Cyber-physical Threats and Vulnerabilities Analysis for Train Control and Monitoring Systems

Mouna Rekik, Christophe Gransart, Marion Berbineau

Cyber-physical Threats and Vulnerabilities Analysis for Train Control and Monitoring Systems

Mouna Rekik
Univ Lille Nord de France,
IFSTTAR, COSYS, LEOST,
F-59650 Villeneuve d'Ascq, France
Email: mouna.rekik@ifsttar.fr

Christophe Gransart
Univ Lille Nord de France,
IFSTTAR, COSYS, LEOST,
F-59650 Villeneuve d'Ascq, France
Email: christophe.gransart@ifsttar.fr

Marion Berbineau
Univ Lille Nord de France,
IFSTTAR, COSYS,
F-59650 Villeneuve d'Ascq, France
Email: marion.berbineau@ifsttar.fr

***Abstract*—Cyber-physical security is a major concern for the new generation of trains. In fact, trains are increasingly relying on automation, control and communication technologies in order to improve the efficiency and safety of their services as well as the comfort of passengers. This dependency introduces certainly new vulnerabilities and entry points to the system which exposes the system to new threat scenarios. This paper deals with cyber-physical security aspects of Train Control and Monitoring Systems (TCMSs). We analyse vulnerabilities and characteristics of railway threat landscape including potential threats, threats agents and motivations. We discuss, also, direct impacts and cascading consequences on the whole system as well as the risk generated.**

***Index Terms*—Railway System, TCMS, Cyber-physical security, Threat, Vulnerability, Risk**

I. Introduction

Technological advances and ongoing digitalization are continuously improving safety and efficiency of railways systems. New generation of trains will use real-time rail information and on-line 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. Train passengers travelling experience will be improved as well through services such as connected infotainment, realtime information, etc. These innovations are accomplished using networked devices along with advanced remote access and control capabilities. Introducing such features for safety critical systems like railway systems brings not only improvements but also new challenges concerning cyber-physical security.

Cyber-attacks are 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 like delays, accidents, injuries or even deaths, to indirect effects, like 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 for each TCMS asset. Yet, such outcomes can be accomplished using a coherent and strategic approach that encompasses all cyber-physical security aspects. The starting point of the selected approach is studying the system vulnerabilities and threat landscape. As such, in this paper, we present security threats and vulnerabilities assessments of TCMS with the aim of identifying threats, quantifying impacts and expected losses, and analyzing criticality of the system assets.

The remainder of this paper is structured as follows. Section II shortly introduces the System under Consideration (SuC). We analyze the system vulnerabilities in section III. Then, we discuss railway threat landscape through a threat model, actors and motivation analysis in section IV, and present potential impacts and risks on railway systems in section V. A detailed threat analysis of some assets of the SuC is presented in section VI. Finally, the paper is concluded, in section VII.

II. System Identification

The starting point of a cyber-physical security analysis is performing a clear identification of the SuC. This step consists in illustrating the SuC assets and Industrial Automation Control System (IACS) included in the system, identifying the access points to the system and defining the security perimeter. Thus, in this section, we detail the proposed architecture of the SuC which is the TCMS, as well as its different functionalities. This step helps to identify the sensitive assets of the SuC.

The TCMS is mainly responsible for providing basic train control functions: -inaugurate the train network, -determine train topology and configuration, -provide orientation information for coupled elements, -manage leading vehicle information, -distribute train topology and configuration, -confirm train configuration, -manage train network operation, -manage train network access and -transmit data. Nevertheless, with the recent advances of Information and Communication Technology (ICT) integrated in the railway industry, a 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. As such, in order to separate the control system ICT from

the comfort ICT, the SuC is clustered into 3 functional domains [1] [2] [3] [4]:

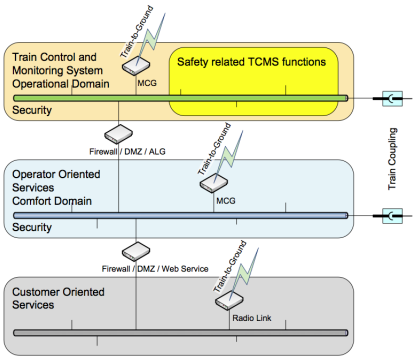

Figure 1: SuC functional domains based model [1]

• TCMS domain includes both safety related and non-safety related TCMS functions. The functions of this domain, which are mandatory to ensure safe train movement and carrying the payload, are : 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 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) are auxiliary services for proper train operation. Funtions of OOS domain are: 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) include 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 modelling, presented in Figure 1, aims to increase flexibility, scalability, and adaptability of the system 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 of communications. For instance, New Dependable Rolling Stock for a more Sustainable, Intelligent and Comfortable Rail Transport in Europe (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 [2]. For safety and security purposes, access between different domains will be limited. Indeed, as shown in Figure 1, the proposed architecture includes also network protection devices between different functional domains since their security and safety requirements differ.

III. 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. The vulnerabilities of railway systems can be divided in two categories [5]: general cyber-vulnerabilities, and vulnerabilities coming from the specificity of railway systems.

1– **General vulnerabilities for IACS**

• Wireless and cellular communications. Although such communication technologies bring 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. The risk of attack 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 the possibility of human error, it introduces new vulnerabilities since the surface of attack increases and therefore the risk of attack is higher.

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 a 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 equipment 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,etc. It is crucial, but also difficult, to ensure smooth interfacing, communication and securing between such independent and heterogeneous systems. This increases system 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.

IV. Railway Threat Landscape

A threat landscape provides an overview of potential threats against the SuC and their characteristics. To this end, in this section, we are identifying the set of threats against a railway system, threat actors and their motivation to attack.

A. Potential threats against TCMS

Railway system is exposed to many types of attacks of different nature. In this section, we present a threat taxonomy that covers mainly cyber-security threats; which are threats directly applied to ICT assets and thus affecting SuC operations. We also present non-IT threats to cover threats to SuC physical assets that are necessary for the system operation. Based on recent studies published by European Union Agency for Network and Information Security (ENISA) [6] [7] [5], threats can be classified into physical threats, accidental threats, disasters and outages, failure and malfunctions (system failure) and malicious actions.

• 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 infrastructure, hardware or ICT connections.

• Accidental damages. These are caused by unintentional insider actions [8] including human errors [9]. Unintentional mistakes can be made by authorized employees, users, developers, and testers during data entry, operations, or system or application development. Such errors can affect system integrity and stability.

• Malicious activities. This type of threats contains cyber-attacks and intentional nefarious activities or abuse targeting railway system assets through digital assets.

B. Threat actors and motivations

Railway systems can be threaten by several types of actors with different motivations. In the following, we present an taxonomy of threat actors against railway systems in order of importance:

• **Nation states** is an emerging, yet critical, class of threat actor against critical infrastructures in general, including railway systems. In fact, these systems provide the essential services for the nation's society and serve as the backbone of its economy, security, and health. As such, they become a significant targets in modern cyber-warfare. Attacks performed by such actors can be politically or economically motivated.

• **Non-state organized threat groups**. This category includes mainly cyber-terrorists but also 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** 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** is a traditional category of attackers that are interested in performing abusive activities against competitor-controlled cyber-physical systems in order to cause concrete damage and gain business advantages.

• **Casual cyber-attackers** that usually have little or no technical skills, launching attacks against connected control systems can cause serious damage, much higher than in the case of simple IT system.

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 [10]. According to [11], Stuxnet was launched by the US and Israel several years ago, in an attempt to sabotage IranâĂŹs 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 other 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 [12]. 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.

V. Risk on railway systems

A risk is defined as the potential that a given threat will successfully exploit vulnerabilities and thereby produce a negative impact on the system. From operator perspective, 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. From passenger perspective, negative impacts can be confidentiality and privacy problems (since the system uses sensing, tracking, real-time behaviour evaluation and automated decisions), interruption and disturbance of transport services resulting in disruption of their daily lives, etc. However, the most critical impact is when passengers health and safety are affected. Indeed, 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.

The aforementioned impacts can affect one or many areas. We distinguish 3 categories of risk based on the impacted area [13]. For each area, we define 3 levels of severity.

• **Safety** : Risks impacting safety differ in terms of severity. In fact, a risk can result in (level1) light and moderate injuries and/or minor damage to the environment, (level2) severe injuries and/or large damage to the environment and even (level3) life-threatening and fatal injuries and/or extreme damage to the environment.

• **Financial** : Financial impacts vary from undesirable financial damage and impact on the public image of the company(level1), to substantial financial damage and a serious impact on the public image of the company(level2), and even existence-threatening financial damage and severe impact to the public image of the company such as the incident may incur people suing the company(level3).

• **Operational** : Impacts on operational aspects may affect comfort functionalities, however the vehicle can be used but with some restrictions(level1). It can also lead to affect an important functionality but the train still can be used, only with massive restrictions(level2). In the worst cases, one or more fundamental functions may be affected such as the train become unusable(level3).

VI. Threat analysis

In this section, we present a detailed threat analysis for TCMS. We describe potential threats, the direct impacts on the attacked asset, the cascading consequences on the whole system, the impacted area (marked I.A)(S, F or O for safety, financial, operational respectively) and the risk level (1, 2 or 3 as defined in paragraph V).In our original work, we performed the analysis for all system assets. In this paper, due to space limitation, we selected two assets of a railway system with different functionalities and levels of criticality: propulsion system from TCMS domain and CCTV surveillance system from OOS domain.

Table I presents a threat analysis of the propulsion system responsible for the movement of a train. The analysis shows that threats on propulsion system (and this is also true for all TCMS domain functions) target mainly the availability (blocking , disconnection, destruction, etc) and integrity (changing configuration, erroneous administration, etc) of the system. Such actions may result in catastrophic consequences on train operation (maximum security level for operational aspects) and thus on passengers safety (maximum security level for safety). This also lead to severe financial impacts for the train operator, but railway sector in general.

OOS domain CCTV surveillance system is responsible for managing surveillance sources, collecting surveillance information, analyzing surveillance functions, displaying surveillance information (selected, or triggered by alarm source) and recording surveillance information. CCTV asset at OOS domain does not cover CCTV for rear view. A threat analysis of CCTV surveillance system is presented in Table II. As shown in this analysis, threats on OOS CCTV affect the system integrity and availability but also customers confidentiality since sensitive data about particular passengers or particular shipped goods and their location in the train may be shared with unauthorized entities. Attacking CCTV system my be a step behind bigger attack on the train (such as criminal or terrorist attacks). For that, attacking the CCTV system may severely affect safety of the passengers and vehicle although it does not directly affect train operations.

VII. Conclusions

In this paper, we performed security threats and vulnerabilities assessments for TCMS. We also presented some results from the detailed threat analysis. This work was conducted as a part of Roll2Rail project. It presents the first step in a selected methodology to establish a cyber-physical secure TCMS. Throughout this analysis, we deduced that the absolute majority of threats targets mainly integrity and availability of TCMS services. The violation of these security properties by attacks against many train subsystems and especially against communication services can lead to the most severe consequences or even catastrophic. Regarding data confidentiality, it is to be considered only for COS and video surveillance from OOS. Further, we will continue the security risk assessment process. As such, a detailed risk assessment will be elaborated to evaluate the criticality of the identified threats on railway systems, and to help suggesting more efficient countermeasures for securing TCMS.

Acknowledgment

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

References

[1] R2R-WP2.1. Specification of Wireless TCMS. Technical report, ROLL2RAIL, 2017.
[2] R2R-WP2.5. WLAN in WTCN Discussion Paper. Technical report, ROLL2RAIL, 2017.
[3] R2R-WP2.5. Architecture for the Train and Consist Wireless Networks. Technical report, ROLL2RAIL, 2017.
[4] R2R-WP2.5. Infotainment and CCTV. Technical report, ROLL2RAIL, 2017.
[5] C. Lévy-Bencheton and E. Darra. Cyber security and resilience of intelligent public transport: Good practices and recommendations. Technical report, European Union Agency for Network and Information Security (ENISA), 2015.
[6] ENISA threat taxonomy: A tool for structuring threat information. Technical report, ENISA, 2016.
[7] Cyber security and resilience of smart cars : Good practices and recommendations. Technical report, ENISA, 2016.
[8] CERT Insider Threat Team. Unintentional insider threats: A foundational study. *Software Engineering Institute Technical Report*, 2013.

Asset: Propulsion					
Class	**Threat**	**Description**	**Direct effect**	**System effect**	**I.A.**
Physical attacks	Vandalism	An attacker could unplug the Access Point from the network or power-off the access point	Propulsion system is not able to exchange information about status of its components. The driver cannot receive information from propulsion system to ensure that the right functioning. The driver is not able to command the propulsion system, the commands are blocked. For safety reasons, the train performs a controlled emergency break.	Massive damage to safety and security related functions can be made. Danger for passengers and vehicle.	S-3 F-2 O-3
	Unauthorized physical access/ Unauthorized entry to premises	An unauthorized person controls propulsion system	increase/decrease train speed in an inappropriate way, propulsion system stops working. For safety reasons, the train performs a controlled emergency break.	Massive damage to safety and security related functions can be made. Danger for passengers and vehicle.	S-3 F-2 O-3
Accidental damage	Erroneous use or administration of devices and systems	An employee may accidentally enter erroneous administration data of propulsion control system.	A bad or erroneous administration and configuration of the system may lead to erroneous actions. The propulsion could stop working and the train cannot move until the problem is fixed.	Financial impacts for the operator	S-0 F-1 O-3
	Using information from an unreliable source	may lead to erroneous use or administration of devices and systems	The propulsion could stop working and the train cannot move until the problem is fixed.	Financial impacts for the operator	S-0 F-1 O-3
	Unintentional change of data in the system or destruction of records	Loss of recorded data about the state of the system	Loss of data used for maintenance purposes	Minor impacts for the operator	S-0 F-0 O-1
Malicious actions	Denial of service attack	An Attacker can conduct DoS attack in order to disconnect the network.	The network is disconnected, no data exchange between propulsion system components. The propulsion system is not able to take the right decision. The driver can not control the propulsion system. For safety reasons, the train performs a controlled emergency break.	Massive damage to safety and security related functions can be made. Danger for passengers and vehicle.	S-3 F-2 O-3
	Eavesdropping /interception /hijacking	An attacker manipulates commands related to propulsion functions.	The Propulsion System makes the train travel to an unauthorized speed.	Massive damage to safety and security related functions can be made. Danger for passengers and vehicle.	S-3 F-2 O-3
	Identity theft	An Attacker can conduct malicious identity theft actions.	Using the identity, the attacker has advanced privileges, and thus can manipulate the system. The attacker makes the train travel to an unauthorized speed, or stops the propulsion system from working. The attacker can manipulate propulsion system and create new entry point to conduct more attacks.	Massive damage to safety and security related functions can be made. Danger for passengers and vehicle.	S-0 F-2 O-3

Table I: Detailed threat analysis for Propulsion control system

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

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

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

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

[13] R2R-WP2.4. Cyber Threat Scenarios for Rail Vehicle IT Systems. Technical report, ROLL2RAIL, 2017.

Asset: Closed-circuit television (CCTV): surveillance system					
Class	**Threat**	**Description**	**Direct effect**	**System effect**	**I.A.**
Physical attacks	Sabotage vandalism Theft	An attacker can put an obstacle in front of CCTV camera or paint the facade of the camera. An attacker can unplug the camera from the system. An attacker can break the CCTV camera. An attacker can steal CCTV cameras.	to loose (partially) visibility of the attacked part of the train. At the worst case, some criminal actions can not be prevented, and once accomplished, they can not be identified, which can seriously risk the safety of the train and passengers	Possible damage to safety and security related functions. Railway operator's reputation can be affected, financial loss.	S-2 F-2 O-0
	Information leakage/ sharing	Confidential information can be shared with unauthorized entities due to intentional human actions (mainly by employees that have access to restricted facilities) which lead to loss of information confidentiality	The attacker could have access to sensitive data recorded by the cctv system, such as particular passengers or particular shipped goods and their location in the train. In the worst case, these information can be used for criminal purposes, which can risk the safety of passengers and the train	Possible damage to safety and security related functions. Railway operator's reputation can be affected, financial loss.	S-2 F-2 O-0
	Unauthorized physical access/ Unauthorized entry to premises	An unauthorized person controls CCTV system	The CCTV can be stopped from working, or blocked. Confidential information can be shared	Possible damage to safety and security related functions. Railway operator's reputation can be affected, financial loss.	S-2 F-2 O-0
Accidental damage	Information leakage/sharing due to unintentional error	An employee could unintentionally share data of CCTV with unauthorized entities	An attacker could take advantage of the unintentional error and access, share, manipulate, or even discard confidential information which lead to loss of information confidentiality	Possible damage to safety and security related functions. Railway operator's reputation can be affected, financial loss.	S-2 F-2 O-0
	Unintentional change or destruction of records	An employee could unintentionally change or destroy recorded data	Error leading to loss of information, including sensitive and important data. In the worst, some criminal or malicious actions performed in the train can not be analyzed	Railway operator's reputation can be affected, financial loss.	S-0 F-2 O-0
	Erroneous administration or configuration of surveillance or recording devices	An employee could unintentionally change administration or configuration some assets or the whole CCTV system	Loss of visibility of parts or all the system. manipulation or loss of information, including sensitive and important data. In the worst, some criminal or malicious actions performed in the train can not be detected and/or analyzed, thus their consequences cannot be prevented	Possible damage to safety and security related functions. Railway operator's reputation can be affected, financial loss.	S-2 F-2 O-0
Malicious actions	Denial of service	An Attacker can conduct Distributed Denial of network service (DDoS) attack on the network or application layers.	Disturb or the communication between CCTV system components and thus limit the controlling capacities of the system. At the worst case, it may lead to disconnect the whole system, and thus loose visibility on the train.	Possible damage to safety and security related functions. Railway operator's reputation can be affected, financial loss.	S-2 F-2 O-0
	Eavesdropping/ Interception/ Hijacking	An attacker can intercept communications to record data transmitted from video capture components to video display and video storage components. Threat of failure of IT hardware or transmission connection due to electromagnetic induction or electromagnetic radiation emitted from an another source. An attacker can maliciously or fraudulently repeat or delay transmission of valid data. Network Reconnaissance, Network traffic manipulation and Information gathering. Man in the middle attack, to sniff the data and command traffic exchanged between the system components, and alter communications.	loss of visibility of parts or all the system. The CCTV can be stopped from working, or blocked. loss of confidential information Malicious re-transmission of valid data may perturb the system or transmission of erroneous or manipulated data and commands. In the worst case, false alarm and emergency situation may be triggered in inappropriate time. Criminal activities could also be covered using such attacks, which lead to inability of performing right reactions when needed to prevent or stop crimes	Possible damage to safety and security related functions. Railway operator's reputation can be affected, financial loss.	S-2 F-2 O-0
	Identity theft	An attacker can steal authentication information for CCTV system users or administrators in order to have more Privileged capacities to control the system.	The attacker may take control of the system. Loss of visibility of parts or all the system. Manipulation recorded/ displayed data or even data analysis Criminal actions occurring in the train can not be detected and/or analyzed, thus their consequences cannot be prevented	Possible damage to safety and security related functions. Railway operator's reputation can be affected, financial loss.	S-2 F-2 O-0

Table II: Detailed threat analysis for OOS CCTV