Cyber-Physical Security Risk Assessment for Train Control and Monitoring Systems

Mouna Rekik, Christophe Gransart, Marion Berbineau

Cyber-Physical Security Risk Assessment for Train Control and Monitoring Systems

Mouna Rekik*, Christophe Gransart* and Marion Berbineau†
*Univ Lille Nord de France, IFSTTAR, COSYS, LEOST, F-59650 Villeneuve d'Ascq, France,
{mouna.rekik, christophe.gransart}@ifsttar.fr
†Univ Lille Nord de France, IFSTTAR, COSYS, F-59650 Villeneuve d'Ascq, France, marion.berbineau@ifsttar.fr

***Abstract*—Future railway systems should bring convenience to people's lives. In fact, due to the move away from bespoke stand-alone systems to open-platform, standardized equipments and increasing use of networked control and automation systems and connected technologies, the efficiency and the safety of railway services are improving. However, this dependence of automation, control and communication technologies makes railway systems becoming increasingly vulnerable to cyber-attacks and security threats which affects the overall performance. This paper deals with cybersecurity concerns facing these systems. As such, we analyse characteristics of railway threat landscape. Then, we discuss the direct impacts of the identified potential threats and their consequences on the whole system and we evaluate resulted risks. For space limitation, we choose to present the impact, likelihood and risk analysis for one functionality of the system, namely External Door control (EDC). Some good practices and related techniques for the development of safer, more comfortable, and more secure future railway systems are also discussed.**

***Index Terms*—TCMS, Cyber-Physical Security, Risk Assessment, Threat, Vulnerability, ISA/IEC 62443**

I. Introduction

The Train Control and Monitoring System (TCMS) is the main part of the control system of a train. It provides a control and monitoring infrastructure that enhances train operations and increases its safety and reliability. The integration of Information and Communication Technologies (ICTs) into the TCMS will improve efficiency of the railway rolling stock industry as it enables the implementation of innovative solutions, services and applications in the quest for smarter, safer and more efficient railway transportation systems. The new generation of trains will use real-time rail information and online environmental data in combination with on-board references to achieve optimal control of the train traction and braking while keeping with travel schedule and reducing energy consumption. Likewise, train passengers travelling experience will be improved through services such as connected infotainment, real-time information, etc.

Nevertheless, the process of increasing the incorporation of ICTs into railway systems presents a growing dilemma. On one hand, this innovation has become an urgent need to maintain a competitive edge comparing to other transportation systems. On the other hand, the introduction of networked devices, remote access and control capabilities, especially with the emergence of wireless communication systems as alternatives to supplant wired systems in the railway industry, all acts to increase the system exposure to cyber-threats. While cyber-technology is complex and fast evolving, cyber-attacks are also becoming increasingly automated and sophisticated. Their impact on critical infrastructures in particular railway systems, can lead to catastrophic consequences, no matter whether they are the intended target or not. Attacks on operational systems could lead to the disruption or the unavailability of the rail transport itself. When informational systems are attacked it can lead to the unavailability of services for the passenger, like being unable to buy a ticket or digitally check a ticket into the system. Consequently, cyber-attacks on the transportation sector create a large impact on society and people's daily life varying from direct effects such as delays, accidents, injuries or even deaths, to indirect effects, such as socio-economic effects.

The work presented in this paper is conducted within the European project ROLL2RAIL under the task *security for* TCMS that aims to identify convenient security countermeasures and to define required protection levels of TCMS assets. Yet, such outcomes can be accomplished using a coherent and strategic approach that encompasses all cybersecurity aspects. In ROLL2RAIL, the selected approach is defined by the standard ISA/IEC-62443 [1]. Due to space limitation, in this paper, we present the cyber-physical security risk assessment of one functionality of TCMS, namely the external door control. This analysis aims to identify system threats, quantify impacts and expected losses. The proposed countermeasures and mitigation techniques are not presented because they are classified.

The remainder of this paper is structured as follows. Section II shortly introduces the methodology selected to establish a security risk assessment for TCMSs. Then, in section III, we identify the System under Consideration (SuC) for the security risk assessment. Next, in section IV, railway threat landscape is discussed through threat and vulnerability assessments. In section V, we present an impact, likelihood and risk analysis of potential threats against the SuC. Finally, in section VI, we review some good practices to be used in transportation system in order to minimise the identified risks.

II. Risk Assessment Methodology

Traditional information systems security is usually based on CIA principle, standing for Confidentiality, Integrity and Availability by priority order. However, for Industrial Automation Control System (IACS) such as TCMS, the priority is generally reversed depending on the specificities of the considered system. For railway systems, the most important aspect is the train movement, for that, security concern is first integrity, then availability and finally confidentiality. In fact, loss of integrity could lead to accidents or collisions, whereas loss of availability would bring the railway system to a halt. Loss of confidentiality is less of an immediate threat, but might result in the leak of sensitive operational information. As such, standards and methodologies developed for traditional information technology systems cannot be applied directly. This issue has received attention not only from researchers, but also from public authorities and standard committees during the last few years. Thereby, several information security standards have

been proposed to address security issues for the particular case of IACS such as ISO/IEC 27000 [2], ISO/IEC 15408 Common Criteria [3], ISA/IEC 62443 [1], EN 50159 [4], RFC 2196 [5], ETSI TS 102 165 [6], German standards like DIN VDE V 0831-102 [7] and DIN VDE V 0831-104 [8], US standards like FIPS PUB 199 [9], FIPS PUB 200 [10] and NIST Special Publications (SP) like SP 800-37 [11], SP 800-53 rev. 4 [12], *etc*. An extensive study on Security standards and guidelines for IACS is available in [13]. From these security standards, ISA/IEC 62443 is considered as the most important one for ROLL2RAIL project. The ISA99 committee, which is responsible for generating the specifications, has made great efforts to bring together numerous standards and recommendations that exist and then to create a comprehensive set of documents that is consistent and broadly applicable in virtually any industrial sector. This and the fact that these specifications have now been recognized by industry worldwide through simultaneous adoption by the IEC give the ISA/IEC 62443 series a strong chance to be a single definitive set of international standards for IACS cybersecurity. This is also testified by the fact that it is recognized as pivotal security standard for Industry 4.0 project[14] and that it will be adopted by CENELEC [15].

The standard ISA/IEC-62443 [1] provides guidance to improve electronic security and help reducing the risk of compromising confidential information or causing degradation or failure of the equipment (hardware and software) of systems under control. Thereby, ISA/IEC-62443 improves the availability, integrity and confidentiality of components or systems used for industrial automation and control, thus it enables the implementation of secure IACS.

The security risk assessment methodology proposed by ISA/IEC-62443 is composed of 13 steps, as presented in Fig. 1. The identification of the SUC is the first step of the methodology. It consists of a functional and design specification phase that aims to identify physical and Information Technology (IT) assets of the system. Step 2 and 3 address the system threat landscape through threat and vulnerability assessments. Once potential threats and system vulnerabilities are identified, their direct impacts and cascading consequences on the whole system should be studied in step 4. Then, the likelihood of each identified threat should be determined in step 5. Step 6 consists of the calculation of the unmitigated risk in a risk matrix using determined likelihood and impact levels. In step 7, the risk created by each identified threat should be evaluated based on the risk matrix. In step 8, countermeasures should be identified to mitigate risks evaluated unacceptable. Then, likelihoods and risks should be re-evaluated in order to measure the effectiveness of proposed solutions. In case some risks are still evaluated unacceptable, a set of additional countermeasures should be proposed and then step 9 and 10 should be repeated until all risks become acceptable. At the end, the security risk assessment should be closed by a documentation phase.

In this paper, we present the security risk assessment of EDC functionality based on the IEC 62443 methodology.

III. SYSTEM IDENTIFICATION

In this section, we present the system under consideration for the security risk assessment.

A. *Train Control and Monitoring System (*TCMS*)*

The TCMS of a train is mainly responsible for providing basic train control functions, such as inaugurating the train

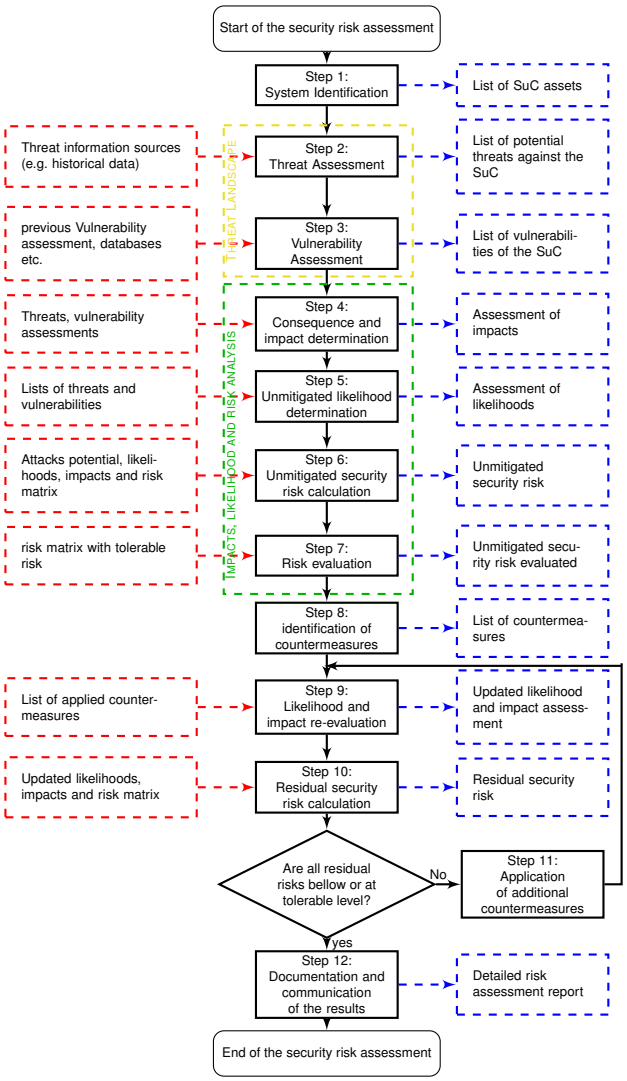

Fig. 1: ISA/IEC-62443 security risk assessment methodology

network, determining train topology and configuration, providing orientation information for coupled elements, managing leading vehicle information, distributing train topology and configuration, confirming train configuration, managing train network operation, managing train network access and transmitting data. Nevertheless, with the integration of advanced ICT in the railway industry, the TCMS is expected to manage a set of sophisticated applications not only for a more reliable train control, but also for operator oriented services and customer comfort purposes. For operational and security purposes, control system ICT should be separated from comfort ICT, as such the TCMS is clustered into 3 functional domains [16][17][18][19]:

- Train Control and Monitoring System (TCMS) domain includes both safety related and non-safety related TCMS functions. The functions of this domain are mandatory to ensure safe train movement and to ensure carrying the payload, such as : main control, train radio, air conditioning, propulsion, brakes, electricity, lavatories, lighting, supporting systems, passenger announcement system, external doors and internal doors, European Train Control System (ETCS), Automatic

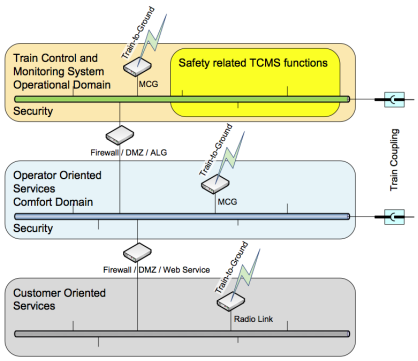

Fig. 2: SUC functional domains based model[16]

Train Protection (ATP), On-board Driving Data Recording System (ODDRS), passenger alarm system and Closed-circuit television (CCTV) for rear view purposes.

• Operator Oriented Services (OOS) domain is where all auxiliary services for proper train operation are considered, such as : priority logic, CCTV for video surveillance purposes, infotainment in train embedded devices, mobile phone amplifiers, automatic passenger counting,vehicle positioning, fare management or ticketing, driver assistance system, E-schedule, diagnostics and Condition Based Maintenance (CBM) systems and Passenger Information System (PIS) (including automatic announcements).

• Customer Oriented Services (COS) domain includes the functions executed by passenger devices such as: access for the passenger's devices (e.g. Wi-Fi access points), Access to the public internet and passenger info-portal.

This three-level modelization, presented in Fig. 2, aims to increase the system flexibility, scalability, and adaptability for future evolutions.

To accomplish all functionalities mentioned above, system actors and devices need to exchange data and commands using communication networks in different communication schemes such as intra-train, train-to-train and train-to-ground communications. Communication networks for future railway systems are expected to be heterogeneous composed of a mixture of several networks and radio access technologies that can be simultaneously accessed by different system actors and devices in order to improve the capacity for communications. For instance, ROLL2RAIL proposes the use of an heterogeneous network architecture combining wireless technologies, such cellular network like LTE, IEEE 802.11, RFID and wired networks where the advantages and specificities of each access network can be taken into consideration [17]. For safety and security purposes, access between different domains will be limited. Indeed, as shown in Figure 2, the proposed architecture includes also additional network protection devices between different functional domains.

B. External Door control function

Due to space limitation, in this paper, we focus on presenting impact, likelihood and risk evaluation (from step 4 to step 7 in the risk assessment methodology) only for EDC system from TCMS domain. As such, in this section, we provide a detailed description of EDC system.

Based on IEC-61375 Standard [20], a distributed train functionality is accomplished using several function interfaces installed within the train in an hierarchical way aiming to remotely control processes.

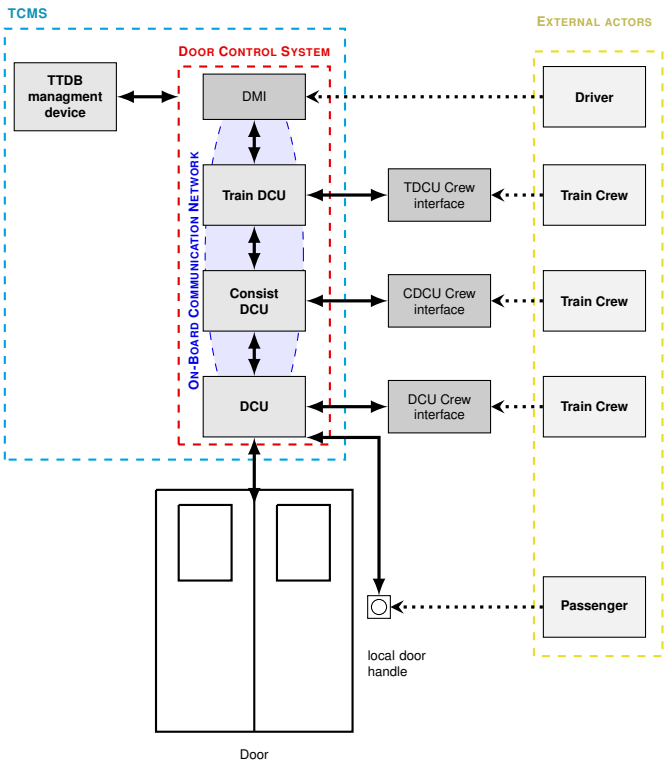

Fig. 3: Door Control System

• one Function Leader (FL) which is responsible to control the function by stimulation of the Function Followers (FFs) (sending commands) and to receive the reactions from the FFs (receiving status);

• one or more Function Follower(s) (FF), at most one per consist network, which is responsible to receive the commands from the FL and to stimulate the Function Devices (FDs). The received reactions from the FDs are cumulated by the FF and provided as function status of the consist to the FL;

• one or more Function Device(s) (FD), which are receiving the commands from the FF, execute the function operations and report the results to the FF.

These parts of the application are distributed over the consists of the train. Different parts of the application in different consists can communicate only via the Train Control Network (TCN).

Likewise, EDC, being a distributed train application, has the same architecture defined above. As presented in Figure 3, the EDC system is controlled by the TCMS through interfaces provided by the Train Door Control Unit (DCU). The Train DCU is then the function leader, it is the controlling part for all doors in the train. The Consist DCU is the function follower, it is the agent for one consist. The DCU is the function device, it is responsible for the physical door. The Door is the physical device dedicated to the DCU. In addition to automatic control interfaces, EDC system parts can be manipulated manually using crew interfaces for maintenance purposes or in case of malfunctioning problems.

IV. RAILWAY THREAT LANDSCAPE

A. Threat Assessment

In this section, we study potential threats against TCMS and their characteristics. As such, we present a threat taxonomy that

covers mainly cybersecurity threats; which are threats directly applied to ICT assets and thus affecting TCMS operations. We also present non-IT threats to cover threats to TCMS physical assets that are necessary for the system operation. Based on several recent studies published by European Union Agency for Network and Information Security (ENISA) [21][22][23], we identify potential threats against TCMS. These threats can be classified into the following categories:

• **Physical attacks**. This type of threats is caused by intentional offensive actions aiming to achieve maximum distraction, disruption, destruction, exposure, alteration, theft or unauthorized accessing of assets such as hardware or ICT connections.

• **Unintentional damages**. These are caused by accidental insider actions[24] including human errors[25]. Unintentional mistakes can be made by authorized employees, users, developers, and testers during data entry, operations, or application development. Such errors can affect the system integrity and stability .

• **Outages and disasters**. This category contains unexpected disruption of services due to outages and disasters including natural and environmental disasters not triggered by human.

• **Failure and malfunctions**. This category covers unexpected failure or disruptions of devices or systems including hardware, software and ICT connexions failure or malfunctioning.

• **Eavesdropping/Interception/Hijacking**. This type of threats contains cyber-attacks and intentional malicious activities or abuse targeting digital assets of a system. Threats from this category consists of altering communication between two parties. These attacks do not have to install additional tools/software on a victim's site.

• **Nefarious activities**. This category also contains cyber-attacks and intentional malicious activities or abuse targeting digital assets of a system. However, attacks belonging to this category usually require the use of tools by the attacker. As such, the threat is accomplished through the installation of additional tools/software or performing additional steps on the victim's IT infrastructure/ software.

The identified threats can be conducted by several types of actors with different motivations. They can be :

• **Nation states** targeting other nations critical infrastructures, including railway systems. In fact, these systems provide essential services for a nation's society and serve as the backbone of its economy, security, and health. As such, they become a significant target in modern cyber-warfare. Attacks performed by such actors can be politically or economically motivated.

• **Non-state organized threat groups** including cyber-terrorists, cyber-fighters and cyber-criminals. Common to all these threat actors is that they can be organized on local, national or international level. However, their motivations and skill level vary. Cyber-terrorists have political or religious motivations and their capability varies from low to high. Whereas, cyber-fighters are patriotic motivated groups of citizens with strong feelings when their political, national or religious values seem to be threatened by another group and are capable of launching cyber-attack to protest and . Cyber-criminals are organized groups with quite high skill level that attack systems for financial gain.

• **Insider threat agents** including employees (staff, contractors, operational staff) and third party (vendors, system integrators, and other third party service and product providers) are considered as dangerous threat actors since they have insider access to private facilities and resources and a significant amount of knowledge that allows them to place effective attacks against sensitive parts of the system.

• **Hacktivists** who are attackers, in many cases with limited technical skills, but rely on ready-to-use attack kits and services, or even third-party botnets, to cause damage to a system e.g., denial of service, defacement as a means of protest. Their protests are often politically motivated.

• **Business-oriented attackers** interested in performing abusive activities against competitor-controlled cyber-physical systems in order to cause concrete damage and gain business advantages.

• **Casual cyber-attackers** with little or no technical skills, launching attacks against connected systems and causing serious damage, especially when it comes to connected control systems. It is important to note that individual non state attackers (such as hacktivists, business-oriented attackers and casual attackers) could also be considered by nation states as allies in a low intensity warfare against an opponent nation.

The aforementioned actors are driven by several categories of motivations. We identify two main motivations:

• **Political purposes**. Since railway systems are part of a nation critical infrastructure, attacking them is considered as a strategical warfare weapon that may cause severe consequences varying from endangering people lives to financial loss and economical impacts. As these systems become increasingly reliant on ICT, they merge as a important target for political motivated cyber attacks. These warefare strategies are already used and they have been multiplied in the few past years. They can be used to cause physical damage or exfiltrating intelligence or secret information. Some well-publicized example is the attack conducted on Iranian Nuclear Facilities by using the worm Stuxnet[26]. According to [27], Stuxnet was launched by the US and Israel several years ago, in an attempt to sabotage Iran's nuclear program. Actors such as nation states and hacktivists fall in this category.

• **Financial purposes**. Transportation systems, including railway systems, are the backbone of national economies, providing connections for people and goods, access to jobs and services, and enabling trade and economic growth. Attacking such systems results in financial loss to the service providers, but also cascading consequences on other domains. At railway operator level, attacks can be financially motivated in order to cause business disruption and sales loss. This can cause significant long-term economic impact when reputation of the operators and trust of customers are impacted[28]. Financial motivated attacks are usually performed by business-oriented actors, but also by nation states actors driven by economic reasons. This category of motivation also existed before critical infrastructures became an appealing and sensitive target.

B. Vulnerability Assessment

The integration of cyber-physical systems into critical infrastructures brings not only benefits but also a new set of vulnerabilities for the whole system. The exploitation of such cyber-vulnerabilities can lead to physical consequences. Based on [23], we identify vulnerabilities of railway systems. These vulnerabilities are divided in two categories:

1- General vulnerabilities for IACS

• Wireless and cellular communications. Although such communication technologies brings several advantages to the system, they introduce typical vulnerabilities because communications take place 'through the air' using radio frequencies and

thus it is difficult to prevent physical access to them, especially in open and accessible areas like public railway infrastructure. Risk of attacks such as interception and intrusion is greater than with wired networks.

• Increasing system automation. Although automation control improves safety and global system operations by removing possibility of human error, it introduces new vulnerabilities since the surface of attacks increases and therefore risk of attacks increases.

2- Specific vulnerabilities for railway use case

• Scale and complexity of railway systems. Railway infrastructure is a large-scale international infrastructure. Applying networked technologies across large railway systems increases number of access points to the system, and thus increases the difficulty and cost. Thereby, securing communications and connectivity between mobile devices on large area is a complicated task.

• Cohabitation between legacy and new systems. Since railway infrastructure is a shared common infrastructure used by different railway companies, the use of legacy equipments and infrastructures introduces new vulnerabilities.

• Multiple independent systems. In addition to legacy problems, railway systems are composed of diverse systems such as sensors, computers, payment systems, emergency systems. It is crucial, but difficult, to ensure smooth interfacing, communication and securing between such independent and heterogeneous systems. This increases vulnerabilities.

• Access to real-time data. Reliable operation of the system requires a non-stop real-time data exchange which may result in costly maintenance and periods of service downtime.

• Online passenger services such as timetabling, passenger information, ticket booking, are also susceptible to cyber attacks.

V. Impacts, likelihood and risk analysis

A. Impacts and Consequences Determination

A risk [29] is the potential that a given threat will successfully exploit vulnerabilities and thereby produce a negative impact on the system such as confidentiality and privacy problems for the passengers (since the system uses sensing, tracking, real-time behaviour evaluation and automated decisions), interruption and disturbance of transport services which, in addition to dissatisfaction of passengers and disruption of their daily lives, can have secondary consequences on other sectors, loss of revenue, reputation and customers trust, etc[23]. However, the most critical impact is when passengers health and safety are affected. In fact, passengers safety is the priority to all railway systems actors, nonetheless, some incidents may endanger health and safety, not to mention threats coming from terrorism that need to be accounted for when protecting railway systems and infrastructure.

In this step, we investigate impacts of potential threats identified in section IV-A. Table I studies, for each threat, direct impacts and unwanted incidents created on the attacked component and the cascading consequences on the EDC.

The identified impacts can affect one or many areas. We distinguish 3 categories of risk based on the impacted area [30]: safety, financial and operational risks. For each category, we define 3 levels of severity. Regarding the impact determination, we used the method presented in [31] with some modifications. According to [31], the consequences in each of category are ranked, as shown in Table II, according to their severity level. Decimal power scaling was used for the rating of the severity of consequences assigning them the impact value to distinguish between the severity of consequences both within each area and between areas.

The total impact is calculated as follows:

$$Impact = Impact_{Safety} + Impact_{Financial} + Impact_{Operational} \quad (1)$$

For evaluating the impact, we use a qualitative scale, presented in Table III, taken from [31].

B. Unmitigated likelihood determination

The calculation of the likelihood is a major challenge, it is usually accomplished using the Attack Potential (AP) calculation method specified by the standardized method Common Criteria [32] which is also used by the ETSI TVRA [33] and in the risk analysis approach described in [31]. Following this approach, the attack likelihood is determined in two steps: first, determining the AP and then, mapping of the AP to a likelihood. Determining the AP consists of measuring the effort required to mount a successful attack against the considered system. It is assumed that the higher is the AP the lower will be the likelihood of a successful attack. The factors considered in the identification the AP and their ranges and values are listed in Table IV (based on [32]).

Then, the accumulated attack potential is calculated as follows:

$$AP = AP_{time} + AP_{expertize} + AP_{knowledge} + AP_{access} + AP_{equipment} \quad (2)$$

After AP calculation step, we move to AP/likelihood mapping step. To this end, five levels are defined to rate the calculated AP. The rating is done following the approach described in [32]. The AP levels and their mapping to the qualitative scale for the likelihood are shown in Table V.

In New Dependable Rolling Stock for a more Sustainable, Intelligent and Comfortable Rail Transport in Europe (ROLL2RAIL) project, the likelihood, presented in Table VII was determined by estimation, because the lack of information about actual conducted attacks on similar systems does not allow calculating the AP.

C. Unmitigated security risk calculation

The unmitigated cybersecurity risk is determined by means of the risk matrix, presented in Table VI, which was defined specifically for the TCMS cybersecurity risk assessment within the ROLL2RAIL project [34]. The risk matrix is used to calculate the resulting level of risk (Likelihood x Impact) and to identify whether it is acceptable or not. In railway systems, a risk is considered as unacceptable in case its level is major or critical, and as acceptable in case its level is minor or negligible [34].

The risk matrix also helps in the suggestion of mitigation solutions. In fact, the countermeasures should be deployed in a way to reduce the threat likelihood but never the impact that it could have in the system. As such, if a threat poses an unacceptable risk, we must move in the matrix to the nearest

TABLE I: Impact Analysis for External Door Control functionality (With Train Lines Safety functions)

Threat class	Threat ID	Threat	Description	Asset	Cascading effects
PHYSICAL THREATS	PT01	Vandalism	An attacker could unplug the Access Point from the network or power-off the access point	On-Board Communication Network	DMI is not able to receive information about doors status. The driver cannot receive information from DMI to ensure that doors are in the right status (such as to verify that all doors are closed before start moving). The driver is not able to command door system, the commands are blocked at the (TDCU- CDCU) level (at the wired level). This also means that the other consists can be out of the control. As such, for safety reasons, the train Line locks the doors. The passengers cannot go out of the train until the doors are opened manually.
	PT02	Vandalism	An attacker could damage door sensors	Door sensors	The door control system can not know the state of the concerned door. The damaged door is locked and cannot be used until it is opened manually.
	PT03	Unauthorized physical access/ Unauthorized entry to premises	An unauthorized person controls the doors of the train by direct manipulation of the DMI	DMI	If the attacker tries to open a door, the Train Line locks it and does not allow opening it when the train is moving. If he tries to send continuously "close" commands to the door so the passengers cannot go out of the train until the doors are opened manually.
	PT04	Unauthorized physical access/ Unauthorized entry to premises	An unauthorized person can manipulate the door control system through TDCU Crew interface.	TDCU Crew Interface	If the attacker tries to open a door, the Train Line locks it and does not allow opening it when the train is moving. If he tries to send continuously "close" commands to the door so the passengers cannot go out of the train until the doors are opened manually.
	PT05	Unauthorized physical access/ Unauthorized entry to premises	An unauthorized person can manipulate the door control system through CDCU Crew interface.	CDCU Crew Interface	If the attacker tries to open a door, the Train Line locks it and does not allow opening it when the train is moving. If he tries to send continuously "close" commands to the door so the passengers cannot go out of the train until the doors are opened manually.
	PT06	Unauthorized physical access/ Unauthorized entry to premises	An unauthorized person can manipulate the door control system through DCU Crew interface.	DCU Crew Interface	If the attacker tries to open a door, the Train Line locks it and does not allow opening it when the train is moving. If he tries to send continuously "close" commands to the door so the passenger cannot go out of the train until the doors are opened manually.
	PT07	Unauthorized physical access/ Unauthorized entry to premises	An attacker could damage the DMI	DMI	The door control system cannot be controlled through DMI. Door control services are inaccessible for the driver. Doors can not be remotely controlled by the driver. In such circumstances,doors are locked by the Train Line and cannot be used until it is opened manually.
UNINTENTIONAL DAMAGE	UD08	Erroneous use or administration of devices and systems	An employee may accidentally enter erroneous use or bad administration of door control system in the maintenance phase.	EDC system	A bad or erroneous administration and configuration of the system may lead to erroneous actions and/or improper monitoring commands. In this case, the whole door control system could stop working, doors could be blocked at their current status. The train cannot move until the door control system is fixed. Such incident may also lead to increase cyber-physical vulnerabilities of the systems and create entrance points for other potential threats.
	UD09	Using information from an unreliable source	Erroneous configuration,installation or maintenance data may be used from unreliable sources	EDC system	This can lead to malfunctioning of the door control system or stopping it completely. Doors could be blocked. The train cannot move until the door control system is fixed. Such incident may also lead to increase cyber-physical vulnerabilities of the systems and create entrance points for other potential threats.
	UD10	Unintentional change of data in the system or destruction of records	recorded data about the state of the system may be changed or deleted	EDC system	The system usually records data about system functioning at the aim to using them not only for maintenance purposes, but also to strengthen the system against the problems and incidents occurring during operation. such incident leads to loss of operational data.
FAILURES/MALFUNCTION	FM11	Failure of device or systems	In case of a hardware failure in DMI and/or TDCU, the driver is not able to command the whole door system. For TDCU crew interface hardware failure, the crew is not able to isolate specific consist from door operation. In the both cases, the failure is at the train level.	DMI, TDCU and/or TDCU crew interface	The train Line locks the doors. The passengers cannot go out the train until the doors are opened manually.
	FM12	Failure of device or systems	In case of a hardware failure in CDCU, the driver is not able to command the door system at the concerned consist. For CDCU crew interface hardware failure, the crew is not able to lock or release doors in specific vehicle of the consist concerned.	CDCU and/or CDCU crew interface	The system may be locally affected, doors at the failed consist cannot be controlled. The train Line locks the doors of the a ected consist. The passengers cannot go out the consist until the doors are opened manually.
	FM13	Failure of device or systems	Hardware failure: DCU and/or DCU crew interface	DCU and/or DCU crew interface	The door connected to the failed DCU fails. The train Line locks the affected door. The door cannot be used until it is opened manually
	FM14	Failure or disruption of communication links	Software or Hardware failure	On-Board communication network	No data exchange. DMI can not receive any information about doors status. The driver cannot receive information from DMI to ensure that all doors are closed before start moving as such the train cannot move. Commands are also blocked at DMI-TDCU level, the driver is not able to command the door system. For safety reasons, the train Line locks the doors. The passengers cannot go out of the train until the doors are opened manually.
OUTAGE	O15	Network outage	Outage of cable or wireless network	On-Board communication network	No data and monitoring commands exchange between door control system entities. DMI cannot receive any information about doors status. The driver cannot receive information from DMI to ensure that all doors are closed before start moving as such the train cannot move. Commands are also blocked at DMI-TDCU level, the driver is not able to command the door system. In case the train is moving, the driver is also unable to command the door system, as such, for safety reasons, The train Line locks the doors. The passengers cannot go out of the train until the doors are opened manually.
EAVESDROPPING	E16	Network Reconnaissance, Network traffic manipulation and Information gathering	Malicious activities my be performed at the aim to identify information about network to find security weaknesses	On-Board communication network	An attacker may learn about weaknesses of the network and use them to disturb the door control system or disconnect its assets.
	E17	Man in the middle / Session hijacking	An attacker can conduct a MiTM attack, sniff the data and command traffic exchanged between different Door control system entities. As such, he can reveal content of door command and status messages (on train level)	On-Board communication network	Operational information could be released.
	E18	Man in the middle / Session hijacking	An attacker may send a falsified door command on the train level (to the TDCU)	On-Board communication network - TDCU	The Train Line locks the doors and does not allow opening them when the train is moving. If the attacker tries to send continuously "close" commands to the door so the passenger cannot go out of the train until the doors are opened manually.
	E19	Man in the middle / Session hijacking	An attacker may send falsified door status information to DMI and/or TDCU. The driver receive an erroneous information about door status.	On-Board communication network - DMI - TDCU	The driver receives a false doors open signalisation, as such he cannot move the train until the DMI notify him that all doors are closed.
	E20	Man in the middle / Session hijacking	An attacker may send a falsified door command on the consist level (to the CDCU)	On-Board communication network - CDCU	The Train Line locks the doors and does not allow opening them when the train is moving. If the attacker tries to send continuously "close" commands to the door so the passenger cannot go out of the train until the doors are opened manually.
	E21	Man in the middle / Session hijacking	An attacker may send falsified door status information to CDCU (on consist level). The driver receive an erroneous information about door status at the attacked consist.	On-Board communication network - CDCU	The driver receives a false information about the doors of the attacked consist are opened, as such he cannot move the train until the DMI notify him that all doors are closed.
	E22	Man in the middle / Session hijacking	An attacker may send a falsified information about actual train/consist composition, or actual train backbone status to TDCU or CDCU (such as erroneous train orientation)	On-Board communication network - TDCU - CDCU	The Train Line locks the doors to not allow opening external doors from the wrong side in the station. If the attacker tries to send continuously "close" commands to the door so the passenger cannot go out of the train until the doors are opened manually.
	E23	Man in the middle / Session hijacking	An attacker may send a falsified door command on the individual door level (to the DCU)	On-Board communication network - DCU	The Train Line locks the doors and does not allow opening them when the train is moving. If the attacker tries to send continuously "close" commands to the door so the passenger cannot go out of the train until the doors are opened manually.

Continued on next page

Impact Analysis for External Door Control functionality With Train Lines Safety – continued from previous page

Threat class	Threat ID	Threat	Description	Asset	Cascading effects
	E24	Man in the middle / Session hijacking	An attacker may send falsified information about train speed to DCU. The doors can be released during train movement or the doors cannot be released when the train stops.	On-Board communication network - DCU	The Train Line locks the doors and does not allow opening them when the train is moving. If the attacker tries to send continuously "close" commands to the door so the passenger cannot go out of the train until the doors are opened manually.
Nefarious Activity	NA25	Denial of Service	An Attacker can conduct Distributed Denial of network service (DDoS) attack at the network layer using several techniques as Protocol exploitation, Malformed packets, Flooding,Spoofing. He can conduct a DDOS attack at the application layer using techniques like Ping of Death, XDoS, WinNuke. He can conduct DDoS attack to both network and application services using amplification/ reflection methods i.e. NTP, DNS .Such type of attack aims to disconnect the network (communication disruption) or degrade the performance of the network, to abuse of resources, to alter network configuration or even physically destroy or alter network components.	On-board communication network	DMI is not able to receive information about doors status. The driver cannot receive information to ensure that doors are in the right status. The driver is also not able to command door system. Door system is out of the control. As such, for safety reasons, the train Line locks the doors. Passengers cannot go out of the train until the doors are opened manually.
	NA26	Malicious code/ software/ activity	An Attacker can access to the network and inject a malicious code, or install a malicious software to conduct a malicious activity within the system. The attacker can use several techniques such as abuse of resources, Worms / Trojans, Rootkits, Elevation of privileges, Viruses, Rogue security software / Rogueware / Scareware, Exploits/Exploit Kits	Door control system	The malicious code or software allows for conducting malicious activities and thus disturbing the system by altering configuration, manipulating data and monitoring commands, disrupting services, disrupting the whole system, changing doors states (unsafe states) or blocking them. The system can also be remotely controlled by attacker using such techniques. If the system detects an abnormal functioning of EDC, the Train Line locks the doors to allow opening them when the train is moving. If the attacker tries to send continuously "close" commands to the door so passengers cannot go out of the train until the doors are opened manually.
	NA27	Identity Fraud	An Attacker can conduct malicious identity theft actions. This can be done using identity theft malicious computer programs such as credentials- stealing trojan	Door control system	Identity Fraud actions allow attackers to access to the door control system with more advanced privileges such as administrator and thus allow them to commit unauthorized activities such as unauthorised use or administration of devices and systems, unauthorised use of software, unauthorized changes of records. If the attacker attempts to open external doors in an appropriate conditions, the Train Line locks the doors to not allow opening them when the train is moving. If the attacker tries to send continuously "close" commands to the door so passengers cannot go out of the train until the doors are opened manually.
	NA28	Manipulation of hardware and software	An attacker can maliciously manipulate hardware and software components of the door control system. Such attacks are done by taking advantages of some IT vulnerabilities, accessing to device software (it could also be done through modifications of code or data, attacking its integrity), or by accessing directly to hardware	Door control system (Network, software and hardware)	Loss control of the system, all door control system components can be damaged. The door control system is disrupted. For safety reasons, the train Line locks the doors. Passengers cannot go out of the train until the doors are opened manually.
	NA29	Manipulation of information	An attacker can maliciously manipulate recorded data about the state of the system. He can also alter system configurations	Door control system	This can lead to loss of data for maintenance and control purposes, malfunctioning of the system in case of altering configuration data which can lead to serious problem and endanger the safety of train and passengers. For safety reasons, the train Line locks the doors. Passengers cannot go out of the train until the doors are opened manually.

TABLE II: Determination of Impact value

Impact Area	Severity level	Description	Impact Value
Safety	1	Life-threatening injuries (survival uncertain), fatal injuries and/or extreme damage to the environment	10000
	2	Severe and life-threatening injuries (survival probable) and/or large damage to the environment	1000
	3	Light and moderate injuries and/or minor damage to the environment	100
	4	No injuries	0
Financial	1	Existence-threatening financial damage and/or the incident will incur people suing the company, severe impact to the public image of the company	1000
	2	Substantial financial damage, but yet not existence-threatening and/or the incident may have a serious impact on the public image of the company	100
	3	Undesirable financial damage and/or the incident may have an impact on the public image of the company	10
	4	No or tolerable financial damage	0
Operational	1	Train unusable, *i.e.*, one or more fundamental functions are affected. The train usage is infeasible.	100
	2	Service required, *i.e.*, an important function is affected. The train/vehicle can be used only with massive restrictions	10
	3	Comfort affected. The vehicle can be used with some restrictions	1
	4	No relevant effects, i.e., at most, an unimportant function is affected and the train/vehicle can be used without restrictions.	0

TABLE III: Impact level

Impact Value	Impact Level
$0-2$	Insignificant
$3-21$	Medium
$22-210$	Critical
>210	Catastrophic

TABLE IV: Attack potential factors, ranges and values

AP Factor	Description	Range	Value
Elapsed Time	The time needed by an attacker to identify a particular potential vulnerability, to develop an attack method and to sustain effort required to perform the attack against the target.	Hours	0
		Days	1
		Weeks	3
		Months	7
Expertise	Level of knowledge of the underlying principles, product type or attack methods.	Layman	0
		Proficient	3
		Expert	6
		Multiple experts	8
Knowledge of Target	Level of target related knowledge needed to perform the attack.	Public	0
		Restricted	3
		Sensitive	7
		Critical	11
Access	Level of access to the target system needed to perform the attack.	Unnecessary or unlimited	0
		Easy	1
		Moderate	4
		Difficult	10
Equipment	Equipment required to identify or exploit the vulnerability and to perform the attack.	Standard	0
		Specialized	4
		Bespoke	7
		Multiple bespoke	9

TABLE V: Likelihood level

AP Value	AP Level	Likelihood Level
$0-9$	Basic	Certain
$10-13$	Enhanced Basic	Likely
$14-19$	Moderate	Possibly
$20-24$	High	Unlikely
>24	Beyond High	Remote

"Acceptable" cell in the vertical direction. To reduce the impact a change of the architecture of the system is necessary. According to this risk matrix, any catastrophic impact shall be avoided by design (introducing additional systems in the system architecture) because independently of the likelihood level the risk would be unacceptable.

TABLE VI: Risk matrix

Likelihood Level	Risk Level			
Certain	Unacceptable	Unacceptable	Unacceptable	Unacceptable
Likely	Acceptable	Unacceptable	Unacceptable	Unacceptable
Possibly	Acceptable	Unacceptable	Unacceptable	Unacceptable
Unlikely	Acceptable	Acceptable	Unacceptable	Unacceptable
Remote	Acceptable	Acceptable	Acceptable	Unacceptable
	Insignificant	Medium	Critical	Catastrophic
	Impact Level			

D. Risk evaluation

When conducting a risk assessment, impacts on the system should be determined without any additional protection system in order to evaluate the real consequences. For the specific case of railway systems, the train operates necessarily with an additional protection control called Train Lines. Train Lines consists of a set of safety functions that aims to protect the train especially in case of abnormal functioning.For example, for EDC, Train Lines system adds doors locking and releasing functions which reduces considerably impacts of the system malfunctioning and especially avoid catastrophic ones.

In the context of ROLL2RAIL, we evaluated impacts of cyber-physcial threats identified in step 2, on the system for

both cases; with and without Train Lines safety functions. We started by studying impacts and consequences with Train Lines safety functions transparent. We noticed that all impacts are evaluated critical or catastrophic (mostly catastrophic). These catastrophic impacts according to the risk matrix, presented in Table VI, cannot be avoided independently the likelihood of the threat. Therefore, the only way to avoid this case is to change the evaluated architecture by taking into account the existence of Train Lines. As such, for the current analysis, we are conducting the security risk assessment including the Train Lines, therefore reducing the impact of security threats and making able to set these threats in an acceptable risk level by introducing new countermeasures in the SuC. Likewise, the impacts presented in Table I are also identified with consideration of Train Lines safety functions.

TABLE VII: Risk Analysis for External Door Control functionality With Train Lines Safety

Threat ID	Impact Area	Severity	Impact Value	Resulting Impact Value	Impact Level	Likelihood Level	Risk Level
PT01	Safety	4	0	20	Medium	Unlikely	Acceptable
	Financial	3	10				
	Operational	2	10				
PT02	Safety	4	0	1	Insignificant	Unlikely	Acceptable
	Financial	4	0				
	Operational	3	1				
PT03	Safety	4	0	20	Medium	Possibly	Unacceptable
	Financial	3	10				
	Operational	2	10				
PT04	Safety	4	0	20	Medium	Possibly	Unacceptable
	Financial	3	10				
	Operational	2	10				
PT05	Safety	4	0	20	Medium	Possibly	Unacceptable
	Financial	3	10				
	Operational	2	10				
PT06	Safety	4	0	20	Medium	Possibly	Unacceptable
	Financial	3	10				
	Operational	2	10				
PT07	Safety	4	0	20	Medium	Unlikely	Acceptable
	Financial	3	10				
	Operational	2	10				
UD08	Safety	4	0	100	Critical	Unlikely	Unacceptable
	Financial	4	0				
	Operational	1	100				
UD09	Safety	4	0	100	Critical	Possibly	Unacceptable
	Financial	4	0				
	Operational	1	100				
UD10	Safety	4	0	100	Critical	Unlikely	Unacceptable
	Financial	4	0				
	Operational	1	100				
FM11	Safety	4	0	20	Medium	Unlikely	Acceptable
	Financial	3	10				
	Operational	2	10				
FM12	Safety	4	0	20	Medium	Unlikely	Acceptable
	Financial	3	10				
	Operational	2	10				
FM13	Safety	4	0	1	Insignificant	Possibly	Acceptable
	Financial	4	0				
	Operational	3	1				
FM14	Safety	4	0	20	Medium	Unlikely	Acceptable
	Financial	3	10				
	Operational	2	10				
O15	Safety	4	0	20	Medium	Unlikely	Acceptable
	Financial	3	10				
	Operational	2	10				
E16	Safety	4	0	100	Critical	Likely	Unacceptable
	Financial	2	100				
	Operational	4	0				
E17	Safety	4	0	100	Critical	Likely	Unacceptable
	Financial	2	100				
	Operational	4	0				
E18	Safety	4	0	20	Medium	Likely	Unacceptable
	Financial	3	10				
	Operational	2	10				
E19	Safety	4	0	20	Medium	Likely	Unacceptable
	Financial	3	10				
	Operational	2	10				
E20	Safety	4	0	20	Medium	Likely	Unacceptable
	Financial	3	10				
	Operational	2	10				
E21	Safety	4	0	20	Medium	Likely	Unacceptable
	Financial	3	10				
	Operational	2	10				
E22	Safety	4	0	20	Medium	Likely	Unacceptable
	Financial	3	10				
	Operational	2	10				
E23	Safety	4	0	20	Medium	Likely	Unacceptable
	Financial	3	10				
	Operational	2	10				
E24	Safety	4	0	20	Medium	Likely	Unacceptable
	Financial	3	10				
	Operational	2	10				
NA25	Safety	4	0	20	Medium	Likely	Unacceptable
	Financial	3	10				
	Operational	2	10				
NA26	Safety	4	0	20	Medium	Likely	Unacceptable
	Financial	3	10				
	Operational	2	10				
NA27	Safety	4	0	20	Medium	Likely	Unacceptable
	Financial	3	10				
	Operational	2	10				
NA28	Safety	4	0	20	Medium	Likely	Unacceptable
	Financial	3	10				
	Operational	2	10				
NA29	Safety	4	0	20	Medium	Likely	Unacceptable
	Financial	3	10				
	Operational	2	10				

Table VII presents the risk evaluation of threats previously studied in section V-A. From the impact-likelihood combination for each unwanted incident, the risk level can be calculated and identified whether it is acceptable or not following the risk matrix presented in Table VI. In case the risk is unacceptable, countermeasure should be applied in order to reduce the likelihood of the corresponding threats.

VI. Good practices

According to the methodology presented in section II, at this level of the risk assessment, we should identify a set of countermeasure with the aim to eliminate unacceptable risks. However, these countermeasures cannot be presented as their are classified. Instead, in this paper, we presents high level countermeasures, sort of good practices that helps to design a properly protected TCMS. In Table VIII, we present a first estimation about time and efforts needed to recover from an unwanted incident, some good practices that helps to avoid exposure of the system to the identified threats or to limit their impacts, and the existent challenges and gaps that may increasing vulnerability and exposure of the system.

VII. Conclusions

In this paper, we presented a security risk assessment of EDC system of Train Control and Monitoring System (TCMS). This work was conducted as a part of ROLL2RAIL project. The security risk analysis showed that the absolute majority of threats targets mainly integrity and availability of the EDC system which can lead to severe consequences. Regarding data confidentiality, this security property is not of huge impact for EDC system. During ROLL2RAIL project, the security risk assessment was conducted for others functionalities of TCMS. At the end, a set of countermeasures was proposed to strengthen the security of TCMS against identified potential threats. The effectiveness of the countermeasures was demonstrated through several iterations of risk evaluation process.

Acknowledgment

This works was supported by the European H2020 Roll2Rail project. The authors gratefully acknowledge the support provided by this institution.

References

[1] ISA-62443: Security for Industrial Automation and Control Systems. Standard, International Society of Automaton (ISA), 2016.

[2] ISO/IEC 27000: Prévisualiser Technologies de l'information – Techniques de sécurité – Systèmes de gestion de sécurité de l'information – Vue d'ensemble et vocabulaire. Standard, ISO and IEC, 2016.

[3] ISO/IEC 15408-1:2009 Preview Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model. Standard, ISO and IEC, 2009.

[4] EN 50159: Railway applications - communication, signalling and processing systems - safety-related communication in transmission systems. Standard, European Committee for Electrotechnical Standardization (CENELEC), 2010.

[5] B Fraser. Rfc 2196. site security handbook. 1997. *URL: http://www. faqs. org/rfcs/rfc2196. html*, 2003.

[6] ETSI - TS 102 165 : Telecommunications And Internet Converged Services And Protocols For Advanced Networking (Tispan); Methods And Protocols. Standard, European Telecommunications Standards Institute (ETSI), 2007.

TABLE VIII: Recovery time and efforts, challenges and Gaps and good practices

Threat class	Threat	Recovery Time and efforts	Challenges and Gaps	Good Practices
Physical Threats	Vandalism Unauthorized physical access/ Unauthorized entry to premises	A physical inspection is needed to fix the damaged component and to ensure its normal functioning	Insecure design or development	An alarm should be triggered once a door is attacked or damaged. Local door controllers should be properly protected. Physical access to driver cabin should be limited/ avoided.
Unintentional Damage	Erroneous use or administration of devices and systems Unintentional change of data in the system or destruction of records	A Software-based vulnerabilities such as erroneous administration, modification of configuration,etc...) may be fixed by an update of the software.	Concerned staff lacks of awareness about security issues and good practices Insecure design or development	Engage in staff training Employ identity management systems and advanced authentication techniques (to request additional Identification, authentication and authorization techniques for administration processes) Employ alarms to protect digital assets (to add alerting notifications and alarms for maintenance and administration processes, that are different from and more sophisticated then when used for controlling processes) Establish a recovery processes and maintain backups of the recorded data
Failures Malfunction	Failure of device or systems Failure or disruption of communication links	For hardware malfunctions and failure, a physical inspection is needed to replace or fix the failing or damaged components and to ensure their back to the normal functioning Software-based malfunctions and failure may be fixed by update For	Concerned staff lacks of awareness about security issues and good practices Insecure design or development (especially maintenance tools)	Implement a disaster recovery processes and define a degraded mode of operations : safe mode should be implemented such as putting all or a number of doors at safe state (depending of the situation and the state of the train/consist/car), isolating the damaged doors until problem is solved for safety purposes, *etc* ...
Outages	Network outage	A physical inspection is needed to fix the damaged components and ensure their back to the normal functioning	Insecure design or development	Implement a disaster recovery processes and define a degraded mode of operations.
Eavesdropping	Network Reconnaissance, Network traffic manipulation and Information gathering Man in the middle / Session hijacking	Recovery time and efforts depend of the attack	Vulnerabilities caused by the deployment and the use of the communication infrastructure in a public environment Insecure design or development	Limit physical access to the communication network Set up intrusion detection solutions to detect hijacking attempts or other advanced measures preventing spoofing
Nefarious Activity	Denial of Service Malicious code/ software/ activity Identity Fraud Manipulation of hardware and software Manipulation of information	Recovery time and efforts generally depend of the attack. Software-based vulnerabilities concerning identification, authentication and authorization may be fixed by updating the software. Some nefarious activities may cause physical damage of some components that can no longer been remotely monitored, as such a physical inspection is needed to ensure the normal functioning of door control system components	Vulnerabilities caused by the deployment and the use of the communication infrastructure in a public environment Insecure design or development Concerned staff lacks of awareness about security issues and good practices	Limit physical access to all EDC system components Set up intrusion detection solutions to detect hijacking attempts or other advanced measures preventing such events Employ identity management systems and advanced identification, authentication and authorization techniques Employ alarms to protect digital assets (additional alerting notifications and alarms whenever configuration is modified or for each action of administration of critical components) Establish a recovery processes and maintain backups of the system state Engage in staff training to rise awareness concerning Identification, authentication and authorization problems

[7] VDE V 0831-102:2013-12: Electric signalling systems for railways - Part 102: Protection profile for technical functions in railway signalling. Pre-standard, the German Institute for Standardization (DIN), 2013.

[8] VDE V 0831-104:2015-10: Electric signalling systems for railways - Part 104: IT Security Guideline based on IEC 62443. Pre-standard, DIN, 2015.

[9] FIPS PUB 199: Standards for Security Categorization of Federal Information and Information Systems. Standard, Federal Information Processing Standards Publication, 2004.

[10] FIPS PUB 200: Minimum Security Requirements for Federal Information and Information Systems. Standard, Federal Information Processing Standards Publication, 2006.

[11] NIST Special Publication 800-37 Revision 1 : Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach . Technical report, NIST, 2014.

[12] NIST Special Publication 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations. Technical report, National Institute of Standards and Technology (NIST), 2013.

[13] W. Knowles, D., D. Hutchison, J. F. Pagna Disso, and K. Jones. A survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection*, 9, 2015.

[14] Control Engineering Europe. Cyber security: a threat to industry 4.0 implementation?

[15] V. Watson, A. Tellabi, J. Sassmannahausen, and X. Lou. Interoperability and security challenges of industry 4.0. *INFORMATIK 2017*, 2017.

[16] ROLL2RAIL-WP2.1. Specification of Wireless TCMS. Technical report, 2016.

[17] ROLL2RAIL-WP2.5. WLAN in WTCN Discussion Paper. Technical report, 2016.

[18] ROLL2RAIL-WP2.5. Deliverable D2.5 - Architecture for the Train and Consist Wireless Networks. Technical report, 2016.

[19] ROLL2RAIL-WP2.5. Infotainment and CCTV. Technical report, 2016.

[20] IEC 61375-2-4 TS: Electronic Railway Equipment – Train Communication Network (TCN) – Part 2-4: TCN Application profile. Standard, International Electrotechnical Commission (IEC), 2016.

[21] Threat taxonomy: A tool for structuring threat information. Technical report, ENISA, 2016.

[22] Cyber security and resilience of smart cars : Good practices and recommendations. Technical report, ENISA, December 2016.

[23] C. Lévy-Bencheton and E. Darra. Cyber security and resilience of intelligent public transport: Good practices and recommendations. Technical report, ENISA, 2015.

[24] CERT Insider Threat Team. Unintentional insider threats: A foundational study. *Software Engineering Institute Technical Report*, 2013.

[25] M. Ahmed, L. Sharif, M Kabir, and M. Al-Maimani. Human errors in information security. *International Journal of Advanced Trends in Computer Science and Engineering*, 1(3), 2012.

[26] J. P. Farwell and R. Rohozinski. Stuxnet and the future of cyber war. *Survival*, 53(1):23–40, 2011.

[27] G. McDonald, L. O Murchu, and S. Dohertyand E. Chien. Stuxnet 0.5: The missing link. Technical report, Symantec, 2013.

[28] J. Vazquez M. Boer. Cyber security and financial stability: How cyber-attacks could materially impact the global financial system. Technical report, Institute of international finance, 2017.

[29] ISO/IEC 27005:2011 technologies de l'information – techniques de sécurité – gestion des risques liés à la sécurité de l'information. Standard, ISO and IEC, 2011.

[30] ROLL2RAIL-WP2.4. Cyber Threat Scenarios for Rail Vehicle IT Systems. Technical report, 2016.

[31] M. Wolf and M. Scheibel. A systematic approach to a qualified security risk analysis for vehicular IT systems. In *Automotive-Safety & Security*, pages 195–210, 2012.

[32] Common Critera, Common Methodology for Information Technology Security Evaluation: Evaluation methodology. Standard, ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission), 2017.

[33] ETSI TS 102 165-1 V4.2.3 (2011-03): Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis. Standard, ETSI, 2011.

[34] ROLL2RAIL-WP2.4. WTCMS Security Risk Assessment Methodology. Technical report, 2016.