory Access Protocol
MPLS	Multiprotocol Label Switching
NBA	Network behaviour analysis
NIDS	Network intrusion detection system
OF	Optical fibre
PA	Public address
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PMC	Policy Management Console
PR	Policy Repository
QOS	Quality Of Service
RA	Resource Availability
RDF	Restricted Data Flow
RRIDS	Rail Radio Intrusion Detection System

Acronym	Description
SI	System Integrity
SIEM	Security Information and event Management
SIL	Safety Integrity Level
SSL	Secure Sockets Layer
TRE	Timely Response to Events
TSI	Technical Specifications for Interoperability
UC	Use Control
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
WDM	Wavelength Division Multiplexing
WeOS	Westermo Operating System
WIDS	Wireless Intrusion Detection System

3. RAIL SYSTEM OVERVIEW

The figure below gives an overview of the railway system:

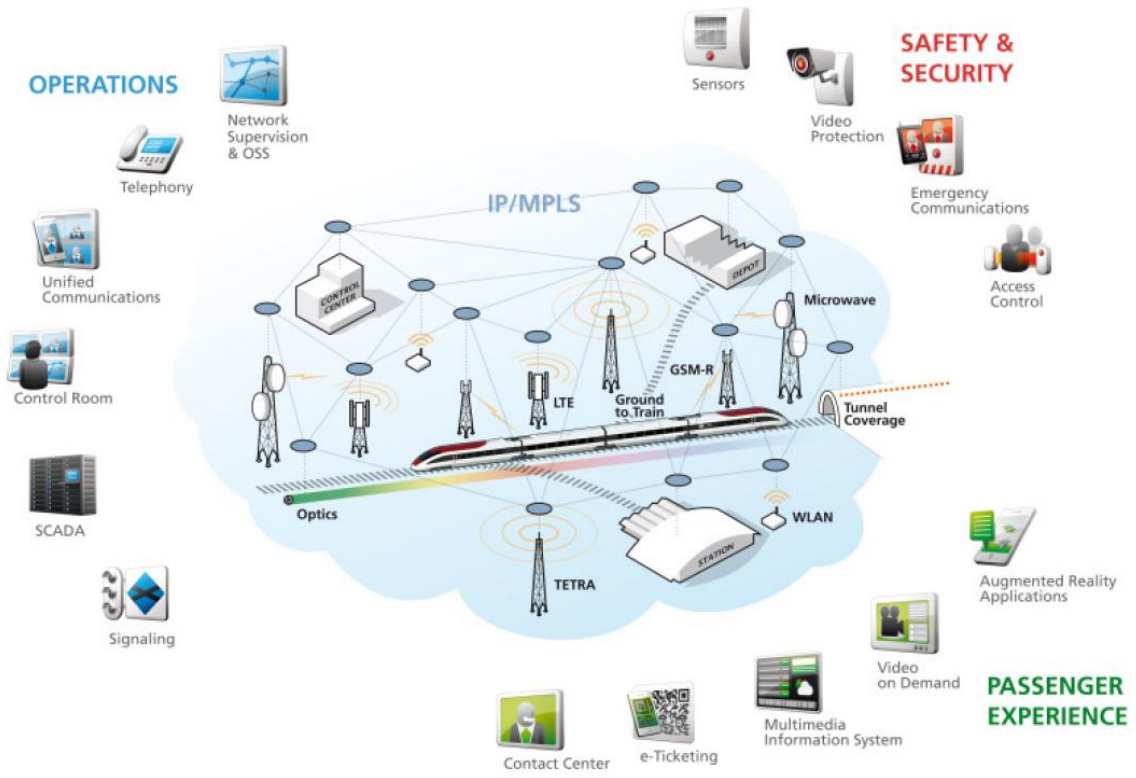

Figure 1 - Railway system scheme

There are several differences between a rail transportation system and a single manufacturing site:

- **Distance** - A rail system covers vast distances, and each segment of the rail system has to communicate with its adjacent segments and with the operations control centre (and backup operations control centre). Transit agencies are expert at the physical security aspects of their systems. Cybersecurity adds a new dimension to the security program. In addition, a rail system includes self-contained equipment rooms located along the tracks, known variously as signal bungalows and waysides.

- **Communication -** A transit agency needs to communicate with maintenance crews on or near the track; with engineers/drivers (if applicable); between the train set and the wayside; and between and among the control and signal devices, such as signals, road crossing gates, track circuits, various maintenance and detection devices, passenger information displays, emergency information displays, advertising displays, and others.

- **Power -** A transit system often has its own traction power stations for electricity. There are power feeds from local utilities that need to be coordinated. Power is distributed via catenaries or third rail. Additional power is required to run all other equipment, including lighting, communications and signals. There are differences between a railway electrical system and most other commercial systems; the most common difference is the use of floating ground.

- **People -** The purpose of a transportation system is to move people. They are the precious cargo of the system, and they expect and need to be delivered safely. Transit systems have many large, public areas, including entrances, exits, platforms, waiting areas and amenities (toilets, cafes, etc.) that must allow everyone access. There are other areas that need to be restricted, such as equipment and power rooms, tracks, signalling systems, employee areas and so on.

- **Access to property-** Transportation system assets, on the other hand, are out in public. Physical security exists—much of it to keep the public from dangerous areas, such as power sources, third rails, overhead wiring, the path of trains and so on—but it is impossible to keep determined individuals away from the transportation system's assets.

  Transit agencies need to focus on prevention and detection of people accessing key

3.1 RAILWAY SYSTEM STAKEHOLDERS

3.1.1 Infrastructure manager

Railway infrastructure is the physical support of the whole railway system.

Infrastructure managers for railways are responsible for management of infrastructure, exploitation, development, and organization and supervision of predictive and corrective maintenance including maintenance works to replace old assets or complete installations.

With predictive maintenance, failures are avoided with programmed actions based on statistics or experience, performing the adequate maintenance actions or replacing the corresponding assets before the foreseen failure.

For corrective maintenance, they are responsible of tracking these activities, supervising the reparation and reviewing and updating statistics for the occurred failure, studying the case and proposing (if needed) changes in predictive maintenance schedule and/or procedures.

They are one of the main agents of railway system, and responsible of making it available for the rest of the stakeholders, to allow them to operate according to the technical specifications and safety rules.

3.1.2 Maintainer

Maintainers are the responsible for performing the scheduled maintenance activities following the stablished procedures, producing maintenance reports for the infrastructure managers.

For corrective maintenance, maintainers perform the activities to re-stablish the correct railway operation, preparing the respective reports for the infrastructure manager.

3.1.3 Passenger operator

Passenger services are managed by passenger railway operators in coordination with traffic management to organize the passenger trains schedule with responsibility on the readiness of trains and passenger services on-board. This passenger services may include internet connection onboard, and this service can be provided by the infrastructure manager.

3.1.4 Interaction with other operators

Operators, freight and passenger ones, obtain their slots for traffic from the traffic manager. International traffic (both passengers and freight) need additional exchange of information to coordinate their services (ticket selling, freight tracking, etc) usually through dedicate VPN and receiving traffic situation information from the traffic manager.

3.1.5 Dependencies with external stakeholders

Several external stakeholders also have information interchange with traffic and maintenance managers, such as ticket selling, last mile transport, external maintenance companies. For all of

them, the information exchange with the railways manager is critical for performing their work, so safe and reliable communication between their systems must be assured.

3.1.6 Interaction in public areas

Station are growing not only as passenger boarding places, but as commercial areas and leisure places.

Station managers are responsible for the passenger information services, providing ticket sales services and even, in some cases, telecommunication services to stores and restaurants.

3.1.7 Interactions in operational environment

Operational environment often includes intermodal stations and ports, where passengers and freight switch the transport method. This implies coordination for all the transport methods for better efficiency by exchanging information on real time about the actors involved (trains, trucks, boats, buses, etc.) For this information interchange is required to link somehow the information from the different stakeholders.

3.2 RAIL FUNCTIONS LOSS SEVERITY

Railway systems may have different nature and purpose, including all related to passenger services, operators, stations, operations, maintenance, etc. These systems are all interconnected by communication networks which can have different configurations, management and physical configuration, but with many connection points which are at the same time their strength and their weakness. These wide communications networks allow the transfer of information for all the involved partners, but they represent also a possibility for the intrusion of possible attackers.

From the point of view of the infrastructure manager, the most sensitive network is the one dedicated to operations, as this is the network in charge of sending the command control to the interlockings along the line. A loss of this network could mean the impossibility to remote controlling the operation of trains and losing track of them in the CTC (Centralized Train Control).

This a long-distance network, as usually the CTC is far from the controlled line or at least at the middle of a long line to control.

This network is also responsible for providing information to other stakeholders about the trains position, which is the basis for other systems as the Passenger Information Services, automatic PA (Public Address), logistic services for freight trains, handover of international trains, etc.

At a higher level (and thus with less effect on other networks) are the stakeholders' networks. Ticket selling, fleet management, freight tracking, passenger services, logistics, station services, etc. Disruption on these networks can lead to various levels of severity effect, but most of them with less critical effect.

In the table below, we can find a classification for the impact of the loss of these networks:

Table 2 - Classification for network loss impact

Network	Description	Impact loss in human context	Impact loss in financial context	Impacto loss in operational context
Field I/O equipment	To interconnect field elements between them and with the interlocking	High	Medium/High	Medium/High
Interlocking	To interconnect interlockings and RBC between them	Medium/High	High	High
Control center	To connect the interlockings to control centers and control center between them	Low	High	High
Passenger services	Information to passenger services (timetables displays, automated public adress)	Low	Medium	Medium
Freight services	Freight tracking for clients, international handover of freights, …	Low	Medium/High	Low
Ticketing services	Connecting with travel agencies with reservation systems, connection with accounting, etc	Low	Medium/High	Low
Infra manger intranet	Internal services for infraestructure manager	Low	Medium/Low	Low

The severity for the impact is only considering the unavailability of the network. In case of malicious hacking, able of taking control of safety elements (field I/O equipment, Interlocking and RBC) the effect could be much worst.

A table including the signalling assets loss impact, can be found on Annex 1.

3.3 RAILWAY SIGNALLING

Within the rail system, railway signalling is considered as a main critical IT system. The security in railway signalling is a composition of different vectors:

- Network security,
- Deployment security,
- and Signalling security.

To design a good security strategy, all vectors need to be considered. While deployment security belongs mainly to the supplier, the other vectors that need to be defined are the Network security and the Signalling security.

The railway system has some particularities: the system is running 24/24 all year round, the availability of the signalling of the critical system leads to unsafe situations, the critical network is huge so that we can never consider them as totally closed. The critical network is a real-time network, therefore certain classical solutions cannot be applied. This is a main part in addition to the safety question of the signalling.

- **Network security:** We define as network security all aspects related to the protection of the telecommunication network that works as a carrier of signalling data. It is envisage protecting the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure. According to the IEC 62443, the network security is composed of three pillars that create the security triad: **technology**, **process** and **people**. Within this triad we have defined **technology** as the set of resources used to uphold availability, integrity and confidentiality. **Process** involves the set of guidelines and standard adopted in to define clear procedures that must be followed in order to ensure the security. Last but not least, we group in **people** the set of formation requirements of the staff, their training and the assignment of roles of responsibility and access, according to the functions the personnel will deploy. This covers the management of people working directly or indirectly with signalling equipment and network, such as the access privileges for people to physically or logically access signalling equipment or places, as well as the requirements for hiring these personnel.
- **Signalling Safety**: This group involves all techniques and technologies related with the signalling system by itself and the mechanisms implemented for facing possible attacks or malfunctions. We subdivide this group also in two. One will be related to the

functional analysis, which is the internal disposition to check the "plausibility" of sent or received message. A plausibility test can be made on two sides: interlocking and control centre. This is the case, for example, if the delivered commands meet with a common signalling behaviour for a pre-defined route-map. It also involves the structure and hardware and software architecture used for the signalling system (protocols for safety, security, etc). The second, the **continuity of the system**, involves all techniques and methodologies used for guaranteeing the continuity of the service in adverse conditions, such as intrusion tests, cooperation with cyber security experts, etc.

- **Deployment security:** This group is related with the operative routines deployed by its company for managing signalling network and equipment. On the one hand it covers the **methodology used for adding new equipment** or replaces the old one while keeping the safety and security levels. Within this group there are also included the deployment agreements established between suppliers and railway manager in terms of product security requirements, as well as the support of the product along its lifetime.

4. SAFETY AND SECURITY REQUIREMENTS

4.1 DEFINITION OF RAIL SAFETY AND SECURITY

Safety is at the core of rail activity. It's the total responsibility of the railways companies, infrastructure and undertakings since the beginning of the rail, whereas security is often a shared responsibility with authorities especially police.

Safety is the state of being "safe". The condition of being protected against physical, social, occupational, psychological, or other types or consequences of failure, damage, error, harm or any other event which could be considered as non-desirable. Safety is protection against accidental events, but these can come from internal causes (faults, errors, omissions…) and external causes (for example 3rd parties at level crossings or natural disasters and climate events)

Security as a state or condition is resistance to harm. From an objective perspective, it is a system or structure's actual (conceptual, and never fully known) degree of resistance to harm. Security is protection against intentional damage (delinquency, terrorism, cyber-attacks ….)

On the one hand, safety policy is managed internally by rail company in a precise framework involving human factors, technical failures, probabilisation of safety events and thinking in term of cost benefit. On the other hand, security policy is structured around partnerships with national authorities. Railways focus on their vulnerabilities and level of threat is defined by the authorities. The threats, especially regarding cybersecurity, are constantly evolving, consequently a probability-based analysis and a cost-benefice approach are less relevant than there are for safety.

Safety and security requirements are originally different but need to be coherent since both safety risk and security threats can lead to exploitation or accidents, causing serious damages and many casualties.

4.2 RAIL SAFETY REQUIREMENTS

At European level there is a common regulatory framework for railway safety which is described in DIRECTIVE 2004/49/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 29 April 2004 on safety on the Community's railways.

The European Union Agency for Railways established the Technical Specifications for Interoperability (TSIs) for the railways systems or subsystems to meet the essential requirements and to ensure the interoperability of the European Community rail systems. Therefore, all systems TSI compliant must fulfil the stablished requirement for the different subsystems. TSIs are covering areas such as Rolling Stock (locomotive and passenger rolling stock, noise and wagons), Fixed installations (infrastructure and energy), Common TSIs (control command and signalling, persons with reduced mobility and safety in railways tunnels) and Functional TSIs (operation and traffic management, telematics applications for freight service and telematics applications for passenger services).

One of the tasks of ERA is also the common approach to safety to support an effective single European rail area, by developing a common approach to safety management systems, risk assessment, the understanding of human performance, safety monitoring and the sharing of safety data.

As it is usual for most of the industrial systems, Safety Integrity Level (SIL) classification is used for railways. This SIL levels are based on the maximum probability of a dangerous failure and a minimum safe failure fraction.

Most of the Control Command and Signalling (CCS) systems, when related to direct control of track devices or detection systems, are required to have a Safety Integrity Level (SIL) 4, as for continuous operation system with direct impact for many human lives, the maximum level for system integrity is required.

Also, railways systems, tend to be fail-safe, even against wrong human behaviour, so a wrong human action on a control device can’t lead to a risky situation as the system will impede these situations, stopping the train if needed if all safety conditions are not fulfilled.

If some external actions can change the SIL level of most sensitive systems (SIL 4), to a lower SIL level, these can lead to unsafe situations even without wilfulness. With an intentional attack SIL level can be reduced to the minimum, and lead to very dangerous and harmful situations.

Having this in mind, is impossible to think of safety without having security in mind, as a fail for security can have huge impact on safety.

4.3 RAIL SECURITY REQUIREMENTS

The following sets of requirements for ensuring information security are needed for equipment performing train and shunting control functions (Railway Automation and Telemechanic systems and devices) and their associated critically important facilities (processes):

1. Requirements for personnel and other people involved in the operation of Railway Automation and Telemechanic systems and devices
2. Physical protection requirements
3. Access management requirements
4. Requirements for data storage devices
5. Software requirements
6. Intrusion detection requirements
7. Information security incidents response requirements
8. Reliability requirements

During formulating the requirements, it is necessary to consider the following points:

- Hardware and software of the Railway Automation and Telemechanic systems and data security hardware and software are allowed to be supplied to the object only if they have unexpired documents according to their technical documentation, and confirming their compliance with the requirements established in the technical documentation;
- Information transmission lines and local area networks that are part of the Railway Automation and Telemechanic systems should be designed in accordance with the established norms of technological design. During the construction of these lines and networks, any deviations from the design documentation are prohibited;
- Radio equipment used within Railway Automation and Telemechanic systems must be registered in accordance with the established procedures;
- All technical means and facilities must not have any damage.

4.4 REQUIREMENTS FOR STAFF

People involved in the operation of Railway Automation and Telemechanic can be categorized in four main groups:

- **Operational staff** – employees of operating companies involved in the management, maintenance and repair of Railway Automation and Telemechanic systems.
- **Users** – people assigned to operational staff and directly involved in processing information.
- **Support staff** – employees of operating companies carrying out work unconnected to the operation of Railway Automation and Telemechanic systems.
- **Administrators** – personnel responsible for installing and carrying out maintenance on Railway Automation and Telemechanic systems software. These people are employees of third-party companies: developers, manufacturers (suppliers) and specialist organizations (service centres) carrying out such work under a contract with the railway company.

4.4.1 Operational staff

People assigned to operational staff should carry out only those tasks that fall within the scope of their official duties, providing such tasks do not violate their established rights of access and do not compromise information security, including attempts to:

- Carry out unauthorized alterations to hardware architecture or Railway Automation and Telemechanic systems software.
- Use non-standard data storage devices.
- Run programs that are not related to the functioning of Railway Automation and Telemechanic systems.
- Circumvent established access procedures.
- Access a public network.
- Carry out other actions that may threaten information security.

4.4.2 Users

The following information security requirements are established for users of Railway Automation and Telemechanic systems:

- The user should promptly report any compromises to information security and/or mistakes they have committed themselves when processing information. They should not search for the cause of the breaches or mistakes themselves.
- The user should not attempt to remove suspicious programs themselves.

4.4.3 Support staff

The following additional information security requirements are set for employees of operating companies:

- The employee should understand the level of his or her authority, the limits of which should be defined in the job description.
- If the employee's official duties change or the employee is transferred to a different control area, the attributes and means by which this employee obtains access to the system should be revised. His or her old account should be closed and new one created.
- Employees that choose to leave the company should have their access rights to Railway Automation and Telemechanic systems revoked. They should return all attributes and means associated with Railway Automation and Telemechanic systems. Access to information created by the outgoing employee should be provided to other authorized employees in a timely manner.
- If an employee is responsible for a breach of information security and fails to report this breach to management, or fails to report it in a timely manner, the employee should be identified and the appropriate disciplinary action taken. The employee should receive prior notice of such disciplinary action.

4.4.4 Administrators

People who are not employees of operating companies who, as part of their official duties, have access to Railway Automation and Telemechanic systems must satisfy the following requirements:

- All actions carried out by such people in relation to Railway Automation and Telemechanic systems should be done under the strict supervision of an authorized employee and documented.

4.5 PHYSICAL PROTECTION REQUIREMENTS

Physical security and protection of Railway Automation and Telemechanic facilities should be provided through the use of the engineering and technical means set out in the railway company's regulatory documentation.

Constant monitoring of communications should be carried out on the outer perimeter of the facility, as well as on premises that house Railway Automation and Telemechanic equipment and software. A permit (access control) system should be in place:

- Lists should be drawn up of people who are permitted access to the facility and/or premises that house Railway Automation and Telemechanic equipment and software. Credentials should be issued in accordance with the rules established in the regulatory documentation.
- The relevant officials must review and approve the access lists and credentials.
- Access lists should be reviewed on a periodic basis, as set out in the regulatory documentation.
- A screening process must be passed before physical access to Railway Automation and Telemechanic is granted.

Railway Automation and Telemechanic equipment and software can only be supplied to the facility if in-date documents confirming the compliance of said equipment and software with the terms set out in the technical documentation can be produced.

Data protection hardware and software can only be supplied to the facility upon production of an in-date certificate. Cable channels and Railway Automation and Telemechanic link systems, as well as local area networks that are part of these systems, should be designed in accordance with the established norms for the technical design of automation and telemechanic devices. When building channels and communication lines, the design of local area networks cannot deviate from the design documentation. Radio equipment used as part of Railway Automation and Telemechanic systems should be registered in the prescribed manner. All the above-mentioned equipment and facilities must be free from damage. Facilities should be equipped with the following:

- Power supply systems with redundancy types and rates suitable for the Railway Automation and Telemechanic system as an electricity user. In case of major emergencies, such power supplies must be capable of de-energizing any part of Railway Automation and Telemechanic system;
- Means of automatic fire suppression and automatic fire warning.

Means of ensuring compliance of the operational conditions of Railway Automation and Telemechanic systems with the requirements of the technical documentation set forth in the relevant specifications should be provided. At the site of Railway Automation and Telemechanic systems setup and operation:

- All hardware, software and firmware installation and uninstallation should be monitored.
- Use of new information processing hardware should be authorized by management based on the results of the relevant expert evaluation.
- Use of personal information processing or storage hardware for any actions related to accessing (interfering with) Railway Automation and Telemechanic systems should either be eliminated or authorized.
- Configuration changes to software and information processing hardware should be conducted only based on and in compliance with duly executed documentation bearing all necessary signatures and stamps and registered in a logbook (record log).

4.6 ACCESS MANAGEMENT REQUIREMENTS

Access management requirements include:

- Identification and authentication requirements.
- Access management requirements.
- Registration and recording requirements.
- Integrity control requirements.

4.6.1 Identification and authentication requirements

Requirements for ensuring safe internetworking between Railway Automation and Telemechanic systems that, according to their operational conditions, can be accessed remotely.

A password policy needs to be applied to all users of Railway Automation and Telemechanic systems. This policy should require to:

- Set up a multiple-use password containing at least six (6) letters and numbers and not containing any personal data or any other information that could identify the user.
- Refrain from sharing their password with others.
- Update the password at regular intervals.

4.6.2 Access management requirements

A list of access objects as well as a list of allowed and authorized access types for each user should be defined in the systems. Any changes to the said access rights can be made by the

Railway Automation and Telemechanic systems administrator only. Railway Automation and Telemechanic systems software should have functionality allowing access to unauthorized objects and access types to be denied.

User identification and authentication based on the active password should take place during logon.

4.6.3 Registration and recording requirements.

Every login (logout), operating system loading, initializing or program halt should be registered

Recording parameters should include: date and time of user login (logout) or system loading (halt), and the results of the login attempt (successful or unsuccessful). In case of Railway Automation and Telemechanic hardware shutdown, logouts should not be registered.

4.6.4 Integrity control requirements.

Railway Automation and Telemechanic system and technological software should have settings to block unwanted programs from running and unauthorized data storage devices from connecting to the system.

System and technological software of Railway Automation and Telemechanic should not contain:

- Software development and debugging tools.
- Tools allowing compiled code modification during information processing.
- Program recovery tools that allow for two copies of system and technological software components to be backed up, regular updating and performance monitoring should be provided.

Requirements for ensuring secure internetworking should be specified upon assigning a railway company or its respective subdivision to Railway Automation and Telemechanic systems, which that according to the terms of operation can be accessed remotely.

4.7 REQUIREMENTS FOR DATA STORAGE DEVICES

Data storage devices used in Railway Automation and Telemechanic systems include:

- Dismountable (portable) electronic data storage devices.
- Paper information carriers (paper data storage devices).

Electronic data storage devices with system and technological software of Railway Automation and Telemechanic systems written on them should provide information modification protection.

Only authorized people should have access to data storage devices. The list of people authorized to access data storage devices should be minimal. People not on the list should never be given access to data storage devices.

The procedures for ensuring the protection of data storage devices from unauthorized access should be defined.

The list of persons authorized to access data storage devices should be minimal. Persons not on the list should never be given access to data storage devices.

All data storage devices at the site of Railway Automation and Telemechanic systems setup and operation should be registered. Electronic data storage devices should bear labels allowing for their unambiguous identification.

The storage locations of data storage devices and their backup copies should be identified. Backup copies should be stored at a separate location to the main storage devices.

Transporting data storage devices should be controlled to ensure the device remains in hands of authorized people only.

Before transferring an electronic data storage device to be used outside of a Railway Automation and Telemechanic systems setup and operation site, such device should first be formatted. Steps taken to format the device should be monitored and documented.

Data storage devices not intended for future use should be disposed of.

4.8 SOFTWARE REQUIREMENTS

Software requirements include:

- Requirements ensuring the nonexistence of undocumented software features.
- Requirements ensuring protection from unauthorized software.
- Antivirus protection requirements.
- Requirements for monitoring the software under operation.

These requirements are obligatory for all software used in Railway Automation and Telemechanic systems. Antivirus protection requirements can be omitted if the software developer (supplier) can justify the inexpediency of using antivirus protection.

For technological software used in Railway Automation and Telemechanic systems, a means of ensuring the nonexistence of undocumented features should be provided.

Use of unauthorized software by the administrator and users of Railway Automation and Telemechanic systems should be prohibited. Moreover, use of any software obtained through insecure communication channels or via a local computer network should be prohibited. Protection from unauthorized software should include steps to investigate the causes of unauthorized or altered files being introduced into software applications.

Railway Automation and Telemechanic systems software should provide for:

- Inspections conducted by the administrator to detect virus threats on software components and identify unknown viruses.
- Restoring software components to their original state, i.e. the state they were in before the virus threats.
- Conducting regular updates of antivirus protection tools.
- Real-time monitoring to detect virus threats.
- Weekly or daily antivirus system self-inspection.
- The ability to remove virus source code from the infected components.

Railway Automation and Telemechanic system software should be monitored in accordance with the railway company's regulatory documentation.

The operation of Railway Automation and Telemechanic systems should allow software bugs to be fixed and developer (supplier) updates to be installed.

4.9 INTRUSION DETECTION REQUIREMENTS

These requirements should be imposed by the railway company or its respective subdivision on facilities that house and operate Railway Automation and Telemechanic systems and which must be accessed remotely. Tools for detecting and alerting users about information threats should be provided.

Moreover, the following information should be registered:

- Information on detected network traffic anomalies.
- Type of detected threats, date and time of threats detection.
- IP addresses of the source and object of the threats.
- Port number of the source and object of the threats.
- Detected threats priority level.

4.10 INFORMATION SECURITY INCIDENTS RESPONSE REQUIREMENTS

Railway company management should be informed immediately of any information security incidents. The following procedures should be introduced at the sites of Railway Automation and Telemechanic systems setup and operation:

- Incident notification and response.
- Feedback on the results of incident response.
- Error analysis. This is to ensure that errors are eliminated and corrective measures taken, to ensure that those measures were themselves not compromised and all actions taken were duly authorized.

Incident management should include detection, analysis, prevention, problem resolution and recovery of Railway Automation and Telemechanic systems after incidents. All information security incidents should be monitored and documented on a continual basis. Incident reports should be provided to set recipients according to the prescribed format, frequency and lists.

4.11 RELIABILITY REQUIREMENTS

Software reliability requirements specification is a foundation of the software developer's work. It should include the desired characteristics of the developed software, but not the development procedure itself. It should be phrased and organized in a manner that would make it complete, clear, precise, unambiguous, verifiable, checkable, adjustable and executable.

Software requirements specification should be expressed and described in a way that is understandable for the personnel.

Software requirements should specify and document all interfaces between the interacting systems. Requirements specification should describe all allowed Railway Automation and Telemechanic system software operation modes along with all programmable electronic devices operation modes, especially in case of failure. Any reciprocal limitations between software and hardware should be specified and documented.

Requirements specification should set the levels of software self-inspection and hardware program check. Software self-inspection means detection and notification by the software of failures and errors.

Both qualitative and quantitative software reliability requirements should be imposed. It is assumed that the software reliability level cannot be the same as or below the Railway Automation and Telemechanic system reliability level.

Railway Automation and Telemechanic systems software architecture should meet the set software reliability requirements. It should identify and assess the reliability significance of the present interaction between the system software and hardware, and analyse the requirements imposed by the system architecture on its software.

The parts of Railway Automation and Telemechanic systems software that most affect the reliability of the system should be minimized. If the software consists of components with different reliability levels, it should be considered as an object with a reliability level equal to the highest reliability level of its components. Cases where there is evidence of independence between components with different reliability levels are considered exceptions. Such evidence should be specified in the software architecture specification.

Architecture specification should be built in such a way as to allow the chosen techniques and steps to meet the software requirements in terms of the set software reliability level.

5. FOUNDATIONAL REQUIREMENTS

ISA/IEC-62443 is a series of standards from the International Society of Automaton that define procedures for implementing electronically secure Industrial Automation and Control Systems. In the standard ISA-62443-1-1 [1], a set of foundational requirements were specified in order to help determined the security level of cybersecurity systems. The standard defines that all aspects associated with meeting a desired security level (people, processes and technologies) are derived through meeting requirements associated with the following foundational requirements:

- Identification and Authentication Control (IAC);
- Use Control (UC);
- System Integrity (SI);
- Data Confidentiality (DC);
- Restricted Data Flow (RDF);
- Timely Response to Events (TRE);
- Resource Availability (RA);

Rather than compressing security levels down to a single number, a vector is used to express the nuances associated with often complex security or protection levels. This vector of security levels allows definable separations between security levels on a requirement by requirement basis.

This chapter contains descriptions of each foundational requirements, as well as cybersecurity technologies commonly used to achieve such requirements.

5.1 IDENTIFICATION AND AUTHENTICATION CONTROL (IAC)

Identification and Authentication Control (IAC) defines the necessary capabilities to reliably identify and authenticate all users (humans, software processes and devices) attempting to access assets or systems [1].

The goal of IAC is to protect the system from unauthenticated access by verifying the identity of any user requesting access to system components (interfaces, data, hardware) before activating

the communication, therefore ensuring protection for three major principles in information security: confidentiality, integrity and non-repudiation.

The system owners will need to build a list of authorized users (human, software processes and devices) for assets in the system, in such a way that users can be uniquely identified and authenticated. Each zone of control in the system may require different security levels, which most likely leads to various access restrictions levels and even differences in the authentication process.

There are multiple ways a user can authenticate before the system, such as passwords, personal identification numbers (PINs), tokens or biometrics [2]. In cybersecurity, the most common authentication mechanism is password authentication. However, the most secure is usually a multifactor authentication, using more than one of the previously mentioned methods [3].

5.2 USE CONTROL (UC)

Use Control (UC) defines the necessary capabilities to enforce the assigned privileges of an authenticated user (humans, software processes and devices) to perform the requested action on the system or assets and monitor the use of these privileges [1].

The goal of UC is to protect the system from unauthorized access by verifying that an authenticated user has the necessary privileges to perform the request action. There actions include reading or writing data, downloading, updating or deleting files and accessing restricted networks. UC is fundamental to ensure data integrity and confidentiality.

Systems owners will need to grant each user (human, software process or device) the necessary privileges to access systems components (data, interfaces or networks). Ordinarily, instead of changing user privileges one by one, authorization groups are created, each with different access levels to system components. Then, users are assigned groups according to their expected privileges and role in the system. User privileges may be dependent not only on the action he is trying to perform, but also his current location time-of-day/date.

5.3 System Integrity (SI)

System Integrity (SI) defines the necessary capabilities to guarantee the integrity of system components to prevent unauthorized manipulation [1].

The goal of SI technologies is to ensure that a system and its data are not illicitly modified or corrupted, mostly by looking for malicious code and unauthorized accesses [4].

Even before production, systems will often go through multiple testing cycles to ensure that the system is working as intended. After production, the SI is dependent on the integrity of its components, each with their own integrity protection based on their security risk assessment.

SI technologies maintain the integrity of physical and logical assets. Physical assets are monitored both while operational and non-operational, for instance, when in storage or during a maintenance shutdown. Logical assets should be monitored while in transit or at rest, such as when being transmitted over a network or when in a data repository.

5.4 Data Confidentiality (DC)

Data Confidentiality (DC) defines the necessary capabilities to safeguard the confidentiality of information on communication channels and in data repositories to prevent unauthorized disclosure [1].

The goal of DC is to ensure any type of information is only made available to authorized users (humans, software processes and devices).

Information confidentiality must be preserved whether at rest or in transit, that is, whether while moving over the network or while in storage. This infers that communication channels and data-stores must have protection against eavesdropping and unauthorized access.

5.5 Restricted Data Flow (RDF)

Restricted Data Flow (RDF) defines the necessary capabilities to segment the control system via zones and conduits to limit unnecessary flow of data [1].

The goal of RDF is to prevent information leakage by reducing the amount of communication channels used and by managing the flow of information.

By examining each system components information requirements, the system owner can specify the necessary information flow restrictions and, consequently, determine the configuration of the conduits used to deliver such information.

Building these information conduits will require the implementation of restrictive networking policies, configured with technologies such as unidirectional gateways, firewalls and demilitarized zones.

5.6 Timely Response to Events (TRE)

Timely Response to Events (TRE) defines the necessary capabilities to respond to security violations by notifying the proper authority, reporting needed evidence of the violation and taking timely corrective action when incidents are discovered [1].

The goal of TRE is to make sure that the system continues operational after an incident (breach, failure, integrity violations) while generating the necessary reports to notify the system administrators and ensuring accountability for the incident.

For the system to have TRE capabilities, asset owners must specify security policies, authorized operation procedures, recovery plans and lines of communication and control needed to respond to security violations [5]. To achieve this, set of diverse technologies must be used as a group, including monitoring and logging tools, network configuration tools and access control tools.

5.7 Resource Availability (RA)

Resource Availability (RA) defines the necessary capabilities to guarantee the availability of the control system against the degradation or denial of essential services [1].

The goal of RA is to ensure that the system is resilient against various types of denial of service attacks. While the system should implement countermeasures to mitigate or even prevent this kind of attack, RA focus is to make sure these incidents don’t affect the security and safety of the system, even in case of partial or total unavailability.

Availability failures such as power outages, system upgrades, hardware failures or denial of service attacks, can be prevented with the usage of tools and techniques like redundancy (power, network and hardware), firewall configurations and failover systems.

6. SAFETY AND SECURITY SOLUTIONS

This task provides a non-exhaustive inventory of the security technologies and processes to ensure a comprehensive protection of the system and especially availability, integrity and confidentiality of the data. The main intent was to capture the landscape for the railway in this subject. However, due to the lack of available information, the work was centred in the best practices and some technologies available in the IT sector and their potential link to the railway environment.

This analysis complements the deliverable on safety and security requirements of rail transport system in multi-stakeholder environments.

The solutions presented are directly covering security issues that can ultimately become safety problems. The safety aspect herein is treated as a possible consequence of security breaches or weaknesses.

6.1 ACCESS CONTROL

Access control ensures that access to resources such as network devices or attached systems can be only accomplished by authorized users, while also allowing analysis and understanding of attacks against protected resources. This section presents access control technologies used in cybersecurity.

6.1.1 Authentication

Authentication is the act of confirming entity identity to grant system access, requesting verifiable characteristics or unique information known by both parties of the process. These authentication credentials can be categorized into [3]:

- Knowledge factors: *"Something you know"*, this factor is based on something the user knows (e.g., a password, security question);
- Ownership factors: *"Something you have"*, this factor is based on something the user has (e.g., physical token, smart card);
- Inherence factors: *"Something you are"*, this factor is based on something the user is or does (e.g., biometric identifiers, signature).

Types of authentication systems differ on the number of combined identification factors used, which in turn provide different levels of security [6]:

- Single-factor: A system that uses only a single factor (e.g., id/password combination). It provides the weakest protection and it is not recommended for transactions which require a higher level of security;
- Two-factor: A system that uses two combined factors (e.g., password plus a physical token), used in very-high-security system;
- Three-factor: A system that uses three combined factors (e.g., password plus a physical token and a biometric identifier).

6.1.2 Perimeter Protection

Perimeter protection (or network segmentation) technologies prevent untrusted/unauthorized system access, creating a barrier (logical and/or physical) between protected and unprotected (open) network areas, to protect a network or a single device.

Content Filtering and Management

Content Filtering and Management monitors the type of data that flows in a network, restricting content access outside user's boundaries (e.g. avoiding potentially dangerous downloads and denying access to certain web pages) and scanning data to find viruses or non-compliant information [6].

Firewalls

A Firewall is a network security technology that monitors and controls the network traffic through a barrier between a secure internal network and outside networks (potentially not secure). It can consist of hardware, software or a combination of both. Firewalls can be categorized into four types [6]:

- Packet filters: Works at the IP layer of the TCP/IP protocol stack [7], matching each IP packet with a defined rule set to allow it to move forward in the network or be

discarded. Rules can include IP address, port number and protocol used. Generally, this type of firewall has low impact on network performance;

- Circuit level gateways: Works at the TCP layer of the TCP/IP protocol stack [7], monitoring TCP handshaking among packets to confirm whether a requested session is genuine or not. This type of firewall hides information about a protected network, because the information passed to a remote computer through a circuit-level gateway appears to have originated from the gateway;
- Application Level Gateways or proxies: Works by inspecting packets in the application layer of the OSI model, filtering application-specific commands such as HTTP GET. The gateway runs a proxy for each service (incoming and outgoing packets cannot access services that do not have a proxy), ensuring no direct contact between a trusted client and an untrusted host (proxy server) (e.g. If the gateway runs a FTP proxy, only packets generated by this service could pass and the other services would be blocked) [8];
- Stateful multilayer inspection: Combine the aspects of the previous types of firewalls: filtering IP packets, checking the legitimacy of the session and filtering packets contents at the application layer;

Denial of service (DoS) attack, one the most common and well known of the network attacks (20% of network attacks [9]), focus on exhausting network, servers, host and application resources. The current countermeasure in the perimeter protection relies on firewalls and Intrusion Detection Systems (IDS), with distinct but complimentary roles. Firewalls implement access control and audit functions (with different security levels) and intrusion detection focus on detect and react to computer misuses [10].

Network Address Translation (NAT)

This technology was designed to provide additional security, hiding the entire internal network behind a firewall and providing transparent routing to end hosts. Private IP addresses (unregistered IP addresses) in the internal network are translated into routable IP addresses (it is possible for all internal addresses to share the same external IP address). NAT allows devices, such as a router, to act as an agent between the Internet/public network and a local/private network [11][12].

Application Level Gateways

The Application Level Gateways (ALG) uses Stateful Packet Inspection (SPI) (also known as Dynamic Packet Filtering) which verifies if the network traffic conforms to the protocol, checking if packet sequence numbers are within a valid range for the session, discarding packets with invalid sequence numbers. Additionally, ALG uses application proxy techniques (see 0 Application Proxy) to control access between networks. Furthermore, ALG can perform NAT [6].

Application Proxy

These systems act as a firewall at the application level, examining packets and with full visibility of data exchanges in this level. Understanding the applications protocols at application level allows security threats to be detected (would not be detected on the packet level) (e.g. scanning a HTTP response body for malware detection) and consequently implement security policies as deemed appropriate.

Demilitarized Zones

A Demilitarized Zone (DMZ) is a physical or logical subnetwork placed between an internal network (trusted zone) and the Internet (untrusted zone) to avoid a direct communication, separating the private network from the external services and providing an additional security layer.

Usually, a DMZ architecture defines three areas [13] controlled by the external and internal firewalls, which protect and restrict access to/from the DMZ:

- The Public area (Internet) is accessible to the external public, typically used for public Web services or application services provided by the company.
- The Middle area (DMZ) is used to host systems that can provide data and application services, preventing external users from accessing the internal area.
- The Internal area represents the corporate or trusted network, with all systems and data in line with company security policies and standards.

Wavelength-Division Multiplexing

In Wavelength-division Multiplexing (WDM) technology, each communication channel is allocated to a different frequency and multiplexed onto a single fibre, creating physically isolated networks over the same optical fibre. Fibre optic sensors can provide perimeter protection, monitoring continuously the integrity of the transmission line, with option of locating possible disturbances, not only ensuring safety of data transfer but also quick response in case of wiretapping [14].

Virtual Private Network

Virtual Private Networks (VPN) are used for interconnecting networks, extending a private network across a public network and enabling remote users to access resources within the private network and receive benefits such as security and reliable connectivity. A dedicated virtual point-to-point or point-to-cloud connection is established to provide secure data channel or channels.

VPNs can be categorized into three types [6]:

- Layer 2 VPNs (L2VPN): Emulates the behaviour of a LAN facility, as if devices were connected to a common LAN segment. Generally, the following services are provided: Virtual Private Wire Service (VPWS) (also known as Ethernet over MPLS or ETHoMPLS), the simplest form for enabling Ethernet services over Multiprotocol Label Switching (MPLS) (a type of data-carrying technique) and Virtual Private LAN Service (VPLS) that supports the connection of multiple sites in a single domain over a IP/MPLS network, deploying a more complete emulated LAN service.
- Layer 3 VPNs (L3VPN): Also known as Virtual Private Routed Network (VPRN), emulates the behaviour of a WAN facility, allowing multiple sites to communicate securely at the IP level over a MPLS network, distributing routing information between sites and forwarding data packets to proper destinations. Typically, L3VPN sends/receives VPN related data using the Border Gateway Protocol (BGP) and uses Virtual Routing and Forwarding (VRF) techniques (multiple routing tables can exist and work in the router simultaneously) to create and manage user data.
- Layer 4 VPN: Establish connections over TCP in the Transport Layer (Layer 4), commonly using Secure Sockets Layer (SSL) (a cryptographic protocol) for establishing an encrypted link, providing a secure channel for securing transactions over public networks.

VPNs are based on the network tunnelling concept, which involves establishing and maintaining a logical network connection (data path) between networked devices. The tunnel is transparent to network operations. VPN protocols for Internet-based VPNs encapsulates the packets within Internet Protocol (IP) packets, supporting authentication and encryption in order to maintain the tunnels secure.

VPNs security aspects are different depending on the type, with more features in ascending order from Layer 2 VPN to Layer 4 VPN. User authentication is not available in Layer 2 VPNs with Frame relay, ATM, MPLS, PPP, L2F technologies and Layer 3 VPNs with MPLS technology. Data encryption, key management and integrity checking are not available in Layer 2 VPNs and Layer 3 VPNs with MPLS technology.

Some examples of technologies / tools / frameworks related:

- F5 Networks VPN: https://f5.com/products/big-ip/access-policy-manager-apm
- Cisco VPN: http://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/index.html
- Citrix VPN: https://www.citrix.com/networking/consolidate-remote-access.html
- Dell SonicWALL VPN: https://www.sonicwall.com

6.2 CRYPTOGRAPHY

Cryptography is about applying techniques for secure communication in order to protect information, preventing third parties from accessing them. Additionally, it is used to authenticate the sender and to ensure non-repudiation and confidentiality. It's based on enciphering/decipher data using mathematical tools with encryption/decryption keys, transforming the original information into a non-intelligible code which is subsequently used to recover the same [6].

6.2.1 Encryption

Cryptosystems can be divided into symmetric-key and asymmetric-key (also known as public-key) algorithm types.

In the first type, encryption and decryption process use the same key or with a second key difference obtainable through a simple transformation. The difficulty of cracking the key ensures the security of algorithm.

Examples of symmetric-key algorithms include [15]:

- Data Encryption Standard (DES): Created in 1975 and standardized in 1977, uses a 56-bit (and 8 parity bits) key and now is considered insecure mainly due key size (too small). A DES key was broken in 22 hours and 15 minutes and theoretical weaknesses in the cipher has been demonstrated.
- Advanced Encryption Standard (AES): Specified in 2001, is nowadays the most popular and widely adopted symmetric-key algorithm. Uses a 128, 192 or 256-bit key, provides full specification and design and is implementable in C and Java.
- Blowfish: Designed in 1993, uses a variable key length (32 up to 448-bit) and a 64-bit block size. Blowfish's block size makes it vulnerable to birthday attacks (attacks that exploit a mathematics problem in probability theory). It is recommended not to use the algorithm to encrypt files larger than 4 GB.

The second type uses a public key, disseminated widely, to perform the encryption process and a private key, known only by the owner, paired with the public key for the decryption process. Only paired keys (public and private) will be able to decrypt, ensuring the security of this type of algorithm.

Symmetric-key algorithms are usually faster than public-key algorithms but with the significant drawback of key management to keep them secure. The main problem of public-key algorithms is the authenticity of the public key, assured by a digital certificate that associates the public key to the holder of the certificate. The public key infrastructure (PKI) binds public keys with entities (person and organizations), certifying the ownership of the keys.

6.2.2 Key Exchange

In key exchange (also known as key establishment), cryptographic keys are securely exchanged, allowing secure encrypted communication between two parties by encrypting messages to be sent and decrypting messages received.

A session key is encrypted using asymmetric encryption with the receiver's public key, sent and decrypted by the receiver’s private key. Both sender and receiver now use the same encryption

key, allowing for symmetric encrypted connection faster than asymmetric encryption. Once that session is over, the key is discarded [16].

The same mechanism applies to transaction keys, but the validity scope of the keys is different, being restricted to only one transaction and no longer to a session.

6.2.3 Digital Signatures

A digital signature is an electronic authentication that binds an entity to digital information and can be independently verified, confirming the identity of the sender and also information integrity. Digital signatures and digital certificates are often used together, seeing that to create a digital signature, you must sign a digital certificate (which proves identity and is issued by a certification authority) [17].

Some examples of technologies / tools / frameworks related:

- Comodo: https://www.comodo.com/
- Symantec: https://www.symantec.com/
- GoDaddy: https://www.godaddy.com/
- GlobalSign: https://www.globalsign.com/en/
- SwissSign: https://www.swisssign.com
- Deutsche Telekom: https://www.telesec.de/en/
- Let's Encrypt: https://letsencrypt.org/

6.3 System Integrity

System integrity involves checking the state of the system periodically, monitoring modifications in critical system files by comparing the current state to a baseline state (integrity measurement) and monitoring code executions, such as executables or libraries, in order to detect and avoid system invasions [18]. This section presents different tools and technologies used to maintain system integrity in computer systems and networks.

6.3.1 Antivirus

Worms, computer viruses and Trojan horses are malicious software programs ("malware") that affect the integrity of the system by modifying the system and its data. Antivirus technology, also known as anti-malware software, helps protect systems against attacks by preventing, detecting and removing malicious software.

A worm is a standalone malware that replicates itself, spreading from one system to another using computer networks, taking advantage of network weaknesses. Computer viruses are a type of malware that replicates themselves when executed, modifying other files by inserting its own code into them, infecting the file(s) and consequently the system. A Trojan horse is a malware which deceives users, hiding harmful code in seemingly harmless and useful programs. Unlike worms and computer viruses, Trojan horses generally do not attempt to replicate themselves [6].

Traditional antivirus relies on signature-based detection methods to identify malwares. A proper signature of the malware file (previously analysed and identified as such) is generated and added to a signature database, which is used to detect suspicious files, matching the signatures [6][3].

In behaviour-based detection, suspicious and unauthorized activities from a running code are monitored, blocking the execution and/or vulnerable resources and alerting the user. This detection method is more effective against worms and Trojan horses. Sandbox detection is a behaviour-based detection technique that executes the suspicious code in a virtual environment, logging and analysing the running actions to determine if the code is a malware [6].

6.3.2 Audit and Monitoring

Most commercial security information and event management (SIEM) solutions provide a combination of types intrusion detection and prevention technologies, with a central management host to receive the reports from the various monitors and alert the network support staff. This section presents these technologies, used to audit and monitor enterprise networks.

Intrusion Detection and Prevention Systems (IDPS)

In cybersecurity, intrusion protection is the process of monitoring events occurring in a computer system or network and analysing them, looking for signs of possible incidents on both software and hardware [19].

These incidents are violations or imminent threats of violation of defined system security policies. Their cause can be varied, for instance, incidents may be caused by unauthorised access to the system via the internet, authorized users tricking the system to gain privileges, or even by malicious software. Incidents can also occur by chance and without intent, for example, a person might mistype the IP address of a computer and accidentally attempt to access a different system without authorization.

Intrusion Detection System (IDS) is a software that monitors and analyses events and resources in a computer system or network, with the purpose of uncovering signs of intrusions (incidents) and to alert appropriate personnel. Intrusion Protection Systems (IPS) maintain all capabilities IDS have, but in addition they are able take actions to prevent or stop detected intrusions [20].

IPDS systems are, in some ways, similar to firewalls, in that they both can prevent intrusions by blocking network communications. However, the difference is that, in the network, firewalls look outwardly for intrusions while IPDS look for anomalies within it, being also able to identify attacks that originate from inside the system.

Most IDPS technologies use multiple detection methodologies, either separately or integrated, to provide a broader and more accurate detection. The primary methodologies IDPS use to detect malicious events are classified in 3 major categories [19][20]:

- Signature-Based Detection: attempts to detect incidents by comparing known threats, recognizable by patterns or “signatures”, against observed events. Signature-based detection is very effective at detecting known threats but fairly useless at detecting previously unknown threats or even just slightly modified signatures.
  Signature-based detection cannot track and understand the state of complex communications, so it cannot detect most attacks that comprise multiple events.
  To achieve the best possible performance, signature-based detection requires constant updates to the known threats signature repository.

- Anomaly-Based Detection: is the process of detecting significant deviations in known behaviour. Profiles are derived from monitoring regular activities, network connections,

hosts or users over a period of time. It can be configured to monitor many behaviour attributes, such as processor usage, number of failed login attempts, or number of emails sent.

Profiles can be either static or dynamic. Static profiles remain unchanged after definition, unless the IPDS is specifically directed to generate a new profile. Dynamic profiles adapt constantly to the monitored conditions. As network and system conditions change over time, static profiles will eventually become obsolete. On the other hand, dynamic profiles are susceptible to evasion attempts from attacks, for instance, an attacker can start with a very small amount of malicious activity and then slowly increase it.

Anomaly-based detection is very good at detecting previously unknown threats. However, it often generates a large number of false positives and, due to the complexity of these events, it can be difficult to pinpoint the exact reason for the detected alert.

- Stateful Protocol Analysis Detection: identifies nonconformities in protocol states by comparing monitored events with predetermine profiles of generally accepted definitions of benign activities for each protocol state.

  While anomaly-based detection uses host or network specific profiles to detect threats, stateful protocol analysis relies on vendor-developed generic profiles that specify certain protocols. Stateful means that IDPS can understand the state of protocols, adjusting its analysis accordingly.

  Due to the complexity of the required analysis, this detection methodology can be very resource intensive. Additionally, stateful protocol analysis cannot detect certain attacks that only use benign protocols, for instance, when an attacker issues a very high number of small benign requests in a short period of time to cause a denial of service.

IDPS systems can be classified according to the type of information they monitor. The primary types of IPDS technologies are [19][20]:

- Network intrusion detection system (NIDS): monitors network traffic and analyses network and application protocol activity to detect suspicious events;
- Wireless intrusion detection system (WIDS): monitors wireless network traffic and analyses wireless networking protocols to detect suspicious events. It cannot monitor events in the application or higher layers (e.g., TCP, UDP) of the wireless network traffic;

- Network behaviour analysis (NBA): examines network traffic to recognize attacks with unusual traffic flows;
- Host-based intrusion detection system (HIDS): analyses each host separately, monitoring their characteristics and network events, looking for suspicious activities.

Although there are many types of IDPS, grouped by the type of information monitored, there are a set of functionalities that all types of IDPS technologies have:

- All generated information is recorded locally and/or sent to centralized logging servers, enterprise management systems and security information and event management (SIEM) solutions;
- Notifications are sent to security administrators regarding important events;
- Reports are generated to summarize and/or provide details to registered events.

Logging Tools

Nowadays, almost every computer software within an organization stores important information regarding their life cycle. Most of them use logs to do so. Some examples include, operating systems and host software programs, antivirus software, firewalls and intrusion detection and prevention systems. All stored information can have an extremely wide variety of sources and formats, related or not to cybersecurity. As logs can contain sensitive information, such as user information and habits, confidential data or security management, it is extremely important to protect them.

Log Management tools help the process of generating, transmitting, storing, analysing and disposing of log data [21]. A successful log management allows for efficient and effective log analysis, letting system administrators extract relevant data regarding organization policies, security and productivity. Security logs are also instrumental in building detailed event reports and to ensure event accountability.

Some examples of technologies / tools / frameworks related to intrusion detection and prevention systems and logging tools:

- Snort: http://static.usenix.org/publications/library/proceedings/lisa99/full_papers/roesch/roesch.pdf
- Juniper:

http://www.juniper.net/us/en/products-services/what-is/ids-ips/

- Cisco Firepower Next-Generation IPS (NGIPS): http://www.cisco.com/c/en/us/products/security/ngips/index.html
- Forcepoint Stonesoft NGFW https://www.forcepoint.com/product/network-security/forcepoint-ngfw
- Suricata IDS https://suricata-ids.org/
- The Bro Network Security Monitor: https://www.bro.org/
- SolarWinds Security Information and Event Management (SIEM) Log & Event Manager: http://www.solarwinds.com/pt/siem-security-information-event-management-software
- Graylog https://www.graylog.org/
- ArcSight Enterprise Security Manager (ESM): https://saas.hpe.com/en-us/software/siem-security-information-event-management
- IBM Security QRadar SIEM: http://www-03.ibm.com/software/products/no/qradar-siem
- LogRhythm Security Intelligence Platform: https://logrhythm.com/products/security-intelligence-platform/
- RSA Security Analytics: https://www.rsa.com/content/dam/rsa/PDF/h13414-ds-pdf-sa-overview.pdf
- McAfee Enterprise Security Manager: https://www.mcafee.com/us/products/enterprise-security-manager.aspx
- Splunk Enterprise: https://www.splunk.com/en_us/products/splunk-enterprise.html
- AlienVault OSSIM: https://www.alienvault.com/products/ossim
- Datadog Cloud Monitoring: https://www.datadoghq.com/
- Logpoint: https://www.logpoint.com/en/

6.3.3 Physical Access

Breaches in physical-layer security can be extremely detrimental to an organization's computer systems or network, including its cybersecurity [22]. For instance, by gaining physical access to a component in the network using an unmonitored ethernet port, an attacker can be able to see the entire system. Other example is when an attacker gains access to the power distribution grid and tampers with the system in some way.

Wireless communications, such as GSM, radio or Wifi can also be considered as a possible points of failure in the physical layer [23]. Radio jamming can block communications between vital system or network components. Wireless spoofing can compromise system integrity and data confidentiality.

Some attacks in the system's physical layer are impossible to stop and some are even very hard to mitigate. Cybersecurity policies and configurations need to take this into account. Despite possible failures in the physical access or hardware levels, the software should be prepared for these situations, implementing the necessary countermeasures to prevent compromising user information, data confidentially and system's integrity and availability.

Some examples of technologies / tools / frameworks related:

- Movement Detection
- Door Sensors
- Cameras
- Network Port physical tracking

6.4 MANAGEMENT

Proper resource management is critical for system and network security. It must properly devise and deploy policies that implement organizational and management requirements. Different management scenarios such as security appliances (firewalls, routers, etc.), network infrastructure, user computers, and servers, require different approaches to dealing with the problems, which often are amplified in large-scale environments [24].

6.4.1 Network Management

Configuration management allows the control and management of computer networks. Involves collecting information about devices and software, setting and verifying security settings, and includes fault management in order to support administration and troubleshooting [24].

Patch management allows managing patches and upgrades for software and related technologies. Involves installing software updates and fixes to add new functionalities or to repair system vulnerabilities, ensuring preventive security measures.

Policy management addresses the complexity and difficult learning curves associated with IT resources and the lack of entire network topology view across different subsets of the network, enabling the definition of business-driven security and Quality of Service (QoS) policies and providing a centralized network configuration. Multiple policy systems may be needed in larger networks with multiple domains to ensure proper control and inter-domain consistency. A more secure and easy to use network is the major benefit of policy management.

6.4.2 Policies

IETF's policy-based management architectural framework (defined in IETF RFC 2753 [25]) is used as the blueprint for policy management. The main functional components of the model include:

- Policy Decision Point (PDP): Also known as policy server (often stand-alone systems), translates policies and transfers them to the PEP using a control protocol, controlling all devices within an administrative domain [6].
- Policy Enforcement Point (PEP): Is a network or security device that accepts/enforces policies received from the PDP and applies on the network traffic passing through the PEP [6].
- Common Open Policy Service (COPS): Is a TCP-based protocol that specifies a simple client/server model, defined in IETF RFC 2748 [26], used to exchange policy information between a PDP and its client's PEPs [6].
- Policy Repository (PR): Hosted in a network directory database (without an established standard), is a data store for all policy information, describing relatively static network information such as users, applications, computers, services and the relationships between these elements. PDPs store more dynamic network information and retrieves policy information from PR to deploy in network elements [6].

- Lightweight Directory Access Protocol (LDAP version 3 [27]): LDAP, is specified in IETF RFC 3377 [28], is a client-server protocol to access and maintain a distributed directory service, allowing information sharing throughout the network. The information model or the interface with directories is based on an entry (which information about some object) composed of a set of attributes, each with a name and one or more values.
- Policy Management Console (PMC): Is comprised of a Human Computer Interface and tools to access the policy management system PMC is used to define network policies, such as business rules, and to access lower-level security configurations. Can be implemented as a web application with access policies.

7. State of the art of currently used solutions

In this section, based on questionnaire sent to UIC members within the ARGUS project, we present some security methodologies and technologies currently used by railway infrastructure managers to protect their system. These solutions are divided in three main blocks: Networks Security, Signalling Security and Deployment Security.

7.1 Network Security

7.1.1 Technologies

- **VPN** – In most cases the network isolation between different services is made by using VPN over IP/MPLS.

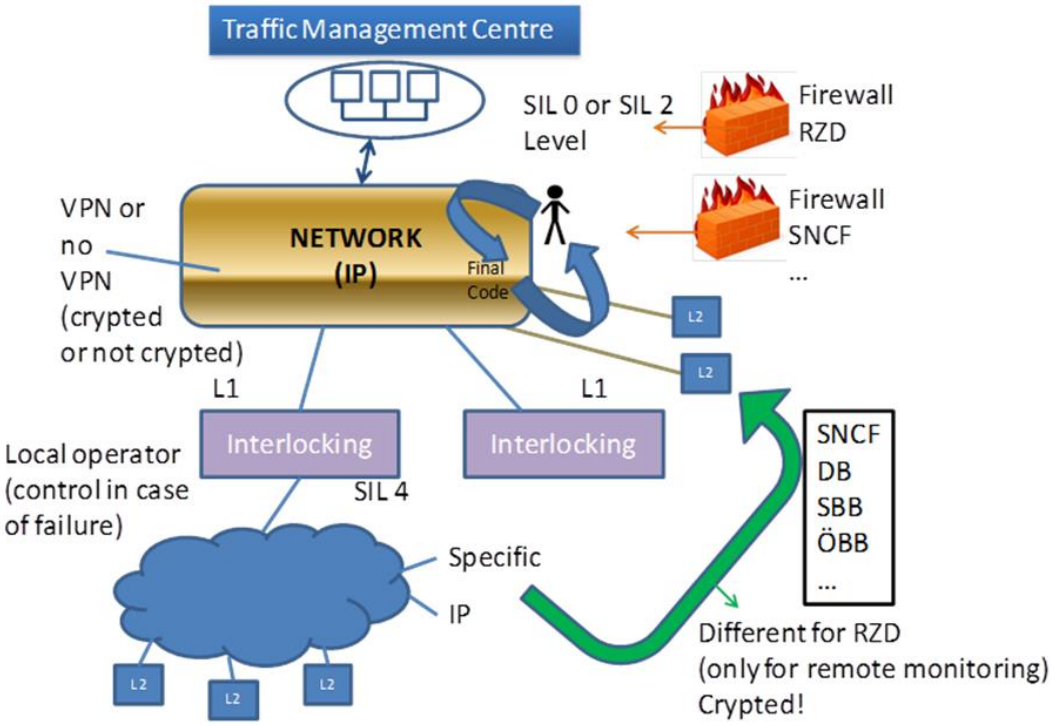

Figure 2 - Network Security "VPN"

This VPNs are usually treated as closed networks, thus according to EN 50159, no cryptography is used to protect the data exchanged through the network. However, this assumption is not valid, because although with VPN it is possible to make an abstraction of the network and limiting the access to VPN for certain services, the physical network equipment underneath must

be reachable from outside in order to allow VPNs with outside access. This means that, although a single VPN is unreachable directly, **if the underneath equipment is attacked and its routing tables are corrupted, the assumed VPN isolation would be avoided.**

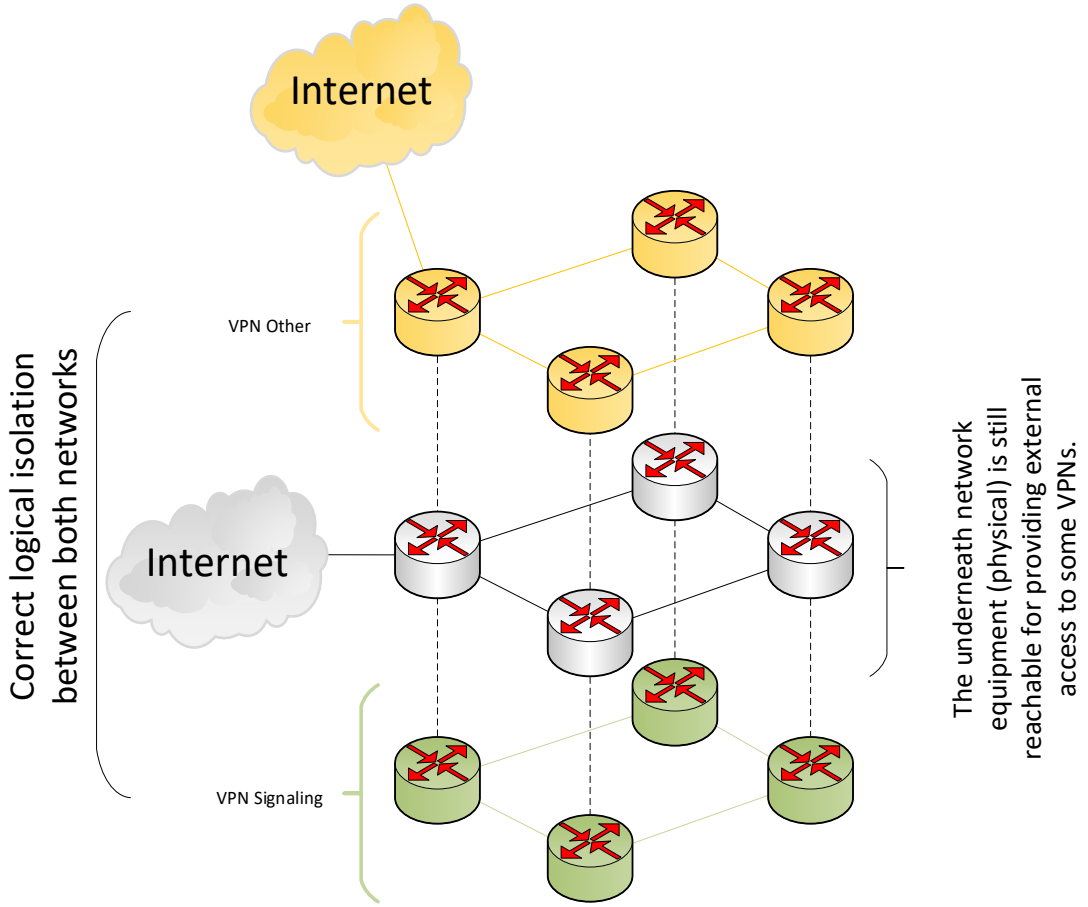

Figure 3 - Network segmentation scheme based on VPNs

In the Figure 3, this abstraction made by VPNs is illustrated. As can be seen, VPNs with and without Internet access using the same underneath physical network are provided. However, **if an attacker arrives to the physical router where the routing table for multiple VPNs is stored, this "virtual" isolation would be completely useless.** In conclusion, the security provided by VPNs belongs to the security of the physical equipment which is shared for different services. This means that these VPNs should not be treated as closed and therefore isolated networks from the rest of services.

- **WDM** – Wavelength-division multiplexing technology makes uses of different frequencies to create physically isolated networks over the same optical fibre. Until now this technology is not widely used in the railway domain for network isolation, but some countries ministers are encouraging to use it in close-future.

- **Cryptography** (PE26) – The norm EN 50159 established that if "open networks" are used in railway signalling, then cryptographic mechanism must be used for protecting it from potential intruders. As using open networks can seem a cost-effective way to carry railway signalling, using cryptography could seem a good idea. However, using cryptography has a negative impact in the signalling by itself. Due to the necessary time needed for doing cryptographic computation (typically 50ms for each operation – encrypt/decrypt), the use of cryptography could suppose an unacceptable delay penalization especially for L0 networks where response time must be less than 50ms. Furthermore, when crypto algorithms are used for securing the signalling communications, the life-cycle of the signalling elements must be considered, as well as the durability of the crypto algorithm's robustness. Although there are national recommendations with estimated dates for the validity of each algorithm, the IT security domain changes day-by-day and the publishing of new vulnerabilities of crypto algorithms cannot be assured.

- **Firewall** – Firewalls play a key role in different network isolation because they can drop specific traffic whereas other traffic is allowed. However, in many cases, firewalls also introduce delays and can't give the maximal guarantee in the time. Moreover, firewalls must be updated frequently (usually once the vulnerability/attack has detected). As alternative with low delay and more efficient, **Data Diodes** are introduced in industrial control systems.

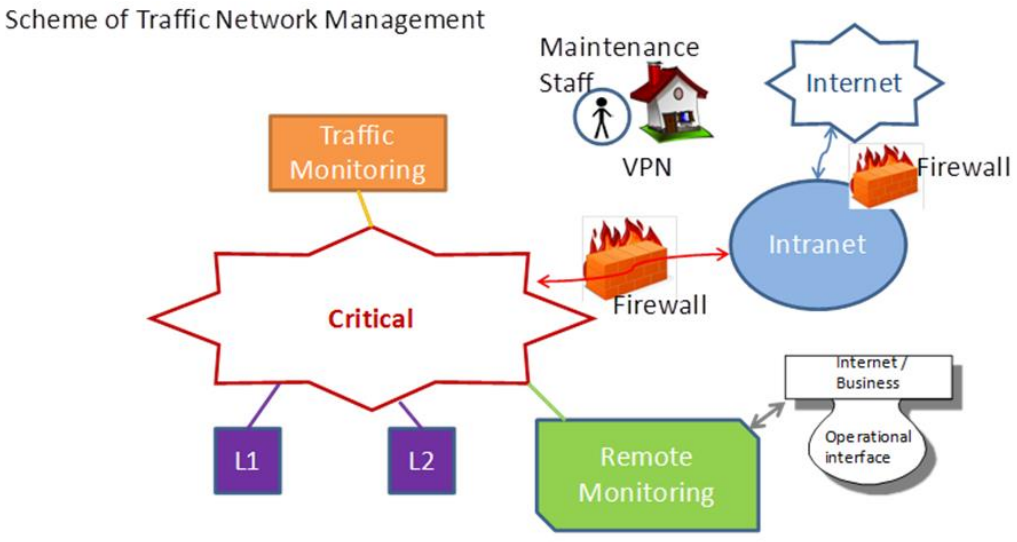

Figure 4 - Typical railways network model

- **DMZ** – A **Demilitarized Zone** is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, such as the Internet. The aim of DMZ is to provide an additional security layer by defining a limited and controlled zone where outsiders can access. The traffic between internal network and a DMZ is usually unidirectional. This means that equipment in the DMZ can receive information from internal network, but cannot access to the internal network and, at the same time, an user from Internet can access the DMZ to consult this information. This security element plays a key role for providing monitoring functionalities while the network isolation is kept.

- **IDS/IDP** – Intrusion Detection Systems and Intrusion Prevention System are used to detect intruders in the network and react to suspicious activities. These systems include sensors that analyse the network traffic along the network and detect suspicious traffic patterns. In case a suspicious activity is detected it can send an alarm to the control centre and/or reset the firewall to react to the "attack". It is worth noting that these security "risky" patterns come from previous detect attacks. However, a correct and non-malicious network activity can have similar network behaviours and consequently be detected by the IDS/IDP as an attack, generating what it is known as a false-positive.

7.1.2 Processes

- **Network segmentation:** The correct segmentation of the network should achieve the role of isolating different services and prevent "traffic leak" from one to another. This segmentation should also be made considering the survivability of the network, that is, if a service of the network is under attack, the rest of the network should have the capacity to keep working normally. This segmentation can be achieved in different ways. Note that the use of one approach for segmentation does not exclude the use of another approach, they are complementary:
    - Geographically: **By regions**.
    - **By services** and connection levels of signalling elements:
        - Monitoring service isolated from signalling service.
        - L1-L2: Network connecting Interlocking with filed elements.
        - L0-L1: Network connecting Interlockings with the Control Centre.

        - L1-L1: Connection between interlocking and between RBCs.
    - **Physically independent networks**: Each network can be physically independent while using the same O.F. as carrier. With WDM each service/network can use different wavelength and different network equipment, mitigation the risk of traffic leak from one network to another.
- **Redundancy (network and elements):** The signalling network, due to its safety needs, must be resilient. Therefore, redundancy of its equipment and network must be guaranteed. The more heterogeneous redundant networks are, the more probabilistically disjoint they will be; therefore, the resilience will be higher. For instance, a combination of fixed networks, radio networks and radiating cables (like in Euroloop). Another option could be the deployment of a fall-back wireless network that would only be activated when the main wireless network is unavailable. This proposal could use Software Defined Radio (SDR) technology for checking free spectrum band to be used, and self-configuring network protocols. This way, an attacker would never know in advance which frequency would be used for a fall-back network, so it could not attack it.
- **Security**: The security must be considered during the design of the signalling system's architecture.
    - Intrusion tests: Internal and external. With government or outsourced companies.
    - Contingency plans: Contingency plans in case of cyber-attacks must be defined and people and network should be ready to face it at any moment.
- Security standards adoption: Railway signalling is an industrial process that has associated multiple international and national norms that are mandatory to fulfil security needs.

7.1.3 People

- **Clear and mandatory policies are defined for the personnel** (from inside or outside) that will work in the operation or maintenance of the elements during their life cycle.
- **Only authorized personnel can access to network or signalling elements**.

7.2 SIGNALLING SECURITY

We define functional security all the security aspect that implies the operational mode of signal element. To clarify the term, we can use the following example: Let's say we have a train operating a route and this train receives orders via radio link. If a hacker can introduce bad commands to the train due to security vulnerability should we assume this risk? From the telecommunication security there is nothing we can do against it. However, from functional security, it would be possible to compare received commands to a set of route-maps associated with a normal performance of the network and detect the introduction of malicious commands.

7.2.1 Functional analysis

- **Real-time functional monitoring system:** The possible valid behaviour for each Interlocking is defined with a functional language and the Interlocking check each received command if its meets the pre-defined behaviours or not.
- Double check of received commands by onboard units. The double check of a command is not a valid safety method. It must be used as a part of ty approach or a safe comparator.
- **NIDS/HIDS** that checks the signalling traffic **from a functional point of view** and alert from unusual traffic patterns.

7.2.2 Continuity of the system

The continuity of the system is based on policies, guides standards and procedures to assure all business-critical processes and services will be available for clients, suppliers and related entities. Therefore, it involves all techniques and methodologies used for guaranteeing the continuity of the service in adverse conditions, such as intrusion tests and cooperation with cyber security experts:

- Intrusion tests: the principle is to simulate authorized attacks on the system that looks for security weaknesses. This intrusion test could be organised internally or externally with cyber security experts and can help determine whether the system is vulnerable to attack, if the defences were sufficient, and which defences (if any) the test defeated.

- Collaboration with national Community Emergency Response Teams (CERT to train staff to be better prepared to respond to emergency situations and to improve coordination with other agencies for managing of incidents, accidents or disasters.

The complete continuity of the system is the philosophy or methodology to develop the business activity, so necessary components for developing a continuity plan must include aspects such as security management, document management, change management, communications systems and others.

7.3 DEPLOYMENT SECURITY

Below some recommended methodology for adding new elements to the network:

- **Software is analysed for virus and tested** before using it for updating equipment's systems.
- **New hardware elements are tested in isolated spaces** to detect failures in their behaviour.
- No software or hardware is acquired if the full specification of the equipment and its source code is provided. **White box policy**.

7.4 OTHER RAILWAY RELATED SOLUTIONS

Below some railway related solutions found in the market are listed:

- Parsons
  - https://www.parsons.com/services/Pages/cybersecurity.aspx
  - https://www.parsons.com/Media%20Library/ICS-SCADA_CYBERSECURITY.pdf
  - https://www.parsons.com/Media%20Library/Cybersecurity-Transportation.pdf
- Thales
  - https://www.thalesgroup.com/sites/default/files/asset/document/cyber_security_0.pdf
  - https://events.thalesgroup.com/innotrans/en/article/769912/Rail-digitalisation-cybersecurity
  - http://www.ertms-conference2016.com/IMG/pdf/1.5_ertms_wc_cyber_security_final.pdf
  - https://www.thalesgroup.com/sites/default/files/asset/document/overview_lowres.pdf
- RAILNOVA
  - https://www.railnova.eu/
- Rail Radio Intrusion Detection System (RRIDS) [29]
  - Detection and dissuasion of cyber-attacks such as: command replay, guessing, and message corruption attacks
- WeOS - Westermo Operating System
  - Implement security procedures in communications between network devices with this operating system

8. RELATIONSHIP BETWEEN FOUNDATIONAL REQUIREMENTS AND CYBERSECURITY TECHNOLOGIES

In the chapter 5, the foundational requirements are briefly described in terms of the different groups. The chapter next to it, captures a non-exhaustive list of potential IT technologies and means to support and enhance cybersecurity levels.

This chapter intends to map the foundational requirements to the technologies presented at chapter 6. The relationship between Foundational Requirements and cybersecurity technologies are presented. The overall foundational requirements are:

- Identification and Authentication Control (IAC);
- Use Control (UC);
- System Integrity (SI);
- Data Confidentiality (DC);
- Restricted Data Flow (RDF);
- Timely Response to Events (TRE);
- Resource Availability (RA);

Table 3 - Relationship between Foundational Requirements and cybersecurity technologies

Technology	Foundational Requirements						
	IAC	UC	SI	DC	RDF	TRE	RA
Access Control							
Authentication	✓	✓		✓			
Content Filtering and Management		✓		✓	✓		
Firewall			✓	✓	✓	✓	✓
Network Address Translation (NAT)				✓	✓		✓
Application Level Gateway				✓	✓		
Application Proxy				✓	✓		
Demilitarized Zones				✓	✓		✓
Wavelength-Division Multiplexing				✓	✓		✓
Virtual Private Network (VPN)				✓	✓		✓
Cryptography							
Encryption				✓	✓		
Key Exchange	✓	✓		✓			
Digital Signatures	✓	✓		✓			
System Integrity							
Antivirus			✓			✓	✓
Intrusion Detection			✓			✓	✓
Intrusion Prevention			✓			✓	✓
Logging Tools	✓	✓	✓		✓	✓	✓

Technology	Foundational Requirements						
	IAC	UC	SI	DC	RDF	TRE	RA
Physical Access			✓			✓	✓
Management							
Network Management		✓	✓	✓	✓		✓
Policies	✓	✓	✓	✓	✓	✓	✓

9. RELATED NORMATIVE

This chapter captures some safety and security normative elements for railway signalling and cybersecurity.

9.1 CYBERSECURITY STANDARDS

This section captures some relevant cybersecurity standards that should be considered and tailored with respect to the safety and security requirements for rail transport systems in multi-stakeholder environments:

- Engineering Cybersecurity Control Framework (e.g. IEC 62433-3-3, IEC 62433-2-1)
- Standards Implementation Guidelines (e.g. NIST 800-82 r2, ISO 27002)
- Reference Architectures and Best Practices (e.g. NIST 800-82 r2)
- Risk Assessment Process (e.g. IEC 62433-3-2, IEC 62433-3-1, NIST 8003-30)
- IT security (e.g. ISO 15408, ISO 27001/2)
- Software Safety for Railway Systems (e.g. IEC 61508, IEC 62279)

9.2 SIGNALLING RELATED NORMATIVE

The following normative is related to Railways (communications, signalling, processing systems, industrial automation and information technologies), with connection with this project.

- DIN V VDE V 0831-101: Semi-quantitative processes for risk analysis of technical functions in railway signalling (in German).
- EN 50126: Railway Applications - The Specification and Demonstration of Reliability, Availability, maintainability and Safety (RAMS).
- EN 50128: Railway Applications - Communications, signalling and processing systems.
- EN 50129: Railway Applications - Communications, signalling and processing systems. Safety related electronic systems for signalling.
- EN 50159: Railway applications. Communication, signalling and processing systems. Safety-related communication in transmission systems.
- APTA-SS-CCS-RP-002-13: Defining a Security Zone Architecture for Rail Transit and protecting Critical Zones.
- STO RZD 02.049-2014: Automated Control Systems of Operating processes and Railway Technical Facilities.

9.3 NOT SIGNALLING RELATED NORMATIVE

- IEC-62443: Security for Industrial Automation and Control Systems.
- ISO/IEC 27000-series: comprises information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).
- ISO/IEC 27002:2013: Information technology - Security techniques - Code of practice for information security controls.
- ISO/IEC 27005:2011: Information technology - Security techniques - Information security risk management.
- Classification Method and Key Measures: Cybersecurity for Industrial Control Systems. ANSSI.
- Detailed Measures. Cybersecurity for Industrial Control Systems. ANSSI.

10. CONCLUSION

As a conclusion, we can state that there is no specific technology available for the Railway environment to ensure the Cybersecurity of System and Data, particularly on signalling system. In spite of this, the railways has been adopting IT solutions, processes and best practices to ensure the security of the system and operation of the business. While the railway network is a closed network, with several separation layers, these are expected to work as intended, but connecting all systems, including signalling to a common network, will for sure raise new challenges and threats.

11. REFERENCES

[1] ISA, "ISA-62443-1-1 - Models and Concepts," in *ISA-62443 - Security for Industrial Automation and Control Systems*, vol. D6E2, no. September, 2016, pp. 3–115.

[2] Environmental Protection Agency, "Information Security - Identification and Authentication Procedure," 2016.

[3] R. Havighurst, "User Identification and Authentication Concepts," 2007.

[4] U.S. General Accounting Office, "Cybersecurity for Critical Infrastructure Protection," Washington, D.C, 2004.

[5] M. Bartock, J. Cichonski, M. Souppaya, M. Smith, G. Witte, and K. Scarfone, "Guide for cybersecurity event recovery," Gaithersburg, MD, Dec. 2016.

[6] International Telecommunication Union (ITU), "Overview of cybersecurity," *Series X: Data Networks, Open System Communications and Security - Telecommunication Security*, vol. X.1205, pp. 1–64, 2008.

[7] Microsoft, "TCP/IP Protocol Architecture," 2000. [Online]. Available: https://technet.microsoft.com/en-us/library/cc958821.aspx.

[8] IPv6.com, "ALG - Application Level Gateway," 2006. [Online]. Available: https://www.ipv6.com/gateways/alg-application-level-gateway/.

[9] McAfee Labs, "McAfee Labs Threats Report," 2017.

[10] J. Haggerty, Qi Shi, and M. Merabti, "Beyond the perimeter: the need for early detection of denial of service attacks," in *18th Annual Computer Security Applications Conference, 2002. Proceedings.*, 2002, pp. 413–422.

[11] P. Srisuresh and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations," Aug. 1999.

[12] Cisco, "Network Address Translation (NAT) FAQ," 2014.

[13] SAFE-T, "Paving the path to the next generation DMZ perimeter - A RSAccess White Paper."

[14] M. Życzkowski, M. Szustakowski, W. Ciurapiński, P. Markowski, M. Karol, and M. Kowalski, "Optical fiber sensors as the primary element in the protection of critical infrastructure especially in optoelectronic transmission lines," 2013, vol. 134, pp. 273–

283.

[15] J. Thakur and N. Kumar, “DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis,” *Int. J. Emerg. Technol. Adv. Eng.*, vol. 1, no. 2, 2011.

[16] Microsoft, “Secret Key Exchange,” *Basic Components of Modern Cryptography*, 2017. [Online]. Available: https://technet.microsoft.com/en-us/library/cc962035.aspx.

[17] Microsoft, “Digital signatures and certificates,” 2016. [Online]. Available: https://support.office.com/en-us/article/Digital-signatures-and-certificates-8186cd15-e7ac-4a16-8597-22bd163e8e96.

[18] George Mathew Koikara, Pruthvi Panyam Nataraj, Ravi Shankar, and Saurabh Desai, “Verify System Integrity,” *IBM Systems Magazine*, 2009. [Online]. Available: http://ibmsystemsmag.com/aix/administrator/security/verify-system-integrity/.

[19] K. A. Scarfone and P. M. Mell, “Guide to Intrusion Detection and Prevention Systems (IDPS),” Gaithersburg, MD, 2007.

[20] H. Liao, C.-H. Richard Lin, Y. Lin, and K. Tung, “Intrusion detection system: A comprehensive review,” *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 16–24, Jan. 2013.

[21] K. Kent and M. P. Souppaya, “Guide to computer security log management,” Gaithersburg, MD, 2006.

[22] Chris Meenan, “How Physical Security Defenses Influence Cybersecurity,” *SecurityIntelligence*, 2015. [Online]. Available: https://securityintelligence.com/how-physical-security-defenses-influence-cybersecurity/.

[23] K. Grover, A. Lim, and Q. Yang, “Jamming and anti-jamming techniques in wireless networks: a survey,” *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 17, no. 4, p. 197, 2014.

[24] S. Bellovin and R. Bush, “Configuration management and security,” *IEEE J. Sel. Areas Commun.*, vol. 27, no. 3, pp. 268–274, Apr. 2009.

[25] R. Yavatkar, D. Pendarakis, and R. Guerin, “A Framework for Policy-based Admission Control,” 2000.

[26] J. Boyle, R. Cohen, S. Herzog, R. Rajan, and A. Sastry, “The COPS (Common Open Policy Service) Protocol,” 2000.

[27] M. Wahl, T. Howes, and S. Kille, “Lightweight Directory Access Protocol (v3),” 1997.

[28] J. Hodges and R. Morgan, “Lightweight Directory Access Protocol (v3): Technical Specification,” 2002.

[29] A. Melaragno, K. R. D. S. Bandara, A. Fewell, and D. Wijesekera, “Rail Radio Intrusion Detection System (RRIDS) for Communication Based Train Control (CBTC),” in *2016 IEEE International Conference on Intelligent Rail Transportation (ICIRT)*, 2016, pp. 39–48.

12. ANNEX 1: SIGNALING ASSETS LOSS IMPACT

Asset	Third party access?	Description of the performed tasks	ERTMS subsystem (select from options or write a new one)	Relation with other ERTMS subsystems (include communication direction among them, e.g.full-duplex, interfaces, connections diagram and relevant information)	Impact of loss in relation to human context (1: no critical, 4: very critical)	Impact of loss in relation to financial context (1: no critical, 4: very critical)	Impact of loss in relation to operational context (1: no critical, 4: very critical)
Axel Counter (trackside equipment)	No	Detect train presence	Wayside equipment	Twisted pair with inside equipment	4	4	4
Track circuit	No	Detect train presence	Wayside equipment	Quad cable to inside equipmente	4	4	4
Signal (ERTMS level 1 and 0)	No	Send information to train driver	Wayside equipment	Quad cable to interlocking	2	2	3
Point Machine	No	Stablish train route	Wayside equipment	Quad cable to interlocking	4	4	4
Controlled Balise (ERTMS level 1 and 0)	No	Send variable information to train (signals information, temporary sped limits...)	Wayside equipment	Twisted pair to LEU	4	4	4
Non-controled Balise	No	Send fix information to train (permanent speed restriction, slope, next balise group, etc...)	Wayside equipment		4	4	4
BTS	No	Send radio information to ERTMS onboard equipment (movement authorisation, etc.)	GSM-R Transmission network	S2M to RBC	1	3	4/2 (with backup system)
RBC	No	Information exchange between train and interlocking. Stablish movement authorization.	RBC	S2M to RBC / IP network with Interlocking (vpn, dark optical fiber ...)	1	3	4/2 (with backup system)
Local ERTMS control	No	Send commands to RBC	Local Control Center	IP network (signalling private network)	1	3	4/2 (with backup system)
Local Maintenance Aid System ERTMS	Yes (maintainer)	Check failures on RBC and review historic	Local control Center	IP network (signalling private network)	1	2	2
Juridical recorder	No	Keep record of system events	Local Control Center	IP network (signalling private network)	1	2	1
Temporary Speed restriction Mgr	No	Set temporary speed restrictions for the system	Local Control Center	IP network (signalling private network)	3	3	4
Key Mgmnt Center	No	Cryptographic keys management for GSM-R transmission	KMC	IP network (signalling private network)	4	4	4

Asset	Third party access?	Description of the performed tasks	ERTMS subsystem (select from options or write a new one)	Relation with other ERTMS subsystems (include communication direction among them, e.g.full-duplex, interfaces, connections diagram and relevant information)	Impact of loss in relation to human context (1: no critical, 4: very critical)	Impact of loss in relation to financial context (1: no critical, 4: very critical)	Impact of loss in relation to operational context (1: no critical, 4: very critical)
Interlocking	No	Wayside equipment control. Generating Movement Authority	Interlocking	IP network (signalling private network)	1 (loss of interlocking means all train stopped) SIL4 system 4 if system is hacked	4	4
Interface control equipment ERTMS	No	Gateway between signaling Network & High availabilty network	Interface	IP network (signalling private network/high availability network)	1	3	4/2 (with backup system)
Communications Front-end	No	Interface between High availability network and Real-time operation network	Interface	IP network (high availability network/real-time operation network)	1	3	4/2 (with backup system)
Centralized Maintenance Aid system ERTMS	Yes (maintainer)	Allow remote access to local MAS	Control Centre	IP network (real-time operation network)	1	1	2
Data server ERTMS	No	Data management for ERTMS remote command on control center	Control Centre	IP network (real-time operation network)	1	3	3
Graphics interface server ERTMS	No	Generate graphics for Videowalll or projection systems	Control Centre	IP network (real-time operation network)	1	1	1
External interface system ERTMS	Yes	Allow connection from external elements to ERTMS system such as staff protection system	Control Centre	IP network (real-time operation network / message oriented middleware)	1	1	1
Operation and Management workstation	No	Allow centralized management of railway operation	Control Centre	Ip network (real-time operation network)	1	3	4
On-board ERTMS equipment	No	Receive information from Eurobalises/Euroloop, show information to driver, establish speed profile based on train and information received from balises and GSM-R. Brake or stop train if speed limits are overridden.	On-board system	Usually commercial module (Siemens, Alstom, CAF, Bombardier, Thales ...) choosen by train manufacturer interfacing with train	1 (loss of ERTMS onboard means train not allowed to move unless under SR or with backup system if available) 4 if system is hacked	3	3