



CYbersecurity in the RAILway sector

CYRail Recommendations on cybersecurity of rail signalling and communication systems

September 2018



Horizon 2020
European Union Funding
for Research & Innovation



Publication: UIC-ETF
Design: Ludovic Wattignies
Legal deposit: September 2018
ISBN: 978-2-7461-2747-0

This work has been carried out as part of the CYRail project (www.cyrail.eu). This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement No 730843 addressing the topic "**Threat detection and profile protection definition for cybersecurity assessment**".

No part of this document may be copied, reproduced, disclosed or distributed by any means whatsoever, including electronic without the express permission of EVOLEO, Coordinator of the EU CYRail Project. The same applies for translation, adaptation or transformation, arrangement or reproduction by any method or procedure whatsoever.

TABLE OF CONTENTS

DEFINITIONS.....	5
ACRONYMS	7
SUMMARY OF CYRAIL PROJECT	9
1. INTRODUCTION.....	11
2. RAIL CONTEXT	13
3. CYRAIL RAIL SCENARIO	15
4. SECURITY ASSESSMENT	17
CYRAIL METHODOLOGY	17
4.1. Introduction.....	17
4.2. Security assessment methodology	18
4.2.1. Identify the System under Consideration (SuC)	19
4.2.2. Performing a high-level cybersecurity risk assessment (HLCRA)	19
4.2.3. Partition of the SuC into zones and conduits and definition of the vulnerabilities of each zone and conduit.	21
4.2.4. Detailed cybersecurity risk assessment	22
4.2.5. Documentation of the process	31
5. DETECTION: EARLY ATTACK AND ANOMALY DETECTION.....	33
5.1. What is an intrusion detection system (IDS)?.....	33
5.2. IDS Process: Three stages	34
5.3. Basic Architecture of an IDS	34
5.4. Main requirements of an IDS.....	35
5.5. The two main classes of IDSs: HIDS AND NIDS.....	35
5.6. Detection methodologies: signature-based, anomaly-based and hybrid.....	36
5.7. IDS Protocol support: IT, OT, IT ADAPTED TO OT.....	36
5.8. Market status quo for IDS-Based Solutions	37
5.9. Evaluation of IDS Solutions	37
6. PREVENTION: RISK MITIGATION AND COUNTERMEASURES SPECIFICATION.....	39
6.1. Five Key mitigation strategies.....	39
6.2. Human Factor	41
6.3. Advanced Mitigation Strategies.....	41
6.3.1. Security by design.....	41
6.3.2. Multiple Independent Layers of Security (MILS)	43

7. INTERVENTION/RESPONSE: ENHANCED ALERTING AND COLLABORATIVE INCIDENT MANAGEMENT	45
7.1. Introduction	45
7.2. State of the art	45
7.2.1. Human Factor and organisation practices	45
7.2.2. Technical solutions	49
7.2.3. Synthesis.....	52
7.3. CYRail recommended system.....	54
7.3.1. Introduction	54
7.3.2. Detection strategy.....	54
7.3.3. System requirements.....	56
8. RESILIENCE: CYBER RESILIENCE MECHANISM.....	63
8.1. Objectives	63
8.1.1. Anticipate.....	63
8.1.2. Withstand.....	63
8.1.3. Recover	64
8.1.4. Evolve	64
8.2. Principles	64
8.2.1. Strategic Design Principles.....	64
8.2.2. Structural Design Principles	65
8.3. Techniques	66
8.3.1. Adaptive Response	66
8.3.2. Analytic Monitoring.....	66
8.3.3. Coordinated Defence.....	66
8.3.4. Deception.....	66
8.3.5. Diversity	66
8.3.6. Dynamic Positioning.....	66
8.3.7. Dynamic Representation	66
8.3.8. Non-Persistence.....	66
8.3.9. Privilege Restriction.....	66
8.3.10. Realignment.....	67
8.3.11. Redundancy	67
8.3.12. Segmentation / Isolation	67
8.3.13. Substantiated Integrity	67
8.3.14. Unpredictability	67
9. SECURITY REQUIREMENTS: PROTECTION PROFILE	69

DEFINITIONS

Access Control – The process of granting or denying specific requests to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., federal buildings, military establishments, border crossing entrances).

Anomaly - An anomaly is a term describing the incidence when the actual result under a given set of assumptions is different from the expected result.

Asset – A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.

Attack - An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity.

Countermeasure – Action, device, procedure, or technique that reduces a threat, a vulnerability, or the consequences of an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

Cyber resiliency – The ability to anticipate, withstand, recover from and adapt to adverse conditions, stresses, attacks or compromises on cyber resources.

Encryption - Conversion of plaintext to ciphertext through the use of a cryptographic algorithm.

False Negative - An instance in which an intrusion detection and prevention technology fails to identify malicious activity as being such.

False Positive - An instance in which an intrusion detection and prevention technology incorrectly identifies benign activity as being malicious.

Intrusion - Unauthorized act of bypassing the security mechanisms of a system.

Intrusion Detection System - Hardware or software product that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from within the organizations).

Intrusion Prevention System - System(s) which can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.

Intrusion Detection and Prevention System - Software that automates the process of monitoring the events occurring in a computer system or network and analysing them for signs of possible incidents and attempting to stop detected possible incidents.

Malicious - Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose.

Resilience – The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents

Risk - a combination of the likelihood of a threat of exploiting an existing vulnerability, and the resulting impact of that unwanted situation.

Residual risk – The risk that remains after countermeasures are taken into account.

Tolerable risk – Level of risk deemed tolerable to an organization in order that same particular benefit or functionality can be obtained.

Unmitigated cybersecurity risk – Level of cybersecurity risk that is present in a system before any cybersecurity countermeasures are considered.

Risk Mitigation - Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.

Signature - A recognizable, distinguishing pattern associated with an attack, such as a binary string in a virus or a particular set of keystrokes used to gain unauthorized access to a system

Threat – any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image or reputation), organizational assets, IACS (Industrial Automation and Control System), or individuals who contrary to security policy, intentionally or unintentionally prevent access to data or cause the destruction, disclosure, or modification of data.

Threat source - either an intended exploitation of a vulnerability or an unintended situation that may accidentally exploit a vulnerability.

Vulnerability - weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

ACRONYMS

Table 1. Acronym Description

Acronym	Description
API	Application Programming Interface
ASM	Automation Systems Manager
AV	Anti-Virus
BTS	Base Transceiver Stations
CC	Common Criteria
CERT	Computer Emergency Response Team
CIS	Collaborative and Information Sharing solutions
CMC	Central Management Console
CMDB	Configuration Management Database
CSIRT	Cyber Security Incident Response Team
CTI	Cyber Threat Intelligence
DPI	Deep Package Inspection
DMI	driver-machine interface
DMZ	Demilitarized Zone
DRAR	Detailed Risks Assessment Requirements
ENISA	European Network and Information Security Agency
ERTMS	European Rail Traffic Management System
GDPR	General Data Protection Regulation
GUI	Graphical User Interface
HIDS	Host-based Intrusion Detection System
HLCRA	High-Level Cybersecurity Risk Assessment
IAC(S)	Identification and Authentication Control(s)
ICS	Industrial Control System
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IMS	Incident Management System
IOC	Indicator Of Compromise
IPS	Intrusion Prevention System
IRSE	Institution of Railway Signal Engineers
ISO	International Organization for Standardization
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MAS	Maintenance Aid System

Acronym	Description
MILS	Multiple Independent Layers of Security
NAC	Network Access Control
NCSC	National Computer Security Centre
NIDES	Next-generation Intrusion Detection Expert System
NIDS	Network-based Intrusion Detection System
NIS	Network and Information Security
OCC	Operation Control Centre
OS	Operating System
OSINT	Open Source Intelligence
OT	Operational Technology
P-BEST	Production-Based Expert System Toolset
PDIS	Security Incident Detection Operator
PP	Protection Profile
RBC	Radio Block Centre
RM	Risk Management
RSVM	Robust Support Vector Machine
SCADA	Supervisory Control And Data Acquisition
SIEM	Security Information and Event Management
SIRP	Security Incident Response Platform
SOC	Security Operation Centre
SL	Security Level
SSH	Secure Shell
SSO	Single Sign On
SuC	System under Consideration
TIP	Threat Intelligence Platform
TOE	Target Of Evaluation
TVRA	Threat Vulnerability and Risk Analysis
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
ZCR	Zones and Conduits Requirements

SUMMARY OF CYRAIL PROJECT

Railway infrastructures are moving towards more intelligent, connected, user-centric and collaborative systems. While this evolution brings many advantages for the industry and users, it also poses new opportunities for cyber-criminals and terrorists.

CYRail aims to deliver tailored specifications and recommendations for secure modern rail systems design and operation. The challenges are multiple: wide and distributed geographical display of rail systems limit the traditional cyber-protection and cyber-defence tools & practices; the heterogeneous nature of rail systems makes them vulnerable to blended attacks; the collaboration with other transportation infrastructures increases the number of points for attack; new passenger-centric services may expose rail systems to threats known in the IoT; last but not least, ICT supporting these trends are not necessarily trusted for critical applications.

CYRail addressed those challenges through a methodical diagnosis and specification process, enforced at each step of the cyber-security chain: operational context and scenarios were defined, followed by a security assessment of railway systems. An analysis of threats targeting those infrastructures was developed as well as the identification of innovative attack detection and alerting techniques. Adapted mitigation plans and countermeasures were defined, taking into account their potential impact on operations. Protection Profiles for railway control and signalling applications were delivered to ensure security by design of new rail infrastructures.

The CYRail consortium took advantage of developments in other industries (aeronautics, automotive and energy) and brought them into the railway sector, taking both similarities and specificities into account. The Consortium was comprised of a well-balanced group of 6 partners (EVOLIO, EUSKOIKER, FORTISS, UIC, AIRBUS and ATSEC) from 5 European countries (Portugal, Spain, Germany, France and Sweden) with complementary skills.

The project main targets are

- Rail manufacturers
- Rail Infrastructure managers
- Rail operators
- Standardization bodies

The following will give an outline on the lessons learnt during the CYRail Project.

1. INTRODUCTION

The main goal of this document is to provide rail infrastructure managers and public transport operators with recommendations issued from the CYRail project on the cybersecurity of **rail signalling and communication systems**.

First step in the project was to describe the rail context and prepare a **rail scenario** which was then addressed by the security analysis performed in CYRail. This is explained in the next two chapters (Chapter 2 and 3).

A key step in the proposed approach to cybersecurity is the assessment of the risks: what are the most critical assets and how to identify them? CYRail proposed a **methodology for assessing the risks**, adapted to the rail system environment, based on the IEC 62443 standard complemented with many concepts from ETSI TVRA. This methodology which has been applied to the rail scenario in order to be validated, is explained in Chapter 4. In order to enrich this risk analysis, a particular focus has been brought in CYRail on analysing past, current and future **threats** that can affect railway systems, including those arising from extended interconnection with external networks and applications, as described in Section 4.2.4.

The next challenge addressed in CYRail was to identify a set of tools and solutions for tackling the detection and response phases, tailored to the operational context of railway systems. In this regard, **early detection of intrusion, attack and anomaly** is a key element in the cybersecurity approach which is addressed in Chapter 5. Beside well-known solutions such as firewalls, encryption, Virtual Private Networks (VPNs), etc, CYRail described the characteristics of Intrusion Detection System (IDS) solutions and proposed some criteria adapted to the railway domain to help the rail actors to evaluate the solutions available on the market.

Once the risks have been calculated and once the detection and incident management frameworks have been specified, **cybersecurity countermeasures** should be applied. Chapter 6 presents a variety of recommendations related to the **risk mitigation strategies** and the recommended architecture (MILS) to be applied. It also underlines that people play a fundamental role in the cybersecurity strategy. Cybersecurity Awareness training for all employees as well as specialised training for concerned staff should be provided.

Chapter 7 then gives an overview on human factor and organisation practices as well as technical solutions available to manage an incident and ensure an adequate timely responding capability while also minimizing the adverse impacts. The proposed **alerting and collaborative incident management system** is a 3-tier system combining:

- detection means (tier 1),
- a centralized alerting and monitoring system (tier 2),
- a collaborative information sharing system (tier 3).

It takes benefit from the latest solutions on the market like SIRPs (Security Incident Response Platforms), to improve alerts and incident response, as well as interfaces to operation teams. The proposed approach supports the decision-making process and allows the involvement of public authorities. Section 7.3 gives detailed description of the recommended approach.

Finally, **Cyber resilience mechanisms** are proposed in Chapter 8 to better protect the system in order to mitigate damage and quickly restore all capabilities and services that were impaired due to a cyber event.

Protection Profiles for railway control and signalling applications were also delivered by CYRail to ensure security by design of new rail infrastructures. This is addressed by Deliverable D6.1 which is summarised in Chapter 9 and publicly available at <http://www.cyrail.eu/>. It will be used as part of the certification process according to ISO/IEC 15408 and the Common Criteria (CC).

2. RAIL CONTEXT

Nowadays, the increasing development of smart cities and communities leads to a high demand for more efficient, smart, and user-friendly solutions in the urban sector, and particularly transport. As a result, public transport is witnessing a significant technological shift with the proliferation of intelligent transportation technologies in the recent years.

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.

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 changing landscape of ICT solutions, combined with increasing customer demands are pushing Railways to replace their existing legacy systems with more modern and standard-based infrastructure such as IP communication networks, in order to improve reliability, efficiency, capacity and customer experience. Thus, Rail Systems are more and more connected and open and Rail Technologies are becoming increasingly interoperable and harmonized.

Nevertheless, the widespread use of ICT solutions carries a significant risk of high potential cyber-attacks or intrusions, from individuals, organisations and governments that could result in a wide range of possible outcomes, from reputational damage, disruption to services, financial and sensitive information loss through to injury and even loss of life.

To prevent such attacks, security mechanisms must be considered at an early stage in order to effectively protect the system.

3. CYRAIL RAIL SCENARIO

A generic rail scenario with a list of assets, different types of communications systems, and operational environments (urban, high speed and others) has been prepared to be taken into consideration in the security analysis performed in CYRail.

In the CYRail scenario, a typical line with ERTMS and ready to be used for trains with level 1 and level 2 was selected, although with the added difficulty of using public networks (internet) as the connection method between sideway devices and remote maintenance and control systems.

The line is controlled through the interlocking; it is equipped with track occupancy detection devices and also with controlled and non-controlled balises for ERTMS different levels.

Furthermore, point machines and switches are used to establish different train routes.

The communication line includes three different communication types:

- The main communication line is a dual optical fibre network.
- GSM-R is installed to send movement authorities to the train driver from the BTS system.
- The third communication channel between the balises and the on-board equipment (short range communication).

Moreover, all the messages sent to the on-board ERTMS equipment must be ciphered, in order not to be changed by an attacker. Thus, a Key Management Centre is connected to the Radio Block Centre through the main communication line.

Finally, a Local Maintenance Aid System (MAS) for the interlocking is used in order to check failures and review the historic and another MAS exists for the RBC (MAS-R). Equally important is the Centralized MAS and MAS-R, connected to the Internet, in order to allow remote access to the interlocking and RBC Maintenance Aid Systems.

The CYRail rail scenario is presented in Figure 1 below.

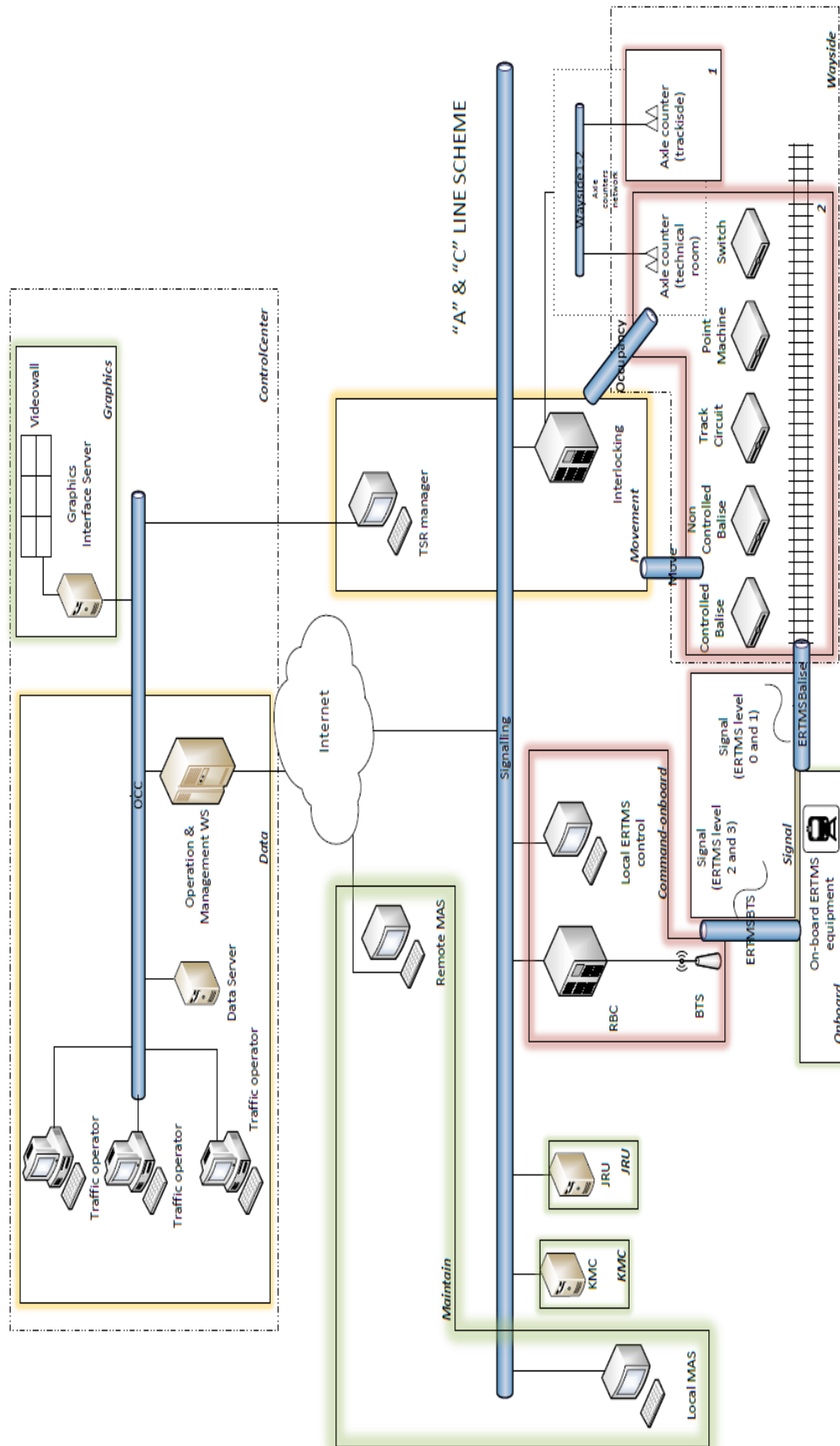


Figure 1. CYRAIL Rail scenario

CYRAIL METHODOLOGY

4.1. INTRODUCTION

The security assessment of a system is the process of:

- evaluating the system vulnerabilities and the threats facing it;
- analysing the probable consequences or risks associated with the vulnerabilities;
- implementing and maintaining countermeasures that reduce the effects of risk to an acceptable level.

The security assessment methodology proposed by CYRail consortium is based on the **IEC 62443 standards**. Accordingly, **three Security Levels** are defined during the security assessment:

- Target SL – the target security level for a zone or conduit;
- Achieved SL – the achieved security level for a zone or conduit;
- Capability SL – the security level capability of countermeasures associated with a zone or conduit or inherent security level capability of devices or systems within a zone or conduit.

A **Target SL** must be defined as a baseline. Then, the risk assessment is performed, and the Achieved SL is calculated in the implementation of the scenario and compared with the Target SL. If the Achieved SL does not fulfil the Target SL, countermeasure must be applied in order to accomplish it. These countermeasures have an associated Capability SL. This process will end when the Achieved SL fulfils the Target SL, describing an iterative risk assessment.

Four different SLs are defined in terms of type of attacker:

- SL 1 – protection against unintentional or accidental attacks.
- SL 2 – protection against intentional attacks with simple means, few resources, usual skills and low motivation.
- SL 3 – protection against intentional attacks with advanced means, average resources, system-specific skills and limited motivation.
- SL 4 – protection against intentional attacks with advanced means, more than average resources, system-specific skills and high motivation.

These Security Levels are defined with a vector whose value corresponds to **each Foundational Requirement (FR)** listed below:

- **Identification and Authentication Control (IAC):** Identify and authenticate all users (humans, software processes and devices) before allowing them to access to the control system.

- **Use Control (UC):** Enforce the assigned privileges of an authenticated user (human, software process or device) to perform the requested action on the IACS and monitor the use of these privileges.
- **System Integrity (SI):** Ensure the integrity of the IACS to prevent unauthorized manipulation.
- **Data Confidentiality (DC):** Ensure the confidentiality of information on communication channels and in data repositories to prevent unauthorized disclosure.
- **Restricted Data Flow (RDF):** Segment the control system via zones and conduits to limit the unnecessary flow of data.

4.2. SECURITY ASSESSMENT METHODOLOGY

The **security assessment methodology** (described in Figure 2) consists in 5 steps:

1. Identification of the System under Consideration (SuC) for the security assessment.
2. Performing a high-level cybersecurity risk assessment (HLCRA): The main goal of the high-level cybersecurity risk assessment is the identification of the worst-case unmitigated risk that the SuC presents to the organization. This assessment's output is the input for the third step of the security assessment.
3. Partition of the SuC into zones and conduits and the definition of the vulnerabilities of each zone and conduit. Besides, a Target SL is defined for each of the zones and conduits.
4. Detailed cybersecurity risk assessment is performed in each zone and conduit, which is composed of twelve steps.
5. Documentation of the process.

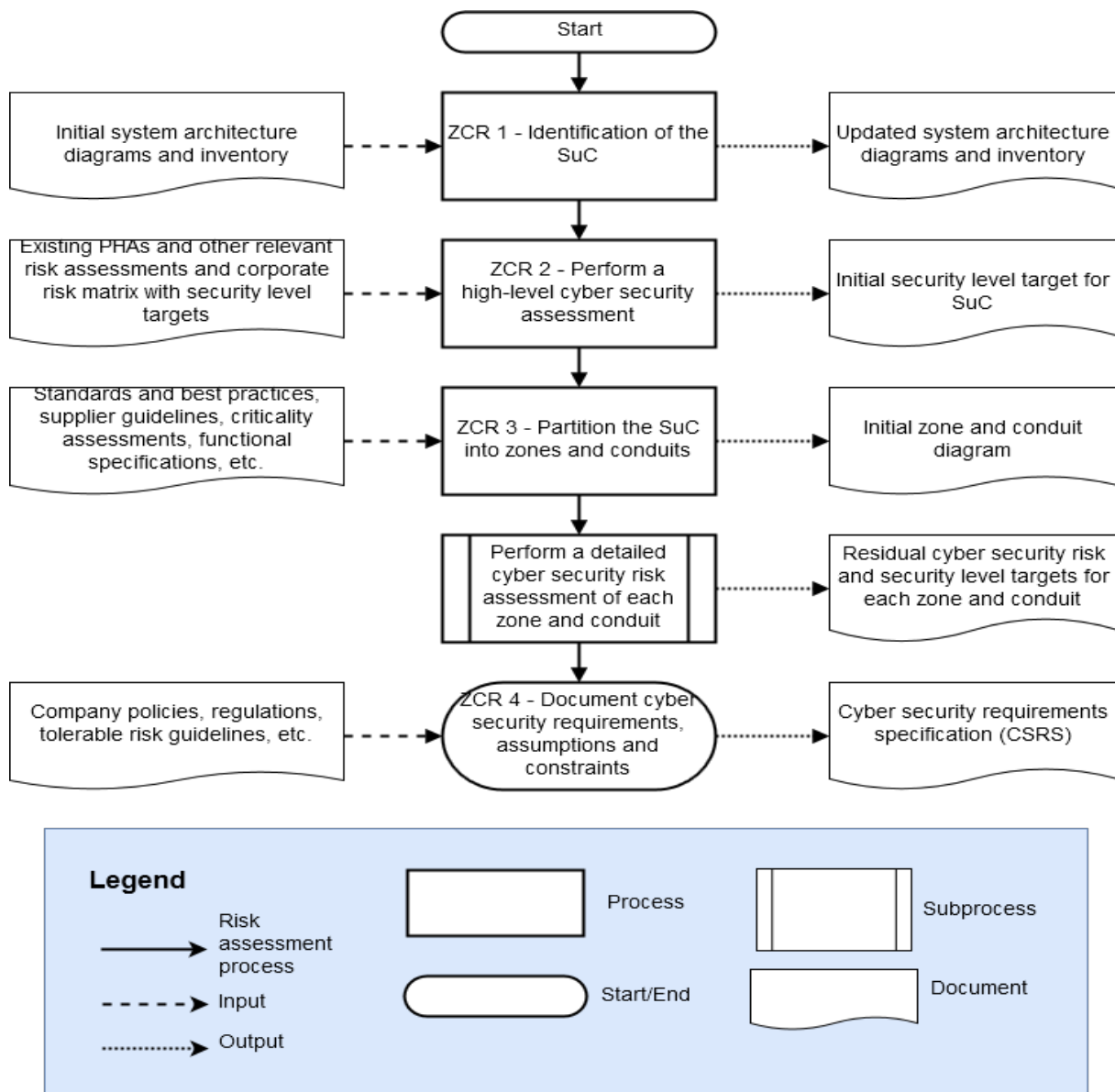


Figure 2. Security assessment process

The five steps of security assessment methodology are described below:

4.2.1. Identify the System under Consideration (SuC)

In CYRail the SuC under consideration is a railway communication scenario, potentially supporting ERTMS level 1 or level 2. This operational scenario is described in Chapter 3.

4.2.2. Performing a high-level cybersecurity risk assessment (HLCRA)

The main goal of the high-level cybersecurity risk assessment is the identification of the worst-case unmitigated risks that the SuC presents to the organization. This assessment's output is the input for the third step of the security assessment.

For the high-level cybersecurity risk assessment, a complete list of assets is needed. These assets may be physical, logical or human assets. However, human assets will not be considered in this high-level cybersecurity risk assessment.

In CYRail case, the list of assets under evaluation is based on the SUBSET-0.26-2¹ and the personal experience of the partners. Although the SUBSET-0.26 differentiates many subsystems under the on-board equipment (DMI, odometry, STM, etc.), CYRail considers all the subsystems as a unique system. This is because any failure in one of the subsystems involves the consideration of all the system as out-of-order.

Accordingly, the following assets are the ones considered for the high-level cybersecurity risk assessment: Axle Counter (trackside equipment), Axle Counter (technical room equipment), Track circuit, Signal (ERTMS level 1 and 0), Point Machine, Controlled Balise (ERTMS level 1 and 0), Non-controlled Balise, BTS, RBC, Local ERTMS control, Local Maintenance Aid System ERTMS, Juridical recorder, Temporary Speed restriction Mgr, Key Management Centre, Interlocking, Centralized Maintenance Aid system ERTMS, Data server ERTMS, Graphics interface server ERTMS, Operation and Management workstation, Traffic Operator (dispatcher), On-board ERTMS equipment.

For each asset, the following characteristics are defined:

➤ **High Level Threat Class**

The ISO 27005 standard provides a list of threats that have been grouped in the seven Foundational Requirements which are:

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

➤ **High Level threat**

Examples of High level threat: An attacker performs actions that is not authorized to perform or manipulates the system to create fake data or disables the system, the communication is jammed, etc.

➤ **Unwanted incident**

Examples of unwanted incident: Unauthorized actions are performed, fake data are generated, system is disabled, the train cannot receive any information from the track-side...

➤ **Consequence**

Examples of Consequence: the train may receive fake movement authorities, the train goes to degraded mode, the train stops...

➤ **Impact**

The Impact is the combination of the effect that a given threat may have from three different perspectives: safety, finances, operational functionality. The impact calculation methodology is given in page 21 (**Impact value or Damage**).

1. The SUBSET 026-2 is the second chapter of the ETCS System Requirement Specification, which has a basic system description.

4.2.3. Partition of the SuC into zones and conduits and definition of the vulnerabilities of each zone and conduit.

According to the IEC 62443, the partition of the SuC into zones and conduits is made following the next steps:

- ZCR 3.1 – Establishment of zones and conduits
- ZCR 3.2 – Separation of business and control system zones
- ZCR 3.3 – Separation of safety-critical zones
- ZCR 3.4 – Separation of temporarily connected devices
- ZCR 3.5 – Separation of wireless communications
- ZCR 3.6 – Separation of devices connected via untrusted networks
- ZCR 3.7 – Zone and conduit drawings
- ZCR 3.8 – Documentation of zone and conduit characteristics

Examples of zone:

Wayside, signal, command-onboard, maintenance, movement, control center (Data / graphics), on board ...

Examples of conduit:

ERTMS (BTS-to-Train communication), ERTMS (Balise-to-Train communication), occupancy (axle counter-to-interlocking communication), signalling network, OCC network...

4.2.4. Detailed cybersecurity risk assessment

It is performed in each zone and conduit, which is composed of twelve steps as described below in Figure 3:

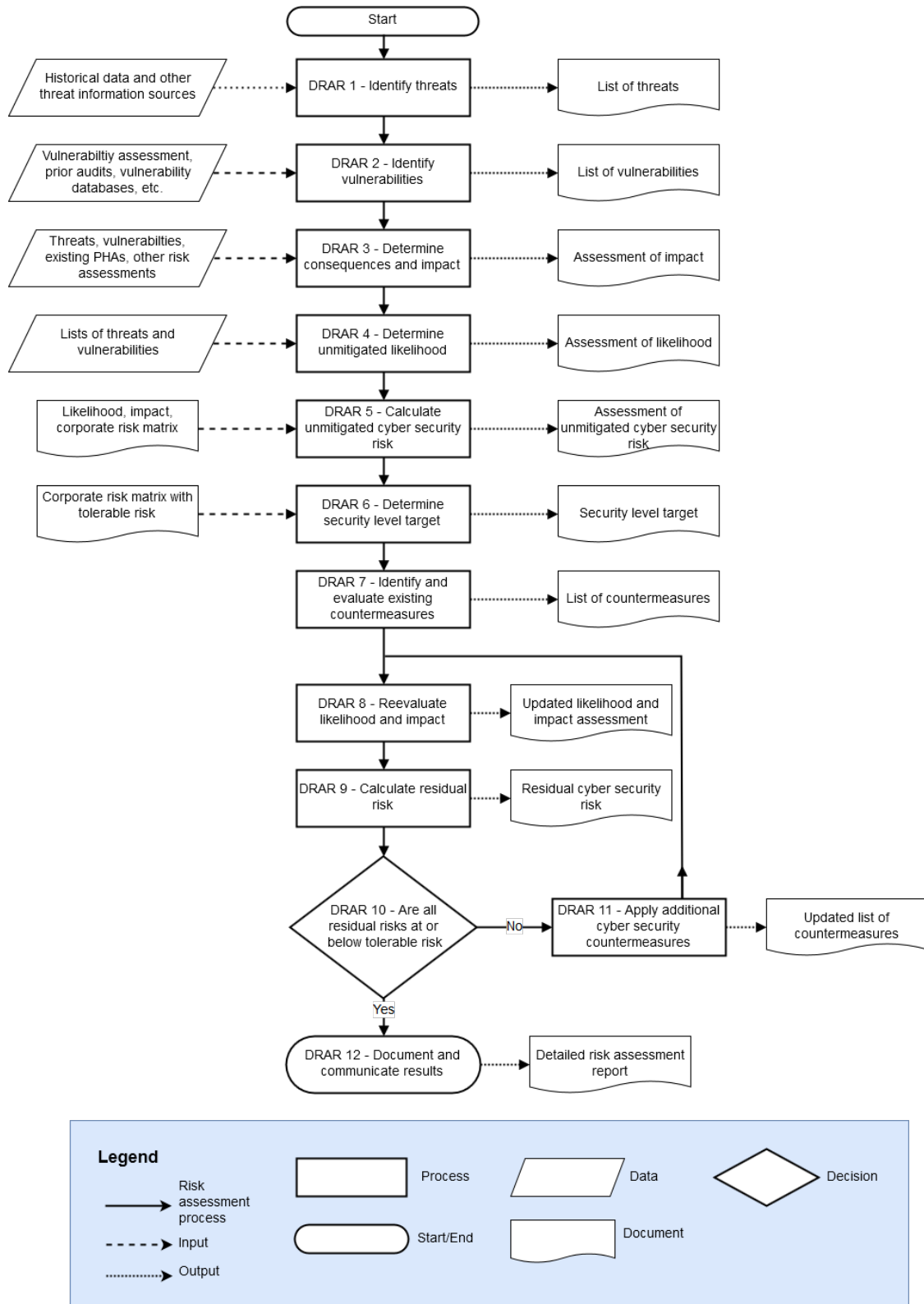


Figure 3. Detailed cybersecurity risk assessment

The twelve steps of the detailed cybersecurity risk assessment are the following:

Step 1: Identify threats

ISO 27005 standard provides publicly a list of threats that have been grouped in the seven Foundational Requirements as stated Table 2.

Table 2. ISO 27005 cyber threats grouping to FR threat classes

Threats	
T.IAC	Forging of rights
T.IAC + T.UC	Abuse of rights
	Illegal processing of data
	Tampering with software
	Use of counterfeit or copied software
	Error in use
T.IAC + T.SI	Fraudulent copying of software
	Unauthorised use of equipment
	Corruption of data
	Tampering with software
	Tampering with hardware
T.IAC + T.DC	Forging of rights
	Data from untrustworthy sources
	Theft or media or documents
	Theft of equipment
	Eavesdropping
	Forging of rights
	Interception of compromising interference signals
	Disclosure
T.IAC + T.RA	Retrieval of recycled or discarded media
	Remote spying
T.IAC + T.RA	Denial of actions
T.RA	Electromagnetic radiation

In CYRail, this approach for threat identification has been complemented with a dedicated **Threat Analysis** focused on past, current and future threats that might affect the railway sector. This analysis has been carried out as follows:

- **Analysis of past incidents:** in the Rail sector and other Transportation sectors, each attack is described, analysed and classified according to classes and attributes that are mentioned below:
 - ▶ **Context:** Geopolitical
 - ▶ **Threat Actor:** Location/Motivation/Resource-level/Sophistication
 - ▶ **Target:** Location/Sector/Zone/Asset

- ▶ **Attack:** Type/Effect/Vulnerability, health and safety
- ▶ **Impact:** Safety/Financial/Operational
- ▶ Additional information: Date and Description of the incident
- **Threat scenarios:**
 - ▶ Identification of new likely threat scenarios consistent with CYRail’s operational context and security assessment.
 - ▶ Overview of the potential future attacks based on threat trends (mostly Advanced Persistent Threats and ransomware attacks) and current flaws in railway systems.
 - ▶ Advisory for enhanced Cybersecurity Awareness at the level of railway operators.
- **Threat taxonomy and ontology:**
 - ▶ **Threat taxonomy:** description of the classes (Context, Threat Actor, Target, Attack, and Impact), definition of their attributes (as listed above, eg. “Location, Motivation, Resource-level, and Sophistication” for the “Threat Actor” class), and identification of the values for each attribute with their definition (eg. “Individual, Club, Contest, Team, Organization, or Government” for the “Resource-level” attribute).
 - ▶ **Threat ontology** (Figure 4), based on the previous Threat taxonomy, to describe how categorized threat information can be used to understand future cyber-threats in their overall context, e.g. in order to derive the level of security risk related to these threats, or their level of impact.

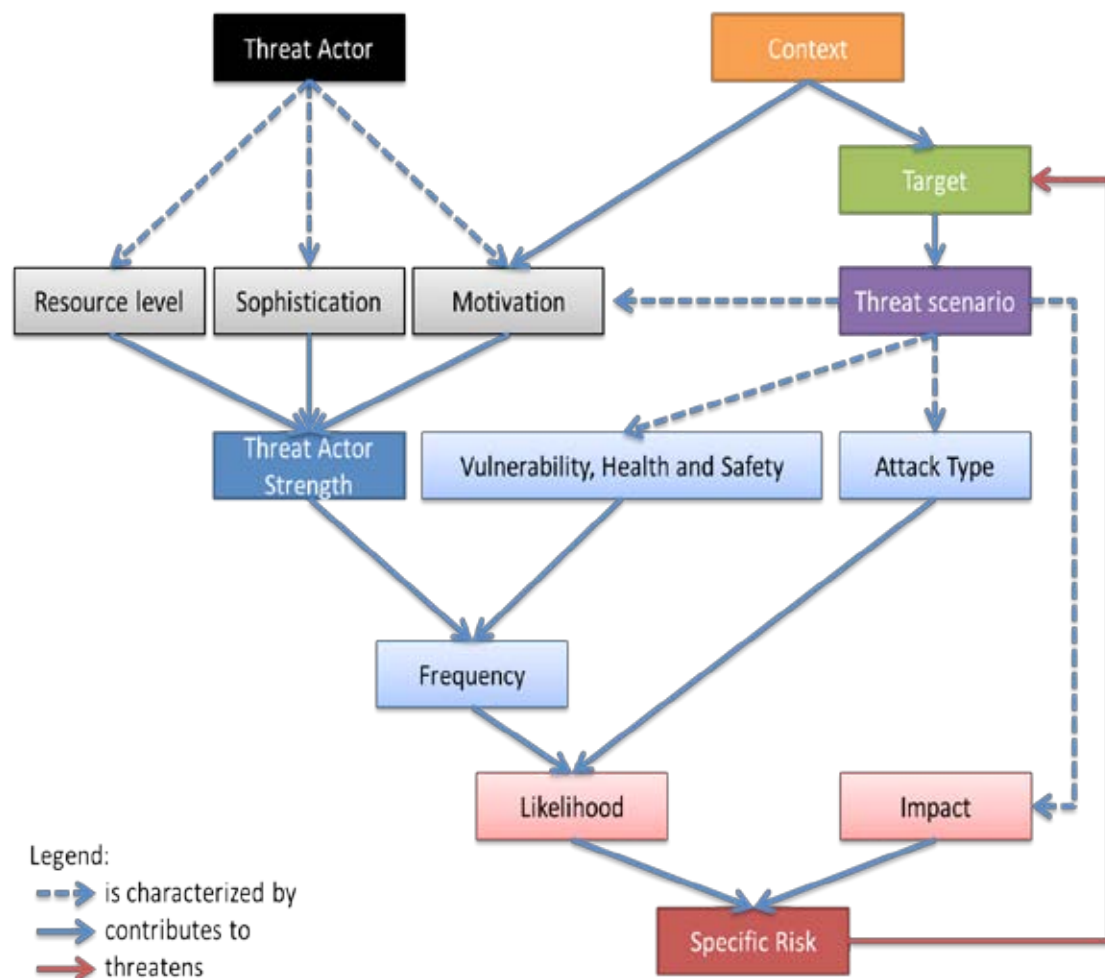


Figure 4. Threat ontology

Step 2: Identify Vulnerabilities

The ISO 27005 provides also publicly a list of vulnerabilities in various security areas, which are associated to the typical threats presented in the previous section, though in some cases other threats may exploit these vulnerabilities as well.

As the security assessment methodology is based on the 62443 series, vulnerabilities must be identified for each zone. The vulnerabilities that have been taken into account for the assessment, are the ones presented below in Table 3.

Table 3. ISO 27005 cyber vulnerabilities association with cyber threats

Threats		Vulnerabilities (ISO-IEC 27005)
T.IAC	Forging of rights	<ul style="list-style-type: none"> ▶ Lack of identification and authentication mechanisms like user identification ▶ Unprotected password tables ▶ Poor password management
T.IAC + T.UC	Abuse of rights	<ul style="list-style-type: none"> ▶ No logout when leaving the workstation ▶ Disposal or reuse of storage media without proper erasure ▶ Lack of audit trail ▶ Wrong allocation of access rights ▶ Lack of formal process for access right review (supervision)
	Use of counterfeit or copied software	<ul style="list-style-type: none"> ▶ Lack of procedures of provisions compliance with intellectual rights
	Error in use	<ul style="list-style-type: none"> ▶ Insufficient security training ▶ Incorrect use of software and hardware ▶ Lack of security awareness ▶ Lack of procedures for classified information handling
	Fraudulent copying of software	
	Illegal processing of data	<ul style="list-style-type: none"> ▶ Unnecessary services enabled ▶ Lack of monitoring mechanisms
	Tampering with software	<ul style="list-style-type: none"> ▶ Uncontrolled downloading and use of software
	Unauthorised use of equipment	<ul style="list-style-type: none"> ▶ Failure to produce management reports ▶ Unprotected public network connections
T.IAC + T.SI	Corruption of data	<ul style="list-style-type: none"> ▶ Widely-distributed software ▶ Applying application programs to the wrong data in terms of time
	Tampering with software	<ul style="list-style-type: none"> ▶ Lack of back-up copies
	Tampering with hardware	
	Forging of rights	<ul style="list-style-type: none"> ▶ Lack of identification and authentication of sender and receiver
	Data from untrustworthy sources	<ul style="list-style-type: none"> ▶ Lack of formal process for authorization of public available information

Threats		Vulnerabilities (ISO-IEC 27005)
T.IAC + T.DC	Theft of media or documents	<ul style="list-style-type: none"> ▶ Unprotected storage ▶ Lack of care at disposal ▶ Uncontrolled copying ▶ Lack of physical protection of the building, doors and windows
	Theft of equipment	<ul style="list-style-type: none"> ▶ Lack of physical protection of the building, doors and windows
	Eavesdropping	<ul style="list-style-type: none"> ▶ Unprotected communication lines ▶ Unprotected sensitive traffic
	Forging of rights	<ul style="list-style-type: none"> ▶ Lack of identification and authentication of sender and receiver
	Interception of compromising interference signals	
	Disclosure	
	Retrieval of recycled or discarded media	
	Remote spying	<ul style="list-style-type: none"> ▶ Insecure network architecture ▶ Transfer of passwords in clear
T.IAC + T.RA	Denial of actions	<ul style="list-style-type: none"> ▶ Lack of proof of sending or receiving a message ▶ Lack of proper allocation of information security responsibilities
T.RA	Electromagnetic radiation	<ul style="list-style-type: none"> ▶ Sensitivity to electromagnetic radiation

Step 3: Determine consequences and impact

The impact is the combination of the effect that a given threat may have from three different perspectives: Safety, Finances, Operational functionality.

Impact value or Damage Potential:

For the calculation of the damage potential, a quantitative measurement which accumulates the possible damage of each perspective will be used. This measurement will be based on the risk reduction factor used for calculating the SIL level defined in the IEC EN 61508 and applied to railways in EN 51028 and EN 51029. The Table 4 below gives the Classification for the Damage Potential (DP) factors.

It is worth noting that all estimations have to consider the worst-case scenario.

Table 4. Classification for the Damage Potential (DP) factors

Damage category	Damage reference	Factor
Safety severity classes	Life-threatening injuries (survival uncertain), fatal injuries	10000
	Severe and life-threatening injuries (survival probable)	1000
	Light and moderate injuries	100
	No injuries	0

Damage category	Damage reference	Factor
Finance severity classes (global sum)	Existence-threatening financial damage (e.g., monetary damage is >30% of annual sales)	1000
	Substantial financial damage, but yet not existence-threatening (e.g., monetary damage is 20%-30% of annual sales)	100
	Undesirable financial damage (e.g., monetary damage is 5%–20% of annual sales)	10
	No or tolerable financial damage (e.g., monetary damage is <5% of annual sales)	0
Operational functionality severity classes	Vehicles unusable, i.e. one or more fundamental functions are affected	100
	Service required, i.e. an important function is affected. The vehicle can be used only with massive restrictions.	10
	Comfort affected, i.e. a function is affected. The vehicle can be used with some restrictions.	1
	No relevant effect, i.e. at most, an unimportant function is affected and the vehicle can be used without restrictions.	0

Resulting impact value:

The total potential damage (DP) can then be calculated by estimating and adding the values of the three individual factors:

$$DP_{\text{total}} = DP_{\text{safety}} + DP_{\text{finance}} + DP_{\text{operation}}$$

Impact category:

Afterwards, the total DP_{total} can be translated to four Impact categories ready to be used for the risk calculations. The Table 5 defines this translation.

Table 5. Impact category translation

DP	Impact category
0-2	Minor
3-21	Moderate
22-210	Major
>210	Critical

Step 4: Determine likelihood of the threat (TVRA methodology)

TVRA methodology is recommended for the calculation of the likelihood of a threat. It's a combination of needed **time** to perform an attack, necessary **expertise** to perform the attack, needed **knowledge** of the scenario, **opportunity** and needed **equipment**

Each of the attack factors are summed in order to calculate an overall attack potential rating as shown in Table 6.

Table 6. Attack potential

Factor	Range	Value
Time to perform an attack (1 point per week)	=< 1 day	0
	=< 1 week	1
	=< 1 month	4
	=< 3 months	13
	=< 6 months	26
	> 6 months	See note 1
Expertise	Layman	0
	Proficient	2
	Expert	5
Knowledge	Public	0
	Restricted	1
	Sensitive	4
	Critical	10
Opportunity	Unnecessary / unlimited access	0
	Easy	1
	Moderate	4
	Difficult	12
	None	See note 2
Equipment	Standard	0
	Specialized	3
	Bespoke	7
NOTE 1: Attack potential is beyond high		
NOTE 2: Attack path is not exploitable		

Calculation of the likelihood of the attacks is made with the addition of all Attack Potential factors:

$$AP_{\text{total}} = AP_{\text{time}} + AP_{\text{expertise}} + AP_{\text{knowledge}} + AP_{\text{opportunity}} + AP_{\text{equipment}}$$

Resulting value, AP, is then mapped to the likelihood levels defined by IEC 62443 Table 7.

Table 7. Mapping of AP level with the likelihood level from IEC 62443

AP value	AP level	Likelihood level
<3	No rating	Certain
3-6	Basic	Likely
7-14	Moderate	Possible
15-26	High	Unlikely
>26	Beyond high	Remote

Step 5: Calculate unmitigated risk

In the proposed calculation of the unmitigated risk, two matrixes are needed.

One of these matrixes will be used for calculating the risk (R) taking the impact (I) and the likelihood (L) of a threat, following the expression: $R = I \times L$. The risk matrix used in the CyRail project to evaluate the risks in ERTMS, is depicted in Table 8.

Table 8. Risk matrix

Likelihood ↑	Certain (5)	5	10	15	20
	Likely (4)	4	8	12	16
	Possible (3)	3	6	9	12
	Unlikely (2)	2	4	6	8
	Remote (1)	1	2	3	4
		Minor (1)	Moderate (2)	Major (3)	Critical (4)
		Impact			

Despite the matrix used in this project, some Infrastructure Managers use a more restrictive matrix, considering the risk level for critical events, always as “Critical”, even with an “Unlikely” or “Remote” likelihood, as seen on Table 10.

For the levelling of each risk value of the matrix, in Table 9 a risk levelling is proposed.

Table 9. Risk levelling

Value	Risk Level
<3	Low
3-5	Medium
6-9	High
>9	Critical

The second matrix to be used for the calculation of the unmitigated cybersecurity risk is the acceptable risk matrix. This matrix is defined by the company owner of the system and identifies the risk level acceptable according to its company and/or national requirements. It is worth noting that this matrix could change from one railway infrastructure manager to another. For this project we have selected a maximum risk level of 3 as acceptable. This assumption allows us to define as unacceptable risk any catastrophic impact, independently of its associated likelihood. Thus, any life-threatening injuries that compromise safety according to Table 4 and Table 5 is considered unacceptable.

The result of all these considerations is the Table 10 below:

Table 10. Acceptable risk matrix

Likelihood ↑	Certain (5)	Unacceptable	Unacceptable	Unacceptable	Unacceptable
	Likely (4)	Unacceptable	Unacceptable	Unacceptable	Unacceptable
	Possible (3)	Acceptable	Unacceptable	Unacceptable	Unacceptable
	Unlikely (2)	Acceptable	Acceptable	Unacceptable	Unacceptable
	Remote (1)	Acceptable	Acceptable	Acceptable	Unacceptable
		Minor (1)	Moderate (2)	Major (3)	Critical (4)
		Impact			

Step 6: Determine Security Level Target

The objective is to identify the most critical security zones; CYRail recommendation is to use the Cyber Risk Reduction Factor (CRRF) defined in the IEC 62443-3-2 which is obtained from the division of the Unmitigated risk by the Tolerable risk.

Step 7: Identify and evaluate existing countermeasures

The results of applying the security assessment methodology will end by providing countermeasures for the assets in order to reduce the risk. These countermeasures will be the basis for the protection profiles.

The document IEC 62443-3-3 provides guidance on types of countermeasures and their effectiveness by assigning a security level capability (SL-C) to each system requirement

Section 6 gives some specifications for mitigation and countermeasures.

Step 8: Re-evaluate likelihood and impact

As described in step 4

Step 9: Re-calculate unmitigated risk (residual risk)

As described in step 5

Step 10: Determine if residual risks are below tolerable risk

The residual risk calculated for each threat shall be compared to the organization's tolerable risk 6. If the residual risk exceeds the tolerable risk, the organization shall determine if the residual risk will be accepted, transferred or mitigated with additional countermeasure.

Step 11: Apply additional countermeasures

Step 12: Document and communicate results

4.2.5. Documentation of the process

In this last step the information obtained during the cybersecurity risk assessment is properly documented. In order to do so, the following information must be recollected:

- ZCR 5.1 – Cybersecurity requirements specification;
- ZCR 5.2 – SuC description;
- ZCR 5.3 – Operating environment assumptions;
- ZCR 5.4 – Threat landscape;
- ZCR 5.5 – Mandatory security policies;
- ZCR 5.6 – Tolerable risk;
- ZCR 5.7 – Regulatory requirements.

EARLY ATTACK AND ANOMALY DETECTION

As already outlined, the widespread use of ICT solutions in the railway environment carries a remarkable risk of high-potential cyberattacks and intrusions potentially perpetrated by individuals, organisations and governments. These kinds of attacks could result in a wide spectrum of possible detrimental outcomes, ranging from reputational damage, service disruptions, financial and sensitive information loss, through to injury and even loss of life.

Being able to effectively protect the system by preventing such intrusions requires security mechanisms to be properly considered when still at early stages. Therefore, it is paramount to find out solid technical solutions for early detection of anomalies and cyber-attacks which are also adapted/optimized for the specificities of the railway environment.

Besides other well-known cybersecurity solutions such as firewalls, encryption, VPNs, etc., an important role towards early attack and anomaly detection may be played by Intrusion Detection Systems (IDS).

Although the market for this kind of solutions cannot yet be considered mature and at present there aren't any IDS solutions specifically conceived for the railway sector, it is currently developing at a fast pace and major expansion is expected for the coming years.

5.1. WHAT IS AN INTRUSION DETECTION SYSTEM (IDS)?

An IDS is a hardware and/or software product, complimentary to other cybersecurity solutions, capable of gathering and analysing information coming from various areas within a computer system or a network with the purpose of identifying signs of possible incidents.

These may be represented by violations (or imminent threats of violation) of computer security policies, acceptable use policies, or standard security practices: whenever an intrusion is detected, the IDS fires an alarm.

An IDS can either search for specific known patterns linked to cyber threats (i.e. signatures) or detect certain deviations from a specified or expected behaviour.

5.2. IDS PROCESS: THREE STAGES

Data collection stage:

One or more sensors -called 'generators'- monitor different sources and collect event records, producing as an output formatted data which is suitable for analysis.

Analysis stage:

Event records are analysed and searched for signs of intrusions or other security concerns.

Response:

When a sign of intrusion is found during the analysis phase, a response is triggered by the system. Responses may vary consistently, ranging from simple logs or reports to automated responses aimed at disrupting the ongoing attack.

5.3. BASIC ARCHITECTURE OF AN IDS

The Figure 5 below gives an overview of the architecture of an IDS:

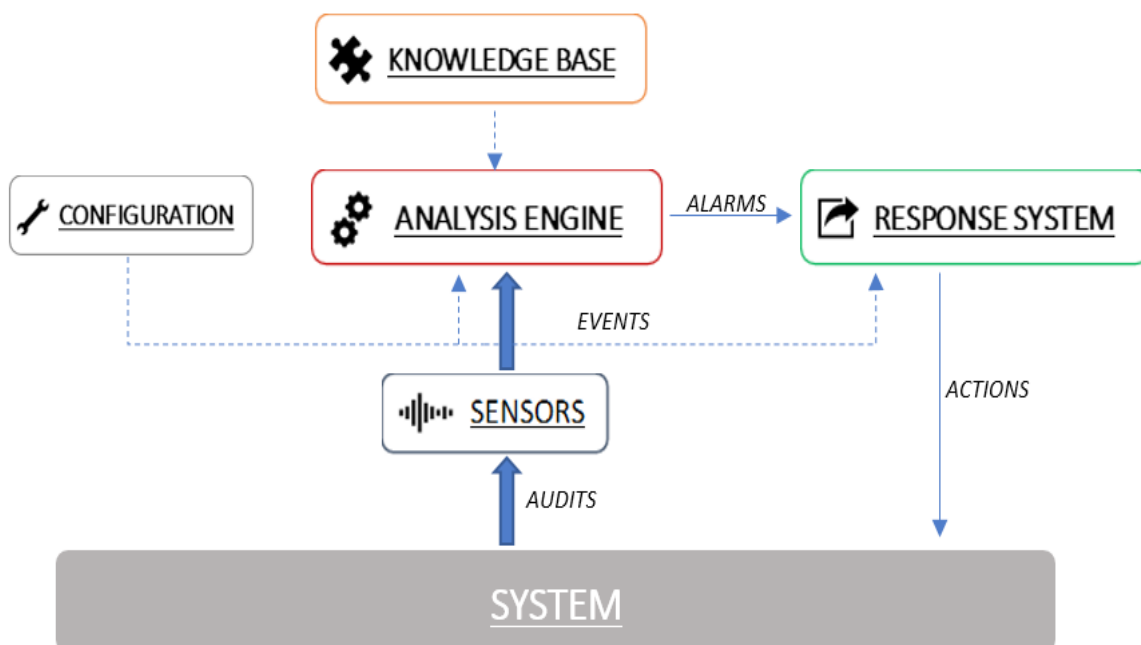


Figure 5. Basic architecture of Intrusion Detection Systems

- **Configuration:** It provides the current state of the IDS.
- **Sensors:** A sensor is a component that collects activity records from the system, generates audit records for necessary events, filters and compresses the relevant ones and ensures their secure delivery to the analysis engine in a convenient format.
- **Analysis engine:** It processes the audit records to determine whether the event corresponds to an anomalous or a misuse behaviour (i.e. deviations from the normal usage patterns or event corresponding to known intrusion patterns or conflicts).

- **Knowledge Base:** A comprehensive repository containing information about known misuse events or intrusion scenarios (i.e. signatures) provided by security experts. These signatures, which summarise all the relevant descriptive elements, are presented in a format that allows straightforward comparison with information found in the event stream.
NOTE: the IDS knowledge base will require frequent updates in order to keep protecting the system against the latest upcoming attacks.
- **Response System:** It ensures that the IDS prevent intrusions on a real-time basis. Its role is to apply rules on the outputs of the analysis engine, and to decide what reactions should be initiated. These reactions may be either fully automated (*preventive system*) or involve human interactions (*reporting system*).

5.4. MAIN REQUIREMENTS OF AN IDS

- **Accuracy:** the IDS should be capable of detecting and distinguishing malicious activities from the legitimate ones.
- **Performance:** It must be able to perform real-time intrusion detection.
- **Completeness:** It should not fail to detect an intrusion. This requirement is extremely difficult to fulfil because it is almost impossible to detect a completely unknown attack with no previous knowledge.
- **Fault tolerance:** It must itself be resistant and robust against malicious attacks.
- **Scalability:** It must be able to monitor the worst-case number of events in a large network topology.

5.5. THE TWO MAIN CLASSES OF IDSS: HIDS AND NIDS

- **HIDS:** Host-based Intrusion Detection System
A HIDS is a software application residing on a single and only monitoring the events occurring within that host for malicious activities. It analyses data such as log files, system calls, file accesses, user or application behaviour etc., and generates alerts once an intrusion has been detected. Being restricted to one host provides a reliable and precise analysis to determine what processes and users are involved in a particular intrusion.
- **NIDS:** Network-based Intrusion Detection System
A NIDS is a standalone hardware device: it consists of a set of single-purpose sensors placed at various points in a network to inspect the data packets from all devices inside the LAN. It monitors network traffic for specified network segments or devices to identify malicious activities such as denial of service attacks, port-scans or even attempts to crack into computers. NIDS provides a wide variety of security features such as information gathering, logging, detection, and prevention.

5.6. DETECTION METHODOLOGIES: SIGNATURE-BASED, ANOMALY-BASED AND HYBRID

Most IDS technologies use multiple methodologies, either separately or integrated, to provide more broad and accurate detection. The primary methodologies are:

- **Signature based detection (Pattern Matching, Rule-based, State-based and Data-mining based techniques):** compares known threat signatures to observed events to identify incidents. This is very effective at detecting known threats but largely ineffective at detecting unknown threats and many variants on known threats. Signature-based detection cannot track and understand the state of complex communications, so it cannot detect most attacks that comprise multiple events.
MAIN DRAWBACKS: inability to detect new attack patterns since no rule would match.
- **Anomaly-based detection (Rule-based, Biology-based, Machine learning-based techniques):** compares definitions of what activity is considered normal against observed events to identify significant deviations. This methodology can be very effective at detecting previously unknown threats. However, anomaly-based detection may inadvertently include malicious activity within a profile, generating many false positives.
MAIN DRAWBACKS: very long 'learning phases' (e.g. 6 months); lack of information about detected anomalies require the intervention of a security analyst to investigate.
- **Hybrid Intrusion Detection:** Due to their inherent characteristics and drawbacks, neither of the two methodologies illustrated above may be fully satisfying as a single choice for end-users. Therefore, organizations typically deploy both the solutions at the same time or rely on hybrid ones which support both methodologies (e.g. NIDES, Haystack, EMERALD).

5.7. IDS PROTOCOL SUPPORT: IT, OT, IT ADAPTED TO OT

The relevance of an IDS can also be assessed depending on the range of supported protocols. In the whole railway context, most of the IT and OT protocols may be used. However, the role and location of IDS sensors would determine the necessity to support IT or OT or both sorts of protocols.

Concerning the IDS type with regard to the supported protocols, the IDS available on the market may be:

- **IT-related IDS;**
- **Adaptations of IT-related IDS to support OT protocols;**
- **Industrial.**

5.8. MARKET STATUS QUO FOR IDS-BASED SOLUTIONS

Currently, both open-source and commercial solutions are available on the market.

Nevertheless, none of the IDS solutions currently available on the market, whether commercial or open-source, have been specifically adapted for railways.

While IT and IT-extended-to-OT market has reached more stability and the products have a higher level of maturity, most industrial IDS vendors are recent SME companies: this may potentially affect negatively their product support capabilities over the next years.

Cumulating both signature-based and anomaly-based is the best option, even if it makes the IDS more complex to manage. Using a full automated learning process to create the behaviour baseline may be risky, if any ongoing intrusion was present at the time the baseline was generated. To mitigate this risk, IDS vendors may provide expert knowledge to tune the anomaly detection rules.

Some solutions include -or interface with- response capacities. This should be considered as a nice-to-have feature (even if far less important than the detection ability).

The capability to interface a SIEM is a must have whatever the type of IDS. The ability to discover the network topology is necessary for industrial IDS as most of them define anomalies based on the knowledge of hosts and devices connected to the network.

5.9. EVALUATION OF IDS SOLUTIONS

According to what has been illustrated in the above paragraphs, IDS solutions available on the market should be analysed and evaluated on the basis of the following elements:

- **EXISTENCE OF AN EXPLICIT CLAIM (BY EDITORS/DEVELOPERS) OF SUITABILITY TO THE RAILWAY SECTOR CONSTRAINTS:** available/not available;
- **TYPE:** IT, IT-extended-to-OT, Industrial;
- **DETECTION MODE:** Signature-based or Anomaly-based;
- **PROTOCOL SUPPORT:** IT, OT, DPI;
- **ASSET DISCOVERY CAPABILITIES:** available/not available;
- **IDS RESPONSE CAPACITY:** available/not available;
- **INTEGRATION CAPACITY** with other elements such as SIEM, CMDB;
- **PRODUCT MATURITY:** Weak, Medium, Good;
- **DEVELOPER'S COUNTRY OF ORIGIN.**

6. PREVENTION

RISK MITIGATION AND COUNTERMEASURES SPECIFICATION

According to the result of the risk assessment (Chapter 4), a set of cybersecurity countermeasures and risk mitigation strategies must be put in place to prevent accidental as well as intentional cyber threats, which may be source to cyber-attacks that exploit vulnerabilities in processes or people in order to impact railway services.

This chapter will present a variety of recommendations related to cybersecurity countermeasures and mitigations strategies that are intended to address the threats targeting railways in order to prevent or minimize their impact on the different critical assets.

6.1. FIVE KEY MITIGATION STRATEGIES

This chapter describes the five key mitigation strategies that can be used to drive cybersecurity activities for railways.

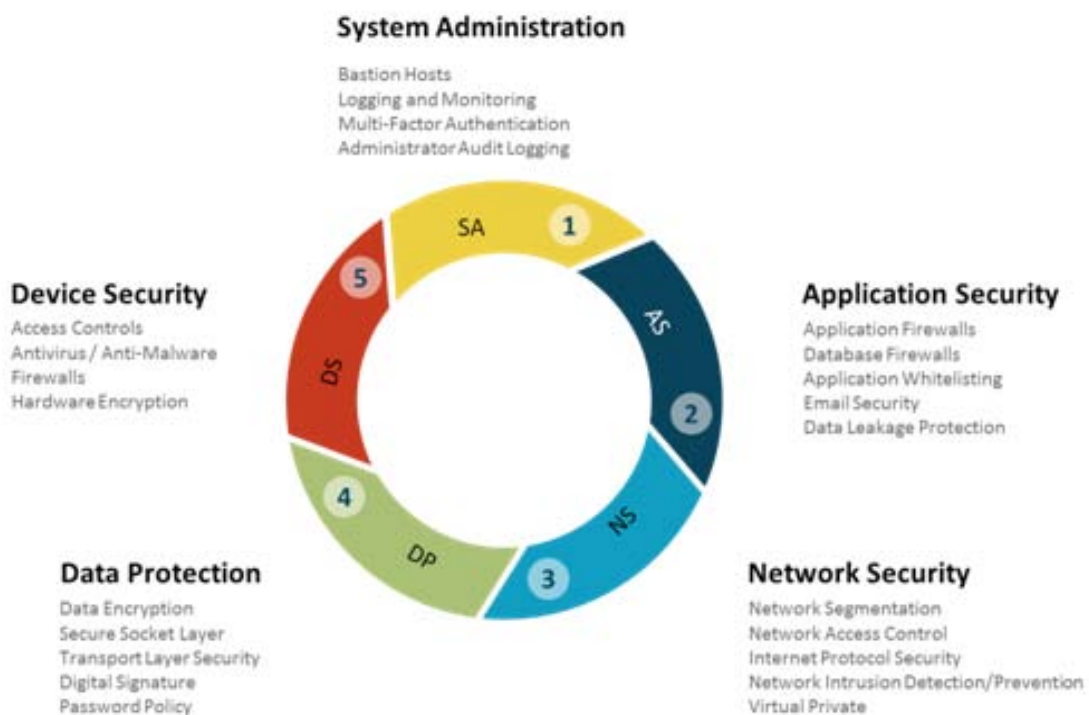


Figure 6. Five key security mitigations for railways

Table 11 below summarizes the major cybersecurity mitigation strategies. Nevertheless, it is important to note that this is not an exhaustive list, but it reflects the most recommended and commonly used cybersecurity mitigation strategies.

Table 11. Cybersecurity mitigation strategies

Functional Area	Cybersecurity Mitigation Strategies
System Administration	Bastion Hosts
	Logging and Monitoring
	Multi-Factor Authentication
	Administrator Audit Logging
Application Security	Application Firewalls
	Database Firewalls
	Application Whitelisting
	Email Security
	Data Leakage Protection (DLP)
Network Security	Network Segmentation
	Network Access Control (NAC)
	Internet Protocol Security (IPSec)
	Network Intrusion Detection System (NIDS)
	Network Intrusion Prevention System (NIPS)
	Network Traffic Analysis (NTA)
	Virtual Private Network (VPN)
Device Security	Computer Access Controls
	Antivirus
	Hardware Encryption
	Firewalls
	In-memory Malware Detection
	Hardware Security Module (HSM)
Data Protection	Data Encryption
	Secure Socket Layer (SSL)
	Transport Layer Security (TLS)
	Digital Signature
	Digital Certificate (PKI)
	Password Policy

6.2. HUMAN FACTOR

There are various technical measures that could limit damage from the different threats targeting railways, such as encryption, access control, logging and monitoring, network segmentation, intrusion detection and prevention. However, **people play a fundamental role in an effective cybersecurity strategy** because they are often the weakest link in the cybersecurity chain.

According to Verizon, there have been over 53,000 security incidents this in 2017, including 2,216 confirmed data breaches, however, over a quarter (28%) of attacks involved insiders. In addition, employees' errors were at the heart of almost 17% breaches. Therefore, railway actors should provide **cybersecurity awareness training** to their employees to ensure they are aware of their responsibilities with regard to cybersecurity concerns.

Cybersecurity training should include training on policies and potential cybersecurity threats to the railway actor and its business. Moreover, **specialized training** should be provided to employees with special cybersecurity responsibilities such as executives, systems administrators, developers, and incident responders.

6.3. ADVANCED MITIGATION STRATEGIES

6.3.1. Security by design

Security by design is based on the concept that **security should play an integral role in the design process from the very beginning**. It is a risk-informed approach that requires multi-discipline teamwork and a clear security strategy.

The main principles of security by design are the following:

Least Privilege

A subject should be given only those privileges that it needs in order to complete its task.

If a subject does not need an access right, the subject should not have that right. Furthermore, the function of the subject should control the assignment of rights. In the design phase of the system, the granularity of privileges and permissions requires to apply this principle precisely.

Fail-Safe Defaults

Unless a subject is given explicit access to an object, it should be denied access to that object.

This principle requires that the default access to an object is none. Whenever access, privileges, or some security-related attribute is not explicitly granted, it should be denied. Moreover, if the subject is unable to complete its action or task, it should undo those changes it made in the security state of the system before it terminates. This way, even if the program fails, the system is still safe.

Economy of Mechanism

Security mechanisms should be as simple as possible.

If a design and implementation are simple, fewer possibilities exist for errors. The checking and testing process are less complex, because fewer components and cases need to be tested. Complex mechanisms often make assumptions about the system and environment in which they run. If these assumptions are incorrect, security problems may result.

Complete Mediation

All accesses to objects be checked to ensure that they are allowed.

Whenever a subject attempt to read an object, the operating system should mediate the action. First, it determines if the subject is allowed to read the object. If so, it provides the resources for the read to occur. If the subject tries to read the object again, the system should check that the subject is still allowed to read the object. Most systems would not make the second check. They would cache the results of the first check and base the second access on the cached results.

Open Design

Security of a mechanism should not depend on the secrecy of its design or implementation.

Designers and implementers of a program must not depend on secrecy of the details of their design and implementation to ensure security. Others can ferret out such details either through technical means, such as disassembly and analysis, or through nontechnical means, such as searching through garbage receptacles for source code listings (called “dumpster-diving”). If the strength of the program’s security depends on the ignorance of the user, a knowledgeable user can defeat that security mechanism. The term “security through obscurity” captures this concept exactly.

Separation of Privilege

A system should not grant permission based on a single condition.

Systems and programs should only grant access to resources when more than one condition is met. This provides a fine-grained control over the resource as well as additional assurance that the access is authorized.

Least Common Mechanism

Mechanisms used to access resources should not be shared.

Sharing resources provides a channel along which information can be transmitted, and so such sharing should be minimized. In practice, if the operating system provides support for virtual machines, the operating system will enforce this privilege automatically to some degree. Otherwise, it will provide some support (such as a virtual memory space) but not complete support (because the file system will appear as shared among several processes).

Psychological Acceptability

Security mechanisms should not make the resource more difficult to access than if the security mechanisms were not present.

Configuring and executing a program should be as easy and as intuitive as possible, and any output should be clear, direct, and useful. If security-related software is too complicated to configure, system administrators may unintentionally set up the software in a non-secure manner. Similarly, security-related user programs must be easy to use and must output understandable messages. If a password is rejected, the password-changing program should state why it was rejected rather than giving a cryptic error message. If a configuration file has an incorrect parameter, the error message should describe the proper parameter.

6.3.2. Multiple Independent Layers of Security (MILS)

The MILS architecture is based on the following four design principles:

- Time and Space Separation
- Controlled Information Flow
- Separation Security Policy
- Reference Monitor

Time and Space Separation

MILS architecture requires that the system be specified as a set of functional units, called “partitions” supported by one or more separation mechanisms (e.g., separation kernel, partitioned communication system). Each partition represents a well-defined set of resources and functionality. The MILS separation mechanisms ensure that private resources (e.g., memory, I/O devices) of a partition are kept isolated from other partitions, including residual data in shared resources, hence space separation. In addition, the execution behaviour of one partition should not unduly influence the execution of another partition, hence time separation.

Controlled Information Flow

The MILS separation mechanisms will allow information to flow only along defined communication paths – allowing a controlled exception to full data separation.

Separation Security Policy

The MILS separation mechanisms enforce policies of type-safety, infiltration, mediation, and exfiltration (TIME):

- **Type safety:** specifies that the data types of the information flow mechanisms are preserved (e.g., the controlled information flow will not allow overwriting of a bounded buffer).
- **Infiltration:** specifies that an executing partition is not able to read or otherwise be influenced by private data of another partition (or the separation mechanism).
- **Exfiltration:** specifies that private data of executing partition cannot be written to, modify or otherwise influence the private data of another partition.
- **Mediation:** specifies that an executing partition cannot use private data from one partition to modify or otherwise influence private data of another partition.

Reference Monitor

This Reference monitor concept, called NEAT, has the four following characteristics:

- **Non-bypassable:** Policy enforcement functions cannot be circumvented.
- **Evaluatable:** Policy enforcement functions are small enough and simple enough that proof correctness is practical and affordable.
- **Always-invoked:** Policy enforcement functions are invoked each and every time.
- **Tamperproof:** Policy enforcement functions and the data that configures them cannot be modified without authorization.

ENHANCED ALERTING AND COLLABORATIVE INCIDENT MANAGEMENT

7.1. INTRODUCTION

While the old vision of early warning cyber-defence systems seeking one-time remediation, cyber-incidents is no longer acceptable, while solid early warning and incident management systems are nowadays required to effectively:

- Help companies in **determining the actual causes** of the threats;
- Better **predict and mitigate the implications** of cyber incidents;
- Actively and fully **involve operators and inform local and state authorities** (as required by the NIS Directive).

Selecting an optimal incident management and early warning system is therefore crucial in order to ensure an adequate timely responding capability while also minimizing the impacts. What may differentiate incident management systems one from another in qualitative terms is their capability of contextualizing to a specific domain all the information gathered from different sources (e.g. threat intelligence, internal data sources).

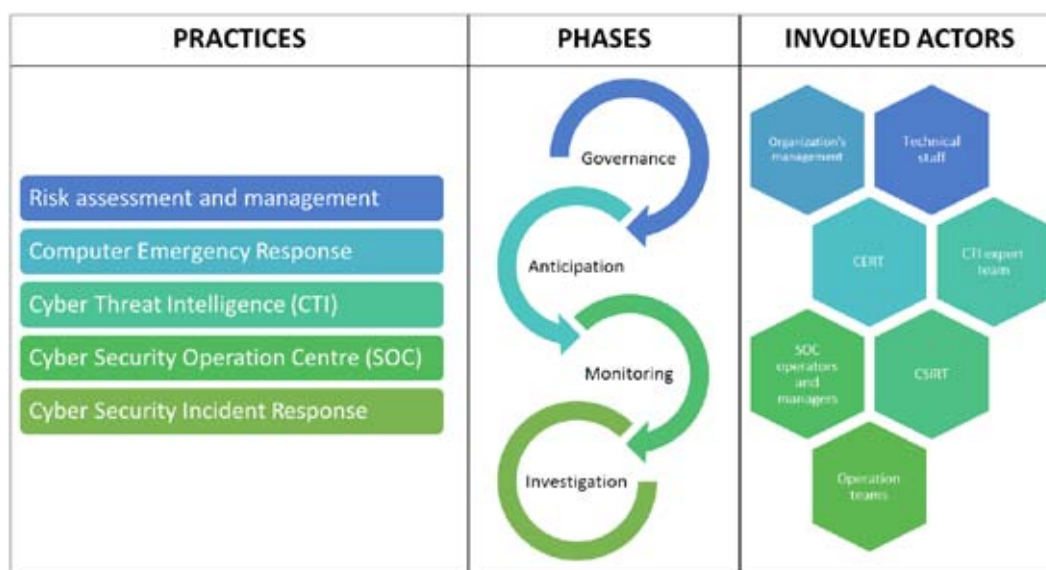
In environments such as IoT, ICS and IT, many practices and technical solutions have been designed to alert and manage cyber incidents. Therefore, in the following paragraphs an overview will be given about both generic and railway-specific practices and technical solutions available.

7.2. STATE OF THE ART

7.2.1. Human Factor and organisation practices

Alerts and incidents management tools have to address a large scope of information that includes: risks, vulnerabilities, threats, intrusion & anomalies, and evidences of compromise. For each type of information, dedicated practices have to be implemented in the overall alerts and incidents management system, as described below.

They will enable the implementation of the four security phases (Governance, Anticipation, Monitoring and Investigation), and involve a diversity of actors:



Cyber Risk Assessment and Management

Cyber risk analysis is the first step when defining a cyber security monitoring strategy which has been described in Chapter 4.

Risk assessment is a key element in the definition of a monitoring strategy such as implemented in a SOC (Cyber Security Operation Centre). Threats descriptions and targeted assets referenced in the risk assessment are further used by cyber experts to define the events generated by systems and sensors (including cyber sensors), that make analysts deduce a cyber intrusion is ongoing. To build an enhanced alerting and collaborative incident management system, it is mandatory to start by a risk assessment.

Table 12. Cyber Risk Assessment and Management

PHASE	ALERTS	INCIDENTS	INVOLVED PARTIES
<ul style="list-style-type: none"> ▶ Anticipation; ▶ Governance (continuous risk monitoring) 	Raised when a risk is detected	Risk on assets due to security breaches , potentially mitigated by existing countermeasures, and/or remediated by reaction plan enforcement. The incident should indicate the effect of the risk and courses of actions to schedule and follow risk mitigation measures enforcement.	<ul style="list-style-type: none"> ▶ Organization's management to define critical assets, decide whether the risk is accepted or not, the investment on countermeasures. ▶ Technical staff (architect, operations/business team, cyber expert) to analyse technical impact, probability and technical solutions.

Computer Emergency Response Team (CERT)

CERT teams may be either private or national/public organization, but in any case, they communicate with nation-level entities (private or public) and CERTs.

Their role is to grant a continuous watch on cyber vulnerability as discovered by software vendors or by cyber experts' community. CERTs analyse vulnerabilities and qualify their potential effects typically through the CVSS (Common Vulnerability Scoring System) and draft guides for the enforcement of prevention measures.

Table 13. Computer Emergency Response Team (CERT)

PHASE	ALERTS	INCIDENTS	INVOLVED PARTIES
Anticipation	Raised when new vulnerabilities are reported	Exposure of vulnerable systems that need to be eliminated adopting corrective actions.	<ul style="list-style-type: none">▶ CERT to describe vulnerabilities, potential impacts and remediation procedures;▶ SOC: collection and analysis of vulnerability bulletins, leading to the definition of the actual vulnerability exploitation feasibility on the rail infrastructure, along with the real impact.

Cyber Threat Intelligence (CTI)

CTI proactively gathers and analyses threat information about attackers' activities and objectives from open sources (OSINT), commercial sources and company's own sources (e.g. SOC) to ensure awareness of new threats, attacker groups and methods. CTI provides support during the investigation phase on cyber incidents (eg. reverse engineering on a malware), helping in determining an ongoing attack's actor.

Table 14. Cyber Threat Intelligence (CTI)

PHASE	ALERTS	INCIDENTS	INVOLVED PARTIES
Anticipation Investigation	Raised when a threat is detected (should include the potential targets within the company)	Targeted threats with effect and countermeasure recommendations, and Indicators of Compromise (IOCs)	<ul style="list-style-type: none">▶ CTI expert team: collects and analyses threat information, supports the SOC and CSIRT teams during the investigation phase▶ CSIRT: brings relevant information to the CTI team, mostly to understand threat actors' tactics and procedures;▶ SOC: requires the CTI team if an observed attack can be linked to a known threat actor, provides data to enhance the CTI knowledge base.

Cyber Security Operation Centre (SOC/CSOC)

The SOC's role is to monitor (in compliance with the risk analysis) and protect the organization's confidential data, production and reputation against cyberattacks occurring daily. It communicates with the monitored organization about detected incidents, explains the situation, and provides recommendations.

The main activities performed by a SOC (which may be structured in different levels) attain **real-time surveillance** and **deep analysis and forensics**. Events from sensors, probes and systems are collected, as well as the network traffic and additional information (e.g. Active Directory, CMDB, vulnerability reports). Detected incidents are linked to violations of policy compliance or intrusions.

Table 15. Cyber Security Operation Centre (SOC)

PHASE	ALERTS	INCIDENTS	INVOLVED PARTIES
Monitoring Investigation	Raised when an intrusion or an anomaly is detected.	Violation of policy compliance, attack, abnormal behaviour mitigated by existing countermeasures, remediated by reaction plan enforcement.	<ul style="list-style-type: none"> ▶ SOC operators (any level) and managers; ▶ Operation teams to get aware of the existence of ongoing incidents like intrusions or misbehaviours, along with their technical impact and resolution/mitigation recommendations; ▶ Organization's managers to agree on closed incidents.

Cyber Security Incident Response Team (CSIRT)

CSIRT is made up by qualified experts whose main duties are related to malicious code analysis and on-site investigation. Once a cyber-attack is suspected or has been reported, CSIRT is tasked with related evidence collection and analysis, along with reporting activities highlighting the exploited vulnerabilities, describing compromise, effect, path, actions of the attackers and providing recommendations for strengthening organization's response and resilience capacities.

Table 16. Cyber Security Incident Response Team (CSIRT)

PHASE	ALERTS	INCIDENTS	INVOLVED PARTIES
Investigation	Raised when some evidence of compromise has been found	Enrichment of data in the incident reports managed by the SOC (confirmation of doubts raised by the SOC, completion of intrusion report) or creation of an incident report in the case when their intervention was requested on suspicion by the affected organization.	<ul style="list-style-type: none"> ▶ CSIRT operators/managers to collect and analyse evidence of compromise in networks and systems; ▶ Organization's management to get the necessary information for taking appropriate decision; ▶ Technical staff (architect, operations/ business team, cyber expert) to analyse technical impact and define and deploy solutions (temporary solutions during the crisis, long-term solutions to enhance protection). ▶ SOC: provides incident reports allowing to start a response course of actions. ▶ CTI: to feed the knowledge base with information on tactics and procedures on real cases gathered by CSIRT.

7.2.2. Technical solutions

Adapted tools and solutions are thus needed to implement the practices described above and support the operational teams in their monitoring and alerting roles. For each solution, the following descriptions address their usage, their functionalities and the required characteristics in terms of information sharing capabilities (in order to raise alerts and/or create incidents, and be interfaced with external systems). These solutions include:

RM	• Risk assessment and Management solutions
TIP	• Threat Intelligence Platforms
SIEM	• Security Information and Event Management systems • Analytics systems
SIRP	• Security Incident Response Platforms
IMS	• Incident Management Systems
CIS	• Collaborative and Information Sharing solutions

Risk Assessment and Management solutions (RM)

Among the risk-related solutions available on the market, some provide risk assessment functionalities, others risk management functionalities, some others both. As compliance to standards is a key point when considering a risk assessment/management solution, most of them are designed targeting specific organizations.

As for the railway sector, both CYRail project and ENISA² sorted inventories of available solutions and tools for Risk Assessment and Risk Management, while the table below summarizes the functionalities that should be granted by such solutions to help addressing both risk assessment and management.

INFORMATION SHARING CAPABILITIES: An important element that should be taken into account when selecting the appropriate RM/RA solution for an organization is the **presence (and sophistication) of interfaces to external systems**.

Most of the currently available solutions cannot alert external systems (e.g., through email messages). Typically, risk reports or extracts are exported as Excel (or CSV), Word, or PDF documents, so that incident tickets must to be created manually and the relation with the threat and countermeasure to be deployed has to be explicitly mentioned in the incident ticket.

2. <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools>

Threat Intelligence Platforms (TIP)

A **Threat Intelligence Platform** is a software system that handles many feeds into a single location, gets alerts in real time, normalizes feed data (by removing duplicates, labelling, enabling user-set rules, etc.), integrates with SIEM, firewall logs, and creates reports and alerts.

A **threat intelligence feed** is a set of indicators and artefacts (IP addresses, domains, hashes) collected from different types of sources that can be open source (called OSINT), customer telemetry, honeypots, scanning and crawling, malware processing, and human intelligence.

INFORMATION SHARING CAPABILITIES: All products have sharing capabilities using widely used formats and protocols, e.g., OpenIOC. Threat Intelligence also leads to reports on existing threats and threat actors. This kind of information is useful for decision-makers and cyber experts. All CTI products have the ability to export reports. Sharing reports usually consists in HTML, WORD or PDF reports.

Security Information and Event Management Systems (SIEM) and Analytic Systems.

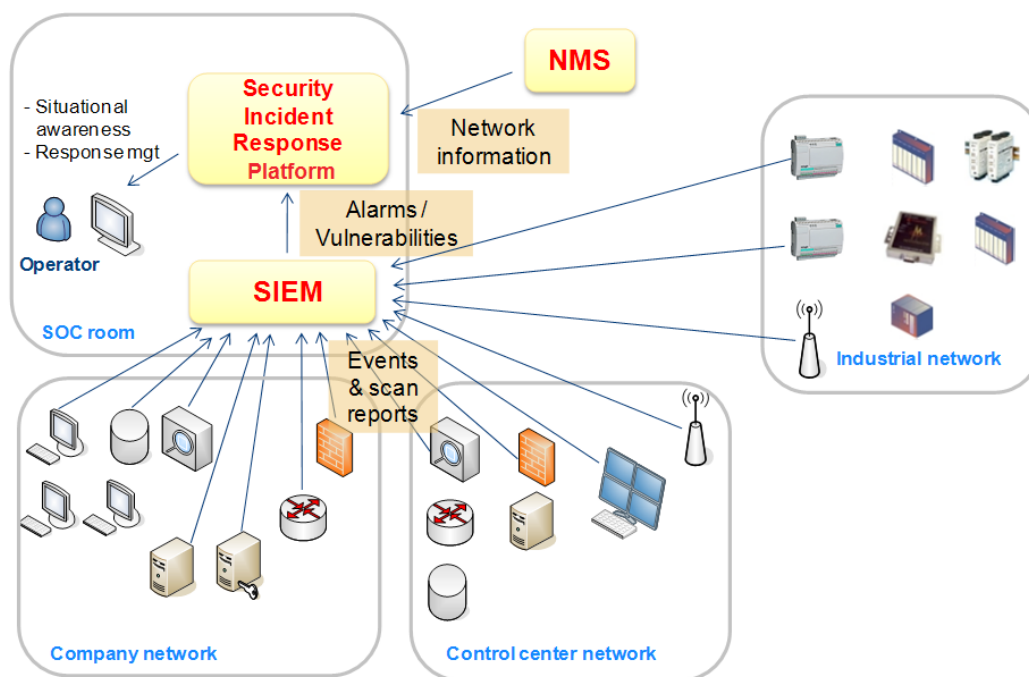


Figure 7. SIEM ecosystem

While SIEMs were initially designed to collect event logs from a variety of sources and perform real-time aggregation and correlation to detect attacks or confirm alerts from sensors such as IDS, nowadays (with the emergence of big data) they tend to provide features around search and analytics with periodic correlation on historians leading to alerts, and deep investigation capacities. They also integrate with TIP to enrich alerts as well as provide security dashboards.

SIEM alerts are technical sets of information, including targeted or compromised systems, as well as attacking sources. Alerts define a level that may be either the technical impact or the priority, or both. Then information shared by SIEM systems mostly targets cyber security experts. As such they are key solutions in a cyber security operation centre but information shared need to be refined before being shared with operation teams. This refinement may be done through additional modules or integrated modules or systems such as SIRP (described in the next paragraph).

INFORMATION SHARING CAPABILITIES: SIEMs have post-alarm action capacities that are usually very open in the way they are able to call remote executable files (e.g. scripts). They also integrate default interfaces with other systems. This enables incident ticket creation, alert sharing, warnings, and data enrichment. They also propose APIs to share with or collect information from external systems.

Security Incident Response Platforms (SIRP)

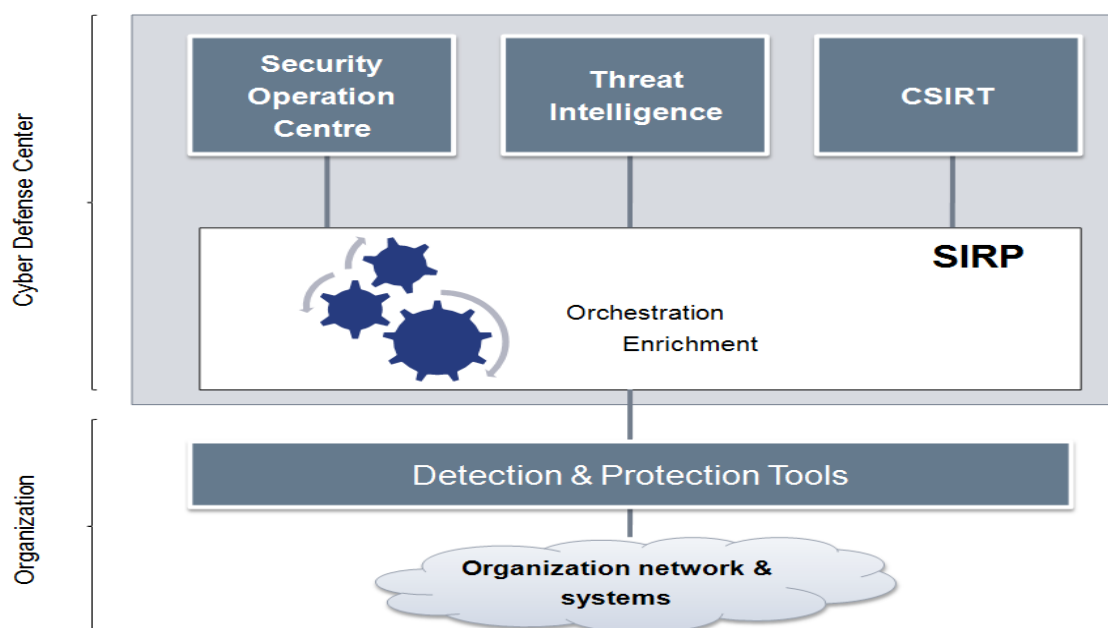


Figure 8. SIRP ecosystem

Security Incident Response Platforms are solutions specifically and meant to support cyber SOC's in the incident response process.

Their main functions are alert/incident analysis (enrichment and cross-correlation) and semi-automated/guided orchestration of incident response through adapted workflows.

The SIRP process can be divided in the following steps:

- **Data collection:** multiple types of data, especially threats and SIEM alerts, seen as incidents;
- **Context Analysis:** definition of the cyber situation induced by ongoing incidents (e.g. which business line is being affected); prior to propose response, the situation can be evaluated through an asset model considering relationships between assets.
- **Response:** SIRPs provide response capacities with a set of connectors to various data sources and external systems, along with email and SMS notifications, and they also publish APIs. SIRPs include an orchestration engine that enables a SOC to define courses of actions after an incident occurs. Reaction workflows are proposed, different depending on the incident type (e.g., DoS, Malware, Policy violation, Integrity loss).

INFORMATION SHARING CAPABILITIES: All SIRP solutions have the same information sharing capacity. The difference comes in the number of supported products. They all have the ability to remotely create/update/close incident tickets managed by ITSM. Some of them can also take into account incident ticket updates made in IMS (synchronisation of information). They have public APIs that virtually enable integration with any external systems (they can share information through emails and SMS). SIRPs can typically export incident reports in various formats such as PDF, HTML, CSV, Excel, Word, and XML.

Incident Management System (IMS)

IMS, also known as Information Technology Service Management (ITSM), are solutions widely used in the IT domain for managing incidents on services and applying the ITIL key processes. In compliance with the ITIL process, they also deal with problems, as an anticipation and prevention of future incidents. Basically, incidents are managed within a reaction process, whereas problems are managed within a proactive process. IMS **manage incident tickets** and **provide some analysis capacities**.

These solutions have been deployed for years in any large company and even if they tend to be quite complex, because they have very deep capacities, they have to be considered at least as legacy systems, which any alerts and incidents management system needs to interface with.

INFORMATION SHARING CAPABILITIES: IMS all have capacities to get information from CMDBs (inventory databases). They also publish APIs to manage assets, issues, problems and incidents.

Collaborative and Information Sharing solutions (CIS)

CIS solutions are dedicated to support project and/or issue management in a collaborative way. Their purpose may address development teams or IT management teams.

The main interest in the CYRail context is that these CIS solutions are designed to facilitate information sharing through collaborative web pages, issue and task management, or even chat in order to enable communication between users (e.g. through public or private channels and direct messaging, integrating social media to get live feed).

Many CIS solutions have already reached a very good level in terms of ergonomics (e.g. creating issues or collaborative pages can be done in minutes without prior training).

These solutions may be useful also if shared by both operation and cyber security teams to exchange information: as an example, when a new threat has been detected by the threat intelligence team, a page could be created and shared with operation and decision teams to explain what the threat actor's objectives are, the threat effects and insight of presence.

7.2.3. Synthesis

The Figure 9 below is a summary table of both inputs and features of the solutions involved in an alerting and incident management system.















	SOURCES	ANALYTICS	DIAGNOSIS	RESPONSE
	 	   	   	   
CERT				Vulnerability related alerts
TIP	TI feeds	Fusion of redundant information	Threat information	Threat related alerts, reports, IoCs
SIEM	Threat related alerts, IoCs, events and sensor alerts	Correlation alerts based on behavior knowledge or expert rules	Cross correlation (vulnerability and threat)	Correlation alerts, post-alerts actions, incidents
ANALYTICS	Any available information	Analysis alerts		Analysis alerts, evidence related to alerts
SIRP	Threat, Analysis, Correlation alerts Incidents	Aggregation and fusion	Contextualization (targeted assets and technical/operational/business impact), enrichment through external knowledge bases	Contextual courses of actions including alerting through any means IN/OUT APIs
RM	Risk analysis, audits	Risks vs criticality and vulnerability	Countermeasure effects	Dashboards and risks & CMs follow up, reports
IMS	Any ticket	Categorization	Remediation action management	Ticket status and comments
CIS	Any issue/ticket/Inputs	Issue data correlation	Workflow	Collaborative pages, chat, APIs

Figure 9. Synthesis of alerting and incident management features

7.3. CYRAIL RECOMMENDED SYSTEM

7.3.1. Introduction

Deploying and maintaining detection means represents a high cost for a company: since many device types are available on the market, it is necessary to select the ones which are more adapted to the railway context.

The proposed alerting and collaborative incident management system is a **3-tier system** combining:

- detection means (tier 1),
- a centralized alerting and monitoring system (tier 2),
- a collaborative information sharing system (tier 3).

It takes benefit from the latest solutions on the market like SIRPs, to improve alerts and incident response, along with an interface to operation teams.

The proposed cyber security incident response approach supports the decision-making process and allows the involvement of public authorities. A two-way communication between cyber security team and operation teams is proposed to better understand impacts of a cyber-attack, and effects of related response actions.

Finally, it has been designed to integrate legacy systems such as IMS and in such a way that it may reuse detection means already in place in zones and conduits and fit any SIEM in the market.

7.3.2. Detection strategy

To determine which situations require an alerting reaction, the output of the risk assessment will be taken into account. A detection strategy, defining the alerts that shall be triggered when unwanted situations are detected, can be established based on the already identified threats on assets and associated countermeasures.

Building a detection strategy makes up the first step in the definition of an alerting system, as it also produces the list of detection means along with the list of alerts that could be raised by the alerting system.

However, it does not necessarily mean real-time detection. Unwanted situations may also be discovered through an investigation or audit process. As a consequence, the alerting and incident management system must allow the manual creation of alerts and incidents by a cyber security operator.

Wherever applicable, sensors or checking processes must be set to automatically or manually raise alerts when abnormal situations are detected.

Alert structure:

- The minimum required information to be included into alerts (whatever the means used for their creation) should be:
 - ▶ **Timestamp**: indicates when the abnormal situation has been detected.
 - ▶ **Asset**: indicates the asset where the abnormal situation has been detected.

- ▶ **Title:** indicates the kind of detected issue through a short text.
 - ▶ **Impact level:** indicates the impact level of the abnormal situation. E.g., a value among “minor”, “medium”, and “major”.
 - ▶ **Sensor:** (optional) indicates which system has detected the abnormal situation.
 - ▶ **User:** (optional) indicates which user has detected the abnormal situation.
 - ▶ **Identifier:** (optional) if the alert comes from a system, and if this one generates a unique identifier per alert, then it is worth having this information to facilitate further investigation.
- Any additional available information should be given to make the situation as understandable as possible and facilitate further investigation.
 - As said, the detection strategy derives from the risk assessment. It permits the definition of both alerts and detection means. When available, technical detection means should be specified; otherwise the tag “N/A” is set. These detection means depend on proposed countermeasures. An alert title is associated to each threat, with a prefix specifying the functional zone. Every alert with related detection means set to “N/A” would be manually created: they result from an investigation or control/audit process.
 - An alert may be the same for different threats because the observed situation may be the same.

Table 17 and Table 18 give examples of alert message that could be raised when a threat occurrence is detected against assets described in the first column of the table. When available, detection systems are specified.

Table 17. Alerts related to “USB autorun on a SCADA asset” threat

Asset	Detection means	Alert
SCADA asset	Antivirus automatically scans external devices and alerts on USB drives trying to use autorun feature Analysis and decontamination solution for USB devices prevents unmanaged USB drives to connect to machines and reports autorun.inf presence on USB drives	[SCD-013] Autorun detected on plugged USB drive

Table 18. Alerts related to “Incursion in the rail IT network” threat

Asset	Detection means	Alert
IT asset	Firewalls: log access to services (authorized and unauthorized ones) and alert on unauthorized attempts	[IT-002] Attempt of unauthorized access to the rail IT network

7.3.3. System requirements

The alerting and incident management system proposed in CYRail (which is physically deployed within the OCC) is structured into three tiers as described in Figure 10 below:

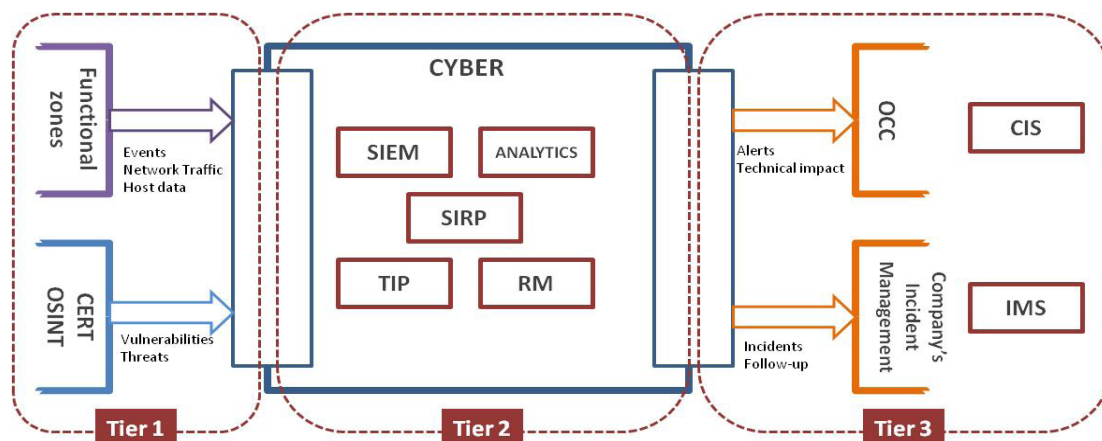


Figure 10. CYRIL system - Functional blocks

TIER 1

It's made up of sensors and event sources such as server and workstation logs (their choice depends upon the risk assessment and detection strategy) located in the different functional zones depending on their role, as described above in the detection strategy.

They generate events and technical alarms that will be used by the security operation centre to have a clear understanding of the cyber security situation and produce alerts.

Referring to the example of alerts in Table 17 and Table 18 described above, it is possible to define the list of detection means that have to be deployed/implemented in the already identified zones as described below in Table 19.

Table 19. List of Tier 1 sources of events and alerts

Detection means	Zone	Asset
Analysis and decontamination solution for USB devices	Wherever SCADA assets are deployed	SCADA asset
Antivirus	Wherever IT assets are deployed	IT asset
	Wherever SCADA assets are deployed	SCADA asset
Checking of enabled security functions	Wherever IT assets are deployed	IT asset
Checking of enabled protocols and remote configuration and programming modes	Wayside 2	Switch
Firewall	Wherever IT assets are deployed	IT asset
	Wayside 2	Switch

Detection means	Zone	Asset
HIDS	Command on-board	RBC
HIPS	Wherever IT assets are deployed	IT asset
IAM	Wayside 2	Switch
	Command on-board	BTS, RBC, Local ERTMS control
Identity and permissions checkers	Command on-board	BTS, RBC, Local ERTMS control
Integrity checker: Firmware integrity and authenticity checkers	Wayside 2	Switch
	Command on-board	BTS Local ERTMS control
Integrity checker: Server integrity controls	Signal	ERTMS level 0 and 1 ERTMS level 2 and 3
Logs: BTS, RBC and local ERTMS control logs	Command on-board	BTS, RBC, Local ERTMS control
Logs: BTS, RBC, local ERTMS and secure NTP event logs		
Logs: Electronic certificate controller logs		Local ERTMS control
Logs: IT asset logs	Wherever IT assets are deployed	IT asset
Mechanisms to monitor and alert the gap between normal activities and abnormal activities.	Conduit	Occupancy, Signalling, ERTMS Balise
	Wayside 1	Axle Counter
	Signal	ERTMS level 0 and 1 ERTMS level 2 and 3
Message integrity controls	Signal	ERTMS level 0 and 1 ERTMS level 2 and 3
NAC	Wayside 2	Switch
Network management system (NMS)	Command on-board	BTS, RBC, Local ERTMS control
NIDS	Wherever IT assets are deployed	IT asset
Patch management	Command on-board	BTS, Local ERTMS control
Secure authentication	Command on-board	BTS, RBC, Local ERTMS control
	Wayside 2	Switch
Security endpoints	Wherever IT assets are deployed	IT asset
Vulnerability scanners	Wayside 2	Switch

Specific requirements for Tier 1 systems:

- As Tier 1 events and alerts are processed by Tier 2 systems, using a *time synchronization service* is mandatory;
- As much as possible *events and alerts must be pushed by Tier 1 systems to Tier 2* systems (usually to the SIEM system); otherwise, means to get events must be provided by the sources (e.g., APIs, access to event files or bases).
- A *secure communication* from these sources to Tier 2 must be enabled.
- Even if they are pushed to the Tier 2, *events and alerts must be locally stored*, i.e. on the detection sources themselves for a limited period of time in order to prevent any loss due network disruption.
- *Detection rules are sensitive information managed by authorized people only*. A specific communication channel should be set with detection means for administration purpose, including rule management. This communication channel should not be shared with the communication channel devoted to event and alert forwarding (separation of roles and need to know).
- *Availability of sources of events and alerts is fundamental to grant detection process is fully operational*. They must be monitored through a checking process, not necessarily done by the security operation centre. However, the security operation centre must be warned as soon as a source of events and alerts is down or suffers some availability issue (e.g., high CPU consumption).

TIER 2

It's comprised within a cyber security zone: it gathers a SIEM, an analytics solution, a SIRP, a TIP and (optionally) a risk management solution.

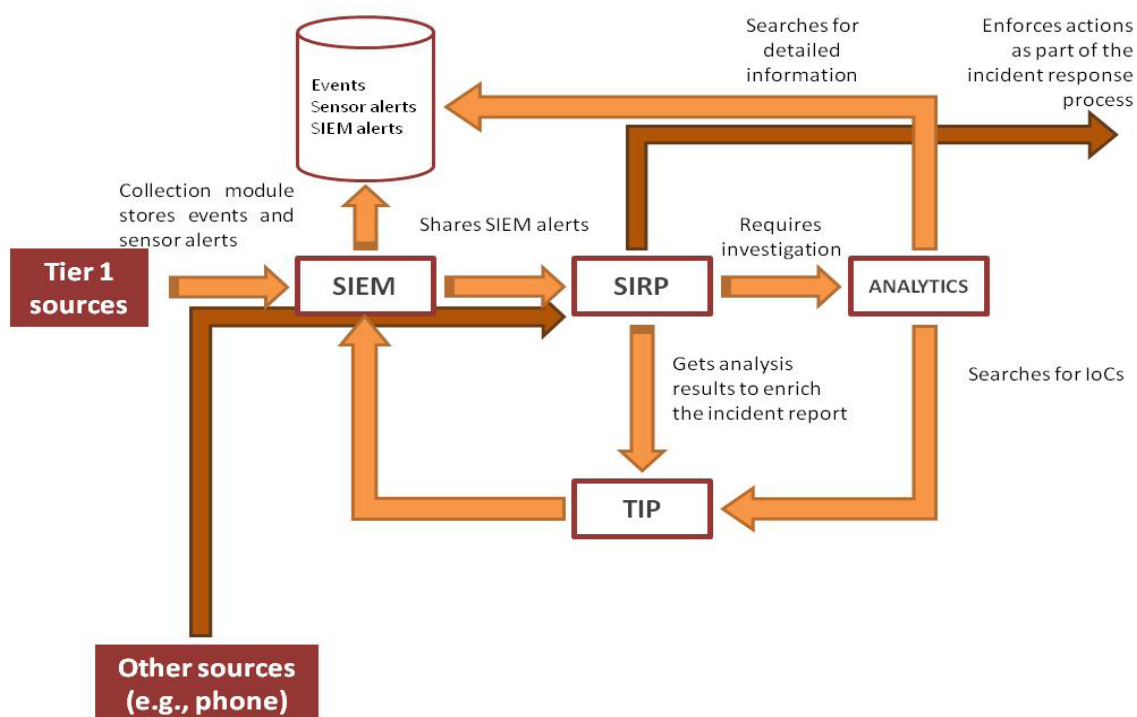


Figure 11. Tier 2 - Main workflow

The Tier 2 of the alerting and monitoring system is a central system located in the security operation centre (SOC). It is devoted to process events and alerts from sensors such as IDS, according to the detection strategy.

Specific requirements for Tier 2 systems:

- The main enforcement point of the detection strategy is a **SIEM**. It must be configured so that, once collected, *events and sensors alerts are normalized to a single format*, and further analysed in respect with the detection strategy.
- *SIEM alerts must be shared to a **SIRP** system* to trigger a response process. The first step is the enrichment of the alert in the goal of giving the necessary information to confirm the alert and qualify it as an incident. This involves communication with other systems such as a TIP and an **analytics system** (that can be a SIEM) specialized in the investigation on big data.
- *The SIRP system must be able to formally qualify a SIEM alert into an incident.*
- *Then the SIRP should be able to evaluate the impact of a cyber incident to railway systems and operations.* This defines the priority in the incident management process.
- *The SIRP system must be able to request the right systems or people depending on the cyber security context* (type of threat, targeted assets), and enable a SOC operator to access information on past incidents, based on criteria from the incident being investigated. The Table 20 below shows the main actions a SIRP can perform within an incident response workflow.

Table 20. Reactions to a cyber security incident

Automated reactions	Assignment Malware analysis Collection of threat intelligence reports Cross correlation with vulnerability Creation of incident ticket/issues Warnings (email, SMS, call API) Priority and/or severity setting
Manual reactions	Any automated reactions + Confirmation of compromise On field investigation Collection of evidence Configuration changes

- *The SIRP should manage sets of conditions that are used to determine which course of actions has to be enforced as incident response.* Conditions are at least about the type of threat, the targeted asset, and the attacker. Any other information reported in the incident may be used as conditions.
- **Dedicated dashboards** should be provided for easily accessing information (including evolution graphs and trends) about:
 - Ongoing alerts and incidents (along with their status and incident management workflow and related;
 - Countermeasures' compliance with security policy and the related risks.
 - Planned actions on countermeasures (e.g. new deployments) to give to operators a clear view on risk level evolutions due to preventive or corrective actions.

TIER 3

It deals with incidents at a broader level, i.e. not limited to cyber security. It consists in incident management and information sharing systems devoted to the communication and synchronization with operation teams.

Requirements for integration in the railway decision-making process: as railway companies usually have IMS solutions in place, so integration with those is required. Even if at this level technical information on how attacks have been performed and detected, cyber security incidents should be reported automatically, once qualified within the SIRP system. This one must be able to send an incident report to the railway IMS, as well as incident report updates describing any change in the situation (“Sent to the railway IMS” tag in the incident managed by the SIRP should be added). Report message content should contain the following information:

- Mention to cyber security;
- Timestamp (detection date);
- Impacted assets (or zones);
- Impact level (e.g., low/medium/high/critical), and its nature (loss of availability, integrity or confidentiality);
- Time for the impact to be perceived (immediate, hours, days, etc.);
- Actions taken by cyber experts to mitigate or remediate the issue;
- Expected time to action completion.

Requirements for integration in the service management:

- IMS solutions manage SLAs (Service Level Agreement), and the SOC has to comply with these SLAs/SSLAs.
- To avoid extra-costs, legacy IMS solutions should be used first to have a single base containing all the incident reports regarding issues on IT-related devices including cyber security issues. However incident resolution is not granted by the IT IMS owners: they are just informed. The proposed resolution approach is a collaborative resolution through a CIS (cf. next section).
- Cyber security incidents should be reported automatically, once qualified within the SIRP system. This one must be able to send an incident report (and updated) to the IT IMS, featuring the same structure described above for reports to railway IMS.

Requirements for Collaborative Incident Resolution, which aim is to grant follow-up by each stakeholder in the railway company:

- Incident resolution should be declared as a project, involving a set of stakeholders, responsible for actions. *Incident description page patterns* should be provided by the CIS to facilitate the reporting of a new incident.
- The CIS should provide *means to follow actions* with an indication of the status (e.g., to do, ongoing, completed) and interface to external systems managing these actions and dynamically update the status.
- *Chat capacity should be enabled to ease the communication among the stakeholders*, and CIS could be considered as a cyber communication portal and may be extended to external organizations like cyber security national agencies, if the regulatory framework requires to. In this case, access control to pages should be implemented and a process describing the role of authorized actors and their permitted views on the cyber communication portal should be defined.

GENERAL ADDITIONAL REQUIREMENTS

- *Access control* to the alert and monitoring system must be implemented, since confidential information is at stake.
- Monitoring and alerting system must be *operational 24/7* even if monitored activities are not necessarily 24/7.
- An *authority* must be stated in case incidents are detected, which may be the SOC authority itself.
- *Points of contact to third-parties* (e.g., public and local authorities, maintenance teams) must be known. As much as possible, means to contact them should be connected to the alert and monitoring system (e.g., pre-filled emails with recipients).

CYBER RESILIENCE MECHANISM

The number of cyber events continues to rise each year. As technologies evolve, so do attack and defence mechanisms. However, both range and sophistication of technologies that attackers have at their disposal are far greater than technologies available for protecting cyber systems. IT and system administrators are not able to fully stop attackers because they cannot keep up with the evolving range of threats. They are always at a disadvantage in this regard.

Therefore, instead of investing only in preventing attacks, organizations have been implementing measures to mitigate damage and quickly restore all capabilities or services that were impaired due to a cyber event. This type of defence is also known as cyber resilience.

8.1. OBJECTIVES

The four main cyber resilience objectives are to: anticipate, withstand, recover and evolve.

8.1.1. Anticipate

In order to successfully anticipate and overcome an attack, there must be complete **understanding** of the company's or system's security environment, that is, their information, assets (human or otherwise), components, risks and vulnerabilities.

With this knowledge, it is possible (to some extent) to **prevent** future attacks by fixing the most dangerous vulnerabilities previously identified, reduce the attack surface, strength the most important assets and even implement measures to counter a predictable upcoming attack.

System administrators, as well as all other relevant actors, should be **prepared** for cyber-attacks by having defined course of actions for foreseeable events.

8.1.2. Withstand

For cyber resilience, to withstand is to maintain essential business functions despite successful execution of an attack by an adversary.

During a successful attack, the system must **continue** essential operations and services, even if only in a degraded or alternative mode. The system must fight through the attack while waiting for it to be addressed, to then enter the recovery phase.

It is important for the system to be able to **constrain** the damage caused by a successful attack, as it will allow defenders to focus their efforts on affected resources, leaving remaining resources available for regular use.

8.1.3. Recover

For cyber resiliency, to recover is to restore any capabilities or services, to the maximum extent possible, that were impaired due to an attack by an adversary.

The recovery process begins after the adversary attack is sufficiently contained or defeated. This process includes:

- **determination of damages** – includes the analysis of tools the attackers used, records produced from monitoring, logging and auditing in order to assert which resources were affected by the attack;
- **restore** capabilities – apply previously defined recovery plans to restore data and services impacted during the cyber-attack. It is of utmost importance to know how business data is being backed up, so data that needs to be restored first to return to normal operations is identified.

8.1.4. Evolve

For cyber resilience, to evolve is to change business functions and cyber capabilities to reduce the adverse impacts of actual or predicted attacks.

Over time, it may be essential to **transform** existing processes or even **re-architect** the current system. These necessities can be triggered by multiple factors, such as:

- Threats: changes in the identity, capabilities, intent or targeting of attackers;
- System: changes in business priorities, workflows, architectural or configuration changes in systems;
- Technologies: new discoveries of vulnerabilities, the introduction of a new technology, phase-out of an established technology, changes on how a current technology is deployed or used.

8.2. PRINCIPLES

This chapter presents design principles related to cyber resilience. These are divided in strategic and structural design principles.

8.2.1. Strategic Design Principles

- Focus on common critical assets;
- Support agility and architect for adaptability;
- Reduce attack surfaces:
 - ▶ Reduce the area of the attack surface: restrict available functionalities (i.e., ports, protocols, functions, and services), deprecate unsafe functions and remove vulnerable APIs;
 - ▶ Reduce the exposure of the attack surface: restrict access privileges, employ layered defences and component isolation;
 - ▶ Reduce the duration of exposure: reduce the window of opportunity by minimizing the time the attack surface is available;
- Assume compromised resources;
- Expect adversaries to evolve.

8.2.2. Structural Design Principles

Structural design principles refer to those that directly affect system architecture and design.

They can be applied in more specific areas of the architecture and be tailored according to system necessities. The following table presents how structural design principles can be related to strategic design principles .

Table 21. Relation between structural and strategic design principles

Structural Design Principles	Strategic Design Principles				
	Focus on common critical assets	Support agility and architect for adaptability	Reduce attack surfaces	Assume compromised resources	Expect adversaries to evolve
Limit the need for trust			X	X	
Control visibility and use	X		X	X	
Contain and exclude behaviours	X			X	X
Layer and partition defences	X			X	
Plan and manage diversity	X	X		X	
Maintain redundancy	X	X			
Make resources location-versatile	X	X			X
Leverage health and status data	X			X	X
Maintain situational awareness	X	X			X
Manage resources (risk-) adaptively	X	X			X
Maximize transience; minimize persistence			X	X	X
Determine ongoing trustworthiness	X			X	X
Change or disrupt the attack surface			X	X	X
Make unpredictability and deception user-transparent					X

8.3. TECHNIQUES

8.3.1. Adaptive Response

Adaptive Response refers to the ability to take actions base on knowledge of the characteristics of ongoing attacks

8.3.2. Analytic Monitoring

Analytic monitoring refers to continuously gather and analyse monitoring data in order to identify vulnerabilities, intrusions and damage.

8.3.3. Coordinated Defence

Coordinated defence refer to effectively and adaptively manage and coordinate multiple mechanisms used to protect critical resources from adversary attacks

8.3.4. Deception

Deception refers to the ability to confuse an adversary through the application of obfuscation and misdirection techniques.

8.3.5. Diversity

Diversity refers to the use of heterogeneity in the implementation of techniques (software, hardware, protocols, network).

8.3.6. Dynamic Positioning

Dynamic positioning refers to the ability to dynamically relocate and distribute critical assets and system components, using virtualization and distributed processing.

8.3.7. Dynamic Representation

Dynamic representation refers to constructing and maintaining representations that reflect the current status of components, systems, services, business' and adversary's activities, as well as effects of alternate courses of action.

8.3.8. Non-Persistence

Non-persistence is the characteristic of providing resources (services, information, connections) only while strictly necessary, being them moved, stopped or deleted.

8.3.9. Privilege Restriction

Privilege Restriction refers to restricting privileges required to use resources as well as those given to users and components, aiming to reduce the damage potential of adversary intrusions.

8.3.10. Realignment

Realignment refers to the process of aligning system resource usage with the necessities of business functions. Realignment aims to reduce attack surfaces by removing nonessential resources from business functions, thus reducing the probability of these resources being used as attack vectors to access or harm critical assets.

8.3.11. Redundancy

Redundancy refers to the intended maintenance of multiple protected instances of critical resources or functionalities. These will work as alternatives (e.g. peak loads, momentary performance requirements) or backups (e.g. failover, damage recovery).

Redundancy has significant synergies particularly with three other cyber resilience techniques:

- **Diversity:** Different technologies (e.g. services, network) are used to provide the same functionality or information;
- **Coordinated Defence:** Different of protection are applied to similar instances;
- **Segmentation:** Distributing instances of a critical resource across different segments.

8.3.12. Segmentation / Isolation

Separation refers to the ability to separate components based on criticality and trustworthiness.

It aims to reduce the attack surface through the applications of physical and/or virtual isolation. Separation also provides the possibility to better and more efficiently protect critical assets, thus reducing cyber security costs.

8.3.13. Substantiated Integrity

Substantiated Integrity refers to the ability to verify that system resources have not been corrupted by an adversary. Various analysis methods are used in substantiated integrity, including:

- **Data validation:** verify if data falls within accepted parameters such as type and range;
- **Business rules validation:** verify if data produced by services or currently stored falls within accepted business or functionality parameters.
- **Integrity validation:** verify if critical data or software were not altered using tamper-evident techniques, such as electronic signatures;
- **Cross validation:** simulate requests to verify if diverse critical services do not present conflicting results.

8.3.14. Unpredictability

Unpredictability refers to the ability to make changes frequently and randomly. Drawing upon diversity, non-persistence and dynamic positioning, these changes can be associated with any part of the system operation. For instance, changing response structure or latency, using different services to achieve the same result, updating access passwords and encryption, changing permitted ports, changing browsers, moving services or data, etc.

9. SECURITY REQUIREMENTS

PROTECTION PROFILE

The work to derive the security requirements is based on the earlier deliverables in the CYRail project. Having a well-defined scenario and risk assessment is necessary to ensure that the security requirements are applicable to the security issues of the railway.

Early on, the attack surface and interconnectivity of different services was identified as a main security issue, which presented a need for separation mechanisms. Rail infrastructure may contain single-purpose or legacy components, whose security depends on isolation. Now these systems risks being vulnerable via interconnected networks. Separation and attack surface reduction were suggested by the mitigation strategies and countermeasures.

The security requirements are specified in a modular Protection Profile. In general, a Protection Profile specifies the security requirements for a certain type of product. ISO/IEC 15408 (also known as Common Criteria or simply CC) is a standard for specifying security requirements and evaluating IT security products against these requirements. The CC does so by providing a common set of requirements for the security functionality (ISO 15408 Part 2) of IT products and for assurance measures (ISO 15408 Part 3) applied to these IT products during a security evaluation. The CC is intentionally flexible, enabling a range of evaluation methods to be applied to a range of security properties of a range of IT products. By having Protection Profiles, the customer knows that evaluated products that have claimed compliance to these Protection Profiles also meet the requirements. The CC also describes what a Protection Profile should include and how it should be structured.

The Protection Profile of the CYRail project specifies the requirements for the network components that shall ensure domain separation and protection of network traffic. The aim is to solve the issue of interconnectivity within large and distributed networked systems. To increase usability of the Protection Profile we looked towards the well-established Protection Profile for Network Devices to draw inspiration from since our requirements would also be applicable to network device. To provide a variety of separation mechanisms we decided to adopt a modular approach and allow for the user to select the desired separation mechanism(s).

The idea of a modular Protection Profile is to specify certain basic functionality as mandatory and then describe additional optional functionality in packages or modules. This has been done for some years in different ways already but was formalized with the CC version 3.1 Release 5 with the concept of Base-PP, PP-Modules and PP-Configurations, as well as the way they can be used to evaluate compliant products.

The deliverable consists of four documents in total. An Introduction and the Protection Profiles. The Protection Profiles consists of a base-PP and two PP-modules:

➤ **The introduction**

An introduction and rationale explaining why, what and how the security requirements were derived for the Protection Profile (PP). The introduction document is intended to improve the understanding for the CYRail project deliverable as well as making the Protection Profile both more accessible and easier to use.

➤ **Base Protection Profile**

The “*Base Protection Profile for Network Separation Mechanisms*” describes the minimum security requirements of a network device that directs data transmitted over computer networks. The PP is intended to act as the Base PP of a PP Configuration. Together with the accompanying PP Modules, said PP Configuration will describe a network device that provides separation of networks and attack surface minimization.

➤ **VLAN Protection Profile Module**

The “*Protection Profile for Network Separation Mechanisms, VLAN Module*” defines the minimum security requirements for Virtual Local Area Network (VLAN) separation. The VLAN separation works at the link layer to create logical broadcast domains to partition and isolate computer networks.

➤ **VPN Protection Profile Module**

The “*Protection Profile for Network Separation Mechanisms, VPN Module*” defines the minimum security requirements for a TOE providing Virtual Private Networks (VPNs) and/or secure communication channels over computer networks. Through these methods, the TOE provides separation of traffic within and outside of said channels.

This was a short summary of the deliverable for security requirements and Protection Profiles. However, as the deliverable is public, please refer to the full documents for further information. The full deliverable is available on the CYRail website: <http://www.cyrail.eu/>.

CONSORTIUM



EVOLEO Technologies LDA,
Portugal



Jakintza Lanezko Ikerkuntza
Investigación Universidad
Empresa, EUSKOIKER, Spain



Fortiss GmbH, Germany



International Union of Railways,
UIC, France



AIRBUS, France



ATSEC Information Security
AB, Sweden

Contact us

info@cyrail.eu
www.cyrail.eu