Int J Syst Assur Eng Manag (April 2019) 10(2):149–159
https://doi.org/10.1007/s13198-019-00778-w

REVIEW PAPERS

# Cybersecurity for eMaintenance in railway infrastructure: risks and consequences

**Adithya Thaduri**[1] · **Mustafa Aljumaili**[1] · **Ravdeep Kour**[1] · **Ramin Karim**[1]

Received: 15 June 2018 / Revised: 14 February 2019 / Published online: 15 March 2019


**Abstract** Recently, due to the advancements in the Information and Communication Technology, there has been lot of emphasis on digitization of the existing and newly developed infrastructure. In transportation infrastructure, in general, 80% of the assets are already in place and there has been tremendous push to move to the digital era. For efficient and effective design, construction, operation and maintenance of the infrastructure, due to this digitization, there is increasing research trend in data-driven decision-making algorithms that are proved to be effective because of several advantages. Since railway is the backbone of the society, the data-driven approaches will ensure the continuous operation, efficient maintenance, planning and potential future investments. The breach and leak of this potential data to the wrong hands might result in havoc, risk, trust, hazards and serious consequences. Hence, the main purpose of this paper is to stress the potential challenges, consequences, threats, vulnerabilities and risk management of data security in the railway infrastructure in context of eMaintenance. In addition, this paper also identifies the research methods to obtain and secure this data for potential possible research.

**Keywords** eMaintenance · Cybersecurity · Risks · Consequences · Railways

✉ Adithya Thaduri
adithya.thaduri@ltu.se

[1] Division of Operation and Maintenance Engineering, Luleå University of Technology, Luleå, Sweden

## 1 Introduction

Data is sensitive for business decisions, risks in competition, data breach issues could lead to safety, societal relevance and loss of reputation. The sensitive information of the critical infrastructure needs to be protected so that the unauthorized people cannot access it that can potentially lead to privacy and security issues of both individuals and organization. The loss of data to other third party could lead to potential hazards such as they can control the assets remotely to achieve their predefined plans.

The information loss of employees within the organization might feel insecure as it could lead to privacy problems and lead to legal and personal threats. The leakage of this sensitive business information might be of hazardous risk if it lands on the competitor, which also pose business reputation (Willett 2008). This information can be categorized as financial transactions, customers and supplier's data, trade exchanges, acquisition plans, internal reports and other kind of information which of most secret to the business organization. Due to digitalization and increase in generation of data, there is an urgent need of new and improved methods of protecting this data from the unauthorized users. There will be several threats, vulnerabilities and risk associated with leakage of this data. In order to achieve the complete security of the data, several issues and challenges will be raised, if not overcome, will lead to serious consequences on both social and business perspective.

Today, cybersecurity becomes a serious issue because of increase in computer abuse. According to Kissel (2013) cybersecurity is the "ability to protect or defend the use of cyberspace from cyber-attacks" and cyberspace is "a global domain within the information environment consisting of the interdependent network of information systems

infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers". There are different types of cyber-attacks like malware, phishing, man-in-the-middle attack, dos/don'ts cross-site scripting, SQL injection, botnets, social botnets, espionage based attacks that steal data and information, drive-by-downloads, last mile interceptions, transmission bugs/intercepts, critical infrastructure, cyber kidnapping, cyber extortion, hacktivism (Matt 2005).

Therefore, to enhance the cybersecurity, most of the countries have already framed data protection laws. Individuals and business organization must compliance with the legal issues and regulations in storing and processing the data (Ahrens et al. 2011). Further, substantial protection mechanisms need to be implemented while dealing with different issues such as security of data, privacy of personnel, commercial confidences, financial information and intellectual property (Smith et al. 2012).

The growing inclination of outsourcing data to third parties offers impending risks to information security and data protection. Thus, due to the applications of cloud technology, the traditional systems will migrate to the cloud platform. As more workloads move to the cloud, organizations are recognizing that traditional security tools are not intended for the distinctive challenges in cloud adoption and, hence, strong security management and control solutions are precisely considered for the cloud to protect the new, agile paradigm (CSA 2016). In addition, there are also several issues while adopting cloud computing in terms of privacy-aware data storage (Itani et al. 2009), secure and scalable access control (Yu et al. 2010), business perspective (Marston et al. 2011), cloud security (Zissis and Lekkas 2012), Big Data (Hashem et al. 2015) and Cyber threats (CSA 2016). Therefore, Cybersecurity is the biggest issue for the customers who subcontract their personal and private data into the cloud storage because it is associated with many cyber risks. There are lots of cyber risks associated with the cloud like, account hijacking, advanced persistent threats (APT), data breaches, data loss, denial of service, insecure API, malicious insiders, misuse and nefarious use of cloud services, insufficient due carefulness, shared technology concerns, system and application vulnerabilities, and weak identity (CSA 2016).

Recently, the Swedish Transport Agency (Transportstyrelsen) was investigated after information about all vehicles in the country—including police and military—was given access to IT workers in Eastern Europe without sufficient security clearance checks (The Local 2017). This was due to an agency that was outsources its maintenance of IT services to IBM administrators in Czech Republic. This problem is a data access problem that led to crisis for the Swedish national security.

Railways in the transport is the important critical infrastructure. The railway industry has a substantial influence on the society in both passenger and cargo. It facilitates the mass transport of people from one place to another and huge supply of goods for trading and business with faster reach and economical value. Cyber incidents might result in a range of conceivable consequences, from status damage through to interruption and even injury and loss of life due to systems being compromised.

## 2 eMaintenance

In the literature, there are several architectures developed for security in railways. Kotenko et al. 2013, develops the architecture of a multi-level intelligent information security system. Bastow 2014 suggested that there is a need for mitigation measures considering a tough security policy, collaboration among legal, government, technology and societal aspects. An integrated approach to security, privacy and dependability (SPD) in embedded systems was developed by SHIELD framework that can be applied to railway surveillance (Priscoli et al. 2017). Being operation and maintenance of railways are of utmost importance, eMaintenance platform is developed at LTU for carrying out decision support systems to meet the demands of the railway industry (Karim 2008). It acts as a maintenance strategy where different tasks are managed electronically using real-time item data, such as mobile devices, remote wireless sensing, condition monitoring, knowledge engineering, telecommunications and internet technologies. Within ISO 27000 (information security) the PDCA model is applied to structure all Information Security Management System (ISMS) processes, where information security requirements and expectations of the stakeholder's act as input, and necessary actions and processes produce information security outcomes that meet those requirements and expectations (ISO/IEC 2007). The main objectives of this research project are:

1. To identify the potential risk and consequences in data/information security lapses in railway infrastructure.
2. To study state-of-the-art research methods in the data/information security and recommend the best suitable methods for railway infrastructure.
3. To carry out research potential of secure data and its cost assessment.

The risk management within information security. However, maintenance may also be viewed as a process within the context of eMaintenance to emphasize information logistic aspects instead of technology. From an information security perspective, one aspect of the process approach is that the users are encouraged to emphasize the

importance of the following (adapted from ISO/IEC 27000). (Söderholm and Karim 2010).

- Understanding an organization's information security requirements and the need to establish policy and objectives for information security, which should be derived from the organization's strategic goals.
- Implementing and operating controls to manage an organization's information security risks in the context of the organization's overall business risks, and thereby be aligned with the controls of other risk management functions.
- Continuous improvement, based on objective measurement.

When considering information security, it can be described by the triad confidentiality, integrity and availability (CIA), which describes characteristics of information. From a strategic eMaintenance perspective, this primarily includes risk functions such as internal control, information security, and dependability management. However, the other risk management functions should also be involved.

## 3 Cybersecurity in railways

Railway is a collaborative business where information is shared between different partners. It is difficult in harmonizing the goals of collaboration among different stakeholders and security issues due to lack of proper mechanism in dealing with multiple partners and defining the requirements. This has to be achieved to ensure that the availability, integrity and confidentiality of the railway information is applied with proper authorization. This has to be also collaborated in sense from top level to the operational level.

Railway systems are moving towards more intelligent and connected systems, which offers new opportunities of attackers and cyber-criminals. The security has to be considered in the transport domain for the protection of operators, for economic aspects and for the security of citizens. The transport domain faces many challenges. First, there is no European law on Cyber Security for transport and is still confronted with low level of awareness. Railway stakeholders have difficulties to dedicate budget for this specific topic. The use of heterogeneous technologies and software solutions leads to very varied and disparate data sets. There is also lot of challenges pertaining to Big Data for Railways (Smith et al. 2012; Katal et al. 2013; Hashem et al. 2015). From an information security perspective, the main concern for Railway sector is to reduce the risk of potential data loss and ensure steady and stable rail operation. In case of problem, important consequences can appear, such as train stop, negative economic effects and loss of confidence and accidents. Protection measures against cyber-attacks in the Railway sector are not yet fully developed. There is a lack of awareness of new risks and the risks are not quite considered due to the high level of safety in the railway domain (Masson and Gransart 2017).

The hazards or probable failures or detrimental outcomes to be avoided due to lapses in security (Bloomfield et al. 2016). These are listed as;

- collision with several trains,
- derailment in a single train,
- disruption to few trains,
- extensive interruption of train services,
- scripting of a condition that leads to fear and prospective loss of life,
- scripting of a condition that leads to passenger distress and frustration,
- threat to safety of the workforce, passengers or the public resulting in harm,
- financial loss,
- criminal damage,
- failure to comply with law,
- loss of reputation in the railway systems due to leakage and leak of sensitive information.

There have been few instances where security issues were surfaced in Railway sector. Those are listed below:

- 2008, a person derailed four tram trains in Lodz, Poland by means of TV remote.
- 2011, a group of pirates attacked remote computers, stopped the train signaling system for 2 days in the North Western of United State
- 2013, NMBS (Belgian national railway) accidently published personal information of several customers
- 2014, Japan Airlines confirmed the possible theft of information of frequent-flier programme members
- 2014, an anonymous information request caused in the release of data on several million journeys commuted by New York taxis in 1 year.
- 2015, it was suspected of pirating subway system in Seoul, North Korea.
- 2016, a ransomware attacked the ticketing system that cyphers the hard disk at San Francisco.
- 2017, Swedish Transport Agency leaked several information on drivers to Eastern Europe due to illegal data access within IBM systems.

The potential systems that can be exposed to cybersecurity in railway are electronic interlocking systems, level-crossing protection systems, automatic block signaling system, track-vehicle transmission systems, additional systems (e.g. communication, failure detection)

(Nowakowski et al. 2017). Thales 2016 illustrated several levels of attacks, such as malwares at Operation Control Centre or interlocking, wireless attacks on wireless communications (GSM-R), password attack on Radio Block Centre, etc. Masson and Gransart 2017 reviewed several European projects that focuses on cybersecurity within the view of Shift2Rail. There are different standards that were developed by international bodies on security. These are ISO 27001, Information security management systems, 2013, NIST SP800-53 (National Institute of Standards and Technology-US), ISA/IEC 62443 (International Society of Automation/International Electrotechnical Commission), APTA (American Public Transportation Association), Network and Information Systems (NIS) Directive, ANSSI (National Agency for Security of Information System). There are also several projects that are looking to cybersecurity in railways; PROTECTRAIL 2014, SECUR-ED 2014, CARONTE 2016, SECRET 2015 and CIPSEC (Álvarez et al. 2017). Through examination of security necessities and technical features, the key security technologies are highlighted (Cao et al. 2014), including access control technology, single sign-on technology, authentication technology and unified security center technology, etc. (Shi 2014).

### 3.1 Access control security

Access control security is the main matter to safeguard system safety. There are several basic approaches in literature. A common approach to implementing access matrix is by means of access control list (ACL (Sandhu and Samarati 1994, Role-Based Access Control (RBAC) (Edwards 1996), Task-Based Access Control (TBAC) (Thomas and Sandhu 1998), Team-Based Access Control (TMAC) (Thomas 1997), Spatial Access Control for collaborative environment (SPACE) (Bullock 1999) and Context-Aware Access Control have extended RBAC (Covington et al. 2001). Access control security comprises of global identity management, the customer identity authentication, single login problem etc. Wijesekera and Jajodia (2003) proposed a proposotional policy algebra. Tolone et al. 2005 listed several requirements for access control. The misplaced listing of secure of eMaintenance data due to wrong access control could lead to hazardous scenarios where this data can be exploited for potential leakage of safety of the infrastructure.

### 3.2 Information transmission security

Enterprise Service Bus (ESB) technology is used to comprehend several systems sharing data and service in the railway information sharing platform. But information security is a basic problem in the transmission process. Web and cloud services are the significant means of information sharing platform. The transmission of eMaintenance data need to be well designed so that "man in the middle" could not encrypt the data from servers.

### 3.3 Data storage security

Data storage security is the significant concern for building railway information sharing platform. Using technology such as cloud data storage and management of decentralized computing technology can improve the safety of the railway store important data, but also brings a complex system structure, management and complex problems. Therefore, study off-site storage, disaster recovery, data recovery, security technology, response information sharing platform to build the new data security situation. For operation and maintenance decisions, the data storage security is important for the existing architectures, mainly, eMaintenance platform that stores the railway operation and maintenance data.

### 3.4 Unified security prevention center

Railway Information Security Center are being centralized to accomplish global security services. Information Security Center can apprehend security control through security audits, intrusion detection, virus analysis etc (Cappelli et al. 2012). In addition, planning and scheduling the entire railway information sharing platform resources, optimize the using of computing, storage system capacity and network bandwidth for the entire railway safety and efficient operation of information systems services (Shi 2014).

## 4 Methods to secure the maintenance data

Cyberspace, which refers to a collection of networks, activities, and new human attitudes. Cyberspace is an integral part of any enterprise. As a consequence, cybersecurity is an absolute prerequisite. Due to the digitization of operation and maintenance data to the servers and cloud, the importance of cybersecurity is imminent to consider for the possible present and future consequences of cyber threats. Instead, there are several efforts has been made to safegaurd the systems with cyber attacks for example, a secure cloud storage system for data forwarding (Lin and Tzeng 2012), a cost-effective privacy preservation of intermediate data sets (Zhang et al. 2013) and a supply chain network game theory model (Nagurney et al. 2017). Furthermore, Levy-Bencheton and Darra (2015) suggested good practices and recommendations and providing cyberdefense against cyber threats (Donaldson et al. 2015) and new approaches for going towards Industry 4.0

(Wegner et al. 2017). Cybersecurity consists of the following four principles that are absolutely needed for any trusted cyberspace engagement (Kostopoulos 2017).

- Maintenance data transmitted or stored are private, to be viewed only by authorized persons. This is the principle of Confidentiality.
- Maintenance data transmitted or stored are authentic—free of errors made in storage or in transit. This is the principle of Integrity.
- Maintenance data transmitted or stored are accessible to all authorized. This is the principle of Availability.
- Maintenance data transmitted or stored are of indisputable authenticity, when supported by acceptable digital certificates, digital signatures, or other explicit identifiers.

The cybersecurity literature presents excellent frameworks as shown in Table 1. Some of the major cybersecurity frameworks include the following (Kostopoulos 2017):

1. $(ISC)^2$ Certified Information Security System Professional (CISSP) Common Body of Knowledge (CBK). (The International Information Systems Security Certification Consortium is also known as $(ISC)^2$).
2. International Organization for Standardization (ISO) 27001 and 27002, version 2013.
3. The National Institute of Standards and Technologies (NIST) Risk Management Framework (RMF) and special publication 800-53 The Council on Cyber Security Critical Security Controls (formerly known as the SANS 20 Controls).

## 5 Threats in cybersecurity for railways

There are several threats associated with cybersecurity for railways. These are listed below:

### 5.1 Causes of cybersecurity threats

The prevalent operational challenge to railway sector is the cybersecurity that involves severe threats to identity, privacy, and data systems. These are listed as

1. *Politically motivated threats* These types of threats that could disrupt the reputation of the organization and also to the government (because railway transport in some countries are run by the government). Sometime, they could occur physical damage too. Normally, these approaches use botnets, an agent that enters into the system and they can control the traffic information and failure related information that could lead to accidents by disabling alarms. They can also launch distributed denial of service (DDoS) attack to disable the operation of railway network.
2. *Non-politically motivated threats* These threats are mostly pertaining to the individual who can obtain financial information and business related information. The immediate victims of these attacks or mostly to passengers but in the larger scale it brings down the reputation of the organization.
3. *Data subcontracting problem and loss of data control* These types of threats are related to recent data leak in Swedish railway network. These threats have significant impacts on partnership with third party organizations so that they could lose contracts, confidentiality and loss of control of data. This compromised data will be widely shared among their network and they can control the infrastructures by thus increasing the risks.
4. *Human factors* One of the major and uncontrollable issues in operation and maintenance of the railway network is the human factors. Because of improper training, negligence, lack of awareness and sometimes sabotage could lead to leakage of data.

### 5.2 Types of threats

There are different types of threats that a railway infrastructure manager or railway operator could get from a single or group of people. These attack could conciliate discretion by data theft, concede integrity by changing data, or negotiate availability by rejecting access to data, services, or systems.

1. *Discretion by data theft* Some examples include passenger's person numbers, credit card numbers, financial transactions, commuting trips (like in New York case), and personal corporate top-secrets. This information will be potentially used for selling in public space or to the competitors. This confidential information or data resides in other places which is of secondary in nature and places in at the site or at the transit locations.
    a. *Databases* The most evident place to discover large pool of data is at the physical location of the database.
    b. *Backups* Usually, organizations of railway infrastructures maintain some of the critical information in backups as a redundant mechanism in the event of failure of main database. Surprisingly, in some instances, these backups are often didn't implement the standard procedure of cybersecurity protection methods. This data could be vulnerable if the attackers can access the backups that could lead to embarrassment to their reputation.

**Table 1** Different frameworks of cybersecurity (Kostopoulos 2017)

| $(ISC)^2$ Common Body of knowledge 10 security domains | ISO 27001/27002v2013 114 controls in 14 domains | NIST SP800-53v4 224 controls in 18 families | Council on cyber security critical security controls-20 controls |
|---|---|---|---|
| 1. Access control | 1. Information security policies | 1. Access control | 1. Inventory of devices |
| 2. Telecommunications and network security | 2. Organization of information security | 2. Awareness and training | 2. Inventory of software |
| 3. Information security governance and risk management | 3. Human resources security | 3. Audit and accountability | 3. Secure configurations for computers |
| 4. Software development security | 4. Asset management | 4. Security assessment and authorization | 4. Continuous vulnerability assessment and remediation |
| 5. Cryptography | 5. Access control | 5. Configuration management | 5. Malware defenses |
| 6. Security architecture and design | 6. Cryptography | 6. Contingency planning | 6. Application software security |
| 7. Security operations | 7. Physical and environmental security | 7. Identification and authentication | 7. Wireless device control |
| 8. Business continuity and disaster recovery planning | 8. Operations security | 8. Incident response | 8. Data recovery capability |
| 9. Legal, regulations, investigations and compliance | 9. Communications security | 9. Maintenance | 9. Security skills assessment and training |
| 10. Physical (environmental) security | 10. System acquisition, development, and maintenance | 10. Media protection | 10. Security configurations for network devices |
| | 11. Supplier relationships | 11. Physical and environmental protection | 11. Network ports, protocols and services |
| | 12. Information security incident management | 12. Planning | 12. Control of administrative privileges |
| | 13. Information security aspect of business continuity management | 13. Personnel security | 13. Boundary defense |
| | 14. Compliance | 14. Risk assessment | 14. Security audit logs |
| | | 15. System and services acquisition | 15. Need-to-know access control |
| | | 16. System and communications protection | 16. Account monitoring and control |
| | | 17. System and information integrity | 17. Data loss prevention |
| | | 18. Program management | 18. Incident response capability |
| | | | 19. Secure network engineering |
| | | | 20. Penetration testing and red team exercises |

c. *Application servers* By bypassing the encryption mechanisms and other protocol based protection methods in the existing system, applications in these servers might lead to potential breaches there by accessing the data.
d. *Systems administrators* If the attackers could identify and steal the authentication details of system administrators of railway infrastructure, they can steal data without leaving the trace on the systems and the organizations only know when they found out this breach from the media. In some cases, organizations use biometric technology to reduce this affect.

2. *Concede integrity-changing data* Generally, breaches in integrity are receiving less consideration than breaches in discretion. If one could change the data such as maintenance history and failure data, the immediate consequence could be accidents and derailments. The other far reaching consequence is that lot of algorithms are developed based on historical data (data-driven methods) for carrying out predictive operation and maintenance of the infrastructure and changes in the data results in incorrect predictions that could lead to chaos. Though these kind of attacks are few at the moment, but in the coming ages, they will grow in a sophisticated way. The various impacts that could lead to the integrity issues are:

a. Reputation of the organization.
b. Misreporting of the financial information that lead to incorrect decisions because of data-driven business decision methods.
c. Changes in the infrastructure information lead to accidents and derailments.
d. Indirect impacts will be increase in cost and reduction in safety.

3. *Availability-rejection of access* By rejecting or denying the access to the organization, the traffic managers cannot operate the trains to control and could lead to complete halt of operation. These specific attacks triggering denial of service can be hard to detect if systems are compromised but not disabled. Often the

systems are damaged when the attack lead to failures by operating systems and railway infrastructure. In broad, intentional attacks on the availability of data can be divided into three categories:

a. Distributed Denial of Service (DDoS) attacks are utilized to efficiently inactivate services in the organization.
b. Directed Denial of Service attacks comprise hacking into the target and then deactivating systems and hence they have to be reconstructed or mended with new facilities. This could lead to new investments within organization.
c. Physical Annihilation attacks contain cyberattacks with physical destruction of the assets. Due to the digitalization and advanced technologies, more complex systems are computer-controlled and these kind of attacks will be more perilous and destructive over time.

### 5.3 Threat model

Threats appear to be multifaceted and can be directed against specific assets, ranging from IPT (Intelligent public transport) systems to data, through to broad organizational structures and entire IPT infrastructures (Chernov et al. 2015). IPT operators lean more towards multifaceted threats affecting complex assets having both physical and digital characteristics. A threat model was proposed that regroups threats into seven threat categories (ENISA 2015):

- Physical and large scale attacks are intentional offensive actions, which aim to achieve maximum distraction, disruption, destruction, exposure, alteration, theft or unauthorized accessing of assets such as infrastructure, hardware, or ICT connections.
- Acts of nature and/or environmental incidents are serious disruptions of the functioning of a society and can be divided into those natural disasters not directly triggered by humans, and environmental disasters caused by humans.
- Accidental errors/malfunctions/failures are related to the condition of not functioning and/or insufficient functioning of any IT infrastructure assets.
- Disruption and/or outages are unexpected disruptions of services or significant decreases in expected quality, and can affect all kind of IPT assets.
- Nefarious activities and/or abuse are intentional actions that target IPT assets, ranging from systems and infrastructure to networks, by means of malicious acts with the aim to steal, alter, or destroy a specified target.
- Unintentional damage refers to the destruction, harm, or injury of property or people by accident.
- Insider threats are similar to nefarious activities, but originate from within the organization being attacked or targeted.

### 5.4 Cyber attacks

The possibility of different cyber-attacks with railway eMaintenance data can be shown in Table 2.

## 6 Challenges

Challenges in cybersecurity are growing on a day-to-day basis (Fischer 2016). According to Kumar et al. (2006) cybersecurity challenges include huge amount of data generated from various network-monitoring devices and necessity for new techniques for managing vulnerabilities and cyber alerts that will help to improve general computer security. The key challenges facing cyber security within IPT can be summarized in the following:

1. *Difficulties to integrate security for safety* Manufacturers and IPT operators usually prioritize the need for safety requirements, due to the fact that IPT operators experience difficulties in understanding the concept of (cyber) security, acquiring the necessary skills and developing the necessary measures to integrate security for safety in their systems.
2. *Inadequate importance and spending being afforded to cyber security* It indicated that transport organizations still do not grant the necessary importance to cyber security within their company. Spending on cyber security also appears to be inadequate in response to the range of multifaceted cyber threats affecting IPT.
3. *Inadequate checking for countermeasures* The majority of transport organizations do not measure the effectiveness of their countermeasures. This in turn produces a lack of awareness and knowledge in relation to what "works" and what "does not work" in cyber security for IPT.
4. *Unwillingness to collaborate and exchange information on cyber security* Overall, transport organizations are less than willing to collaborate on and exchange information about cyber security with other industry players, most likely because of the reputational costs, competitive pressures, awareness and other indirect losses related to cybercrime.
5. *Slow phasing out of legacy systems* The existence and use of legacy systems can weaken cyber security. However, the security and threat environment within IPT is beginning to shift towards connected transportation systems as they become increasingly interconnected to the wider world.

**Table 2** Cyber-attacks linked to the source of attacker, his intention and the compromised security element

| Cyber-attack | Source | Actor | Action | Security element |
|---|---|---|---|---|
| Tapping, snooping, scavenging, shoulder surfing and traffic analysis and traffic operational data. | Internal or external | Human | Malicious | Confidentiality |
| Modification, masquerading, replay and repudiation of acquired data | Internal or external | Human | Malicious | Integrity |
| Denial of service attacks, riot/civil disorder, arson, labor unrest, procedural violation | Internal or external | Human | Malicious | Availability |
| Careless use of wireless networks, posting information to discussion boards and blogs, sending sensitive information via e-mail and instant messaging, Improper disposal of sensitive media and failing to log off before leaving workstation | Internal | Human | Non-malicious | Confidentiality |
| Failure and maintenance data entry errors and omissions | Internal | Human | Non-malicious | Integrity |
| Programming errors, including syntax and logic problems | Internal | Human | Non-malicious | Availability |
| Compromising emanations, eavesdropping, takeover of authorized session | Internal or external | Technological | Non-malicious | Confidentiality |
| Jamming (telecomm) | Internal or external | Technological | Non-malicious | Availability |
| Faults in power supply and data networks | Internal | Technological | Non-malicious | Availability |
| Earthquakes, hurricanes, wind, flood, Tsunami, fire, lightning, animals and wildlife | External | Natural disaster | Non-malicious | Availability |

6. *Inadequate data exchange between IPT and Smart Cities operators* Data exchanges between IPT and different Smart Cities operators tend to be restricted, uncoordinated and ad-hoc. The potential implications of this uneven data exchange include weaker security as threats are not being communicated and there is uncertainty over who is responsible for the security of individual components within systems that integrate multiple stakeholders.
7. *Weak situational awareness of cyber threats* Due to the fast moving and interconnect nature of IPT, transport organizations are struggling to achieve a full awareness of the range of cyber threats and boundaries for securing the IPT landscape.
8. *Resistance to security adoption* One finding from the field work indicates that some countermeasures are widely adopted even though they are not considered effective (e.g. monitoring ICT systems for hardware and software faults), while others that are considered effective are frequently not deployed. This underlines a resistance to adapt within the IPT sector and a culture where things are done because operators are told to do them and/or have always done them rather than because they work.

## 7 Vulnerabilities

By implementing cyber-physical systems into critical infrastructures, IPT brings benefits but also introduces a new set of vulnerabilities and risks to operators and society as a whole. Historically, cyber and physical systems have operated fairly independently of one another, however, IPT is leading to an integration of both domains and therefore to a situation where the exploitation of cyber vulnerabilities can result in physical consequences. This brings both new vulnerabilities and risks. Since IPT is relatively new and on the making, information on IPT vulnerabilities mainly originates from research, requirements and generic assumptions.

### 7.1 General vulnerabilities

*Common to other IT systems* This category relates to areas that communally affect other IT systems (i.e. customer privacy and personal data, customer security and physical security and publicly accessible devices). This also includes vulnerabilities in commercially available mainstream IT products and systems.

- *Wireless and cellular communication* Wireless communication44 and cellular services introduce all the typical vulnerabilities in the area of communication conducted between points not connected by an electrical conductor. For example, inadequate security protocols, inadequate authentication mechanisms, energy constrain, poor security and unreliable communication.
- *Integration of physical and virtual layers* The physical and virtual layers are becoming increasingly permeable as cyber and physical systems become networked and remotely accessible.

- *Cohabitation between legacy and new systems* IPT evolves at different rates among operators because of several factors including; resource availability, user preferences, and scale and accessibility. Inconsistency of IPT technologies introduces new vulnerabilities. Blind-spots may emerge in areas where legacy equipment and infrastructures are still used.
- *Increased automation* While the process of removing or limiting human interaction for IPT systems through increased automation improves safety by removing the possibility of human error, it also introduces new potential vulnerabilities. These include, but are not limited to: an increased number of system access points and, therefore, potential attack vectors; skill atrophy; cascading failures; and changes in emergency response plans.

### 7.2 Specific vulnerabilities

*Scale and complexity of transportation networks* This refers to the difficulty of mapping the entire IPT system and the difficulty of securing the connectivity of mobile devices within transportation networks. Other issues include; the need to trust components and participants within the network, working with teams with different skills and competences, and the effective involvement of multiple stakeholders.

- *Applying networked technology across large transport systems* This leads to a large number of system access points stemming from the presence of networked technology across these large systems, which in turn increase both the difficulty and cost of properly securing each system device.
- *Multiple interdependent systems* This refers to the burden of ensuring the smooth interfacing, communication, and security among interdependent systems. These diverse systems include; sensors, computers, payment systems, financial systems, emergency systems, ventilation systems, automated devices, power relays, etc.
- *Access to real-time data* IPT requires nonstop access to real-time data which in turn leads to higher costs associated with maintenance and service downtime and therefore increased vulnerability.
- *Higher volumes of passengers and freight* This refers to logistical and security hurdles of physically accommodating enormous volumes of passengers and freight, along with the reality that security breaches could result in public safety risks.
- *Online passenger services* The online provision of passenger services that historically have only been available offline, means these functions and now susceptible to all the associated cyber risks.

## 8 Risks

### 8.1 Business risks

Business risks usually affect different and multiple components due to dependencies in the affected IPT assets.

1. *Impact on operations* When operations are impacted, service usually follows a degraded mode. Specific actions are needed to recover operations, usually in a limited timeframe.
2. *Loss of revenue* In the case of an incident, operations can become limited or suspended, which leads to some loss revenues.
3. *Impact on reputation/loss of trust* In the case of major service disruptions, risks can also cover reputational damage and the loss of revenue which can directly impact a company's bottom line.
4. *Non-compliance with the regulation on data protection* The disclosure of personal data, voluntarily or not, is covered by regulation.
5. *Risks on hardware and software* Risks related to the manipulation or destruction of IPT components, hardware and software impact the stability and availability of the IPT systems.
6. *Reliance on invalid information* The area of multiple interdependent systems is also becoming a more relevant source of concern as traffic operators become more interconnected with each other and with other smart operators.
7. *Lack of security of dependencies* The more IPT is moving towards "a system of systems", the more important is to understand the dependencies among involved components.
8. *Unavailability of a dependency* The IPT service depends on several internal and external dependencies. Hence, the IPT service may suffer from the unavailability of a dependency and become unavailable.

### 8.2 Societal risks

Societal risks are mainly triggered by the manipulation and destruction of IPT components

1. *Effective transportation systems are vital to society* enabling the movement of passengers and goods and noteworthy impacts on economic, social and environment factors.

2. *Unavailability of the IPT service* Given the nature of societal assets, these components tend to be integrated systems which are shared among multiple stakeholders. This amplifies the interdependency effect and consequently increases the risk that such events will lead not only to interrupted and disrupted transport services.
3. *Disruption to the society* Incident on the transport system will bring disruption to the society with several impacts on the economy and the life of the citizens. In case of severe network gridlocks, societal financial losses and slower economic growth could also occur.
4. *Passengers' health and safety* Passengers safety in IPT is the priority of all actors. Yet, specific incidents may impact the transport system and bring a risk to health and safety (e.g. derailing train…).
5. *Environmental impact* The reliance on ICT assets to control energy assets (e.g. fuel, gas, electricity) may lead to increased energy consumption with an environmental impact.
6. *Confidentiality and privacy* The increased use of sensing, tracking, real-time behavior evaluation and automated decisions within IPT raises new risks against the confidentiality and privacy of citizens.

## 9 Conclusion and future work

There is increasing trend on emphasis of cybersecurity, especially in area of IT and information systems. Due to digitalization of railway systems, those issues with IT is bundled with the issues related to the physical infrastructure. Hence, this paper raises several threats, challenges, vulnerabilities and risks in the railway infrastructure. Some of the existing methods to secure the data is also briefed. Due to above aforementioned factors, there is a necessary need to concentrate on the issues of cybersecurity in railways. Being maintenance as important factor in the railways, there is a vital need for incorporating cybersecurity protection systems to reduce these threats and vulnerabilities in eMaintenance platform. The extension of this work is to develop a comprehensive framework with including all the above issues into account. A pilot case study is also being considered to implement secure protection methods with the above platform.



## References

Ahrens J, Hendrickson B, Long G, Miller S, Ross R, Williams D (2011) Data-intensive science in the US DOE: case studies and future challenges. Comput Sci Eng 13(6):14–24

Álvarez A, Ioannidis S, Schlehuber C, Rodríguez F, Vallero V (2017) CIPSEC Project [Online]. https://upcommons.upc.edu/handle/2117/106378

Bastow MD (2014) Cyber security of the railway signalling & control system. IRSE ASPECT

Bloomfield R, Bendele M, Bishop P, Stroud R, Tonks S (2016) The risk assessment of ERTMS-based railway systems from a cyber security perspective: methodology and lessons learned. In: International conference on reliability, safety and security of railway systems. Springer, pp 3–19

Bullock A (1999) Space: spatial access control for collaborative virtual environments. Doctoral dissertation, University of Nottingham

Cao N, Wang C, Li M, Ren K, Lou W (2014) Privacy-preserving multi-keyword ranked search over encrypted cloud data. IEEE Trans Parallel Distrib Syst 25(1):222–233

Cappelli DM, Moore AP, Trzeciak RF (2012) The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (Theft, Sabotage, Fraud). Addison-Wesley, Boston

CARONTE project: creating an agenda for research on transportation security. In: CIT2016—XII Congreso de Ingeniería del Transporte, València, Universitat Politècnica de València (2016)

Chernov AV, Butakova MA, Karpenko EV (2015) Security incident detection technique for multilevel intelligent control systems on railway transport in Russia. In: 23rd Telecommunications forum telfor (TELFOR), 2015. IEEE, pp 1–4

Covington MJ, Long W, Srinivasan S, DEV AK, Ahamad M, Abowd GD (2001) Securing context-aware applications using environment roles. In: Proceedings of the sixth ACM symposium on access control models and technologies 2001. ACM, pp 10–20

Donaldson S, Siegel S, Williams CK, Aslam A (2015) Enterprise cybersecurity: how to build a successful cyberdefense program against advanced threats. Apress, New York

Edwards WK (1996) Policies and roles in collaborative applications. In: Proceedings of the 1996 ACM conference on computer supported cooperative work 1996. ACM, pp 11–20

ENISA (2015) Cyber security and resilience of intelligent public transport. Good practices and recommendations, European Union Agency for Network and Information Security. https://www.enisa.europa.eu/publications/good-practices-recommendations. Accessed 25 Feb 2018

Fischer EA (2016) Cybersecurity issues and challenges: in brief. Congressional research service

CSA Top Threats Working Group (2016) The treacherous 12: cloud computing top threats in 2016. Cloud Security Alliance (CSA), Feb

Hashem IAT, Yaqoob I, Anuar NB, Mokhtar S, Gani A, Khan SU (2015) The rise of "big data" on cloud computing: review and open research issues. Inf Syst 47:98–115

ISO/IEC (2007) 27001:2005, Information technology—security techniques—information security management systems—requirements

Itani W, Kayssi A, Chehab A (2009) Privacy as a service: privacy-aware data storage and processing in cloud computing architectures. In: Eighth IEEE international conference on dependable, autonomic and secure computing, 2009, DASC'09. IEEE, pp 711–716

Karim R (2008) A service-oriented approach to e-maintenance of complex technical systems (Doctoral dissertation, Luleå tekniska universitet)
Katal A, Wazid M, Goudar RH (2013) Big data: issues, challenges, tools and good practices. In: Sixth international conference on contemporary computing (IC3), 2013. IEEE, pp 404–409
Kissel R (2013) Glossary of key information security terms. NIST Interagency Reports NIST IR, 7298(3)
Kostopoulos G (2017) Cyberspace and cybersecurity. CRC Press, Boca Raton
Kotenko IVE, Saenko IB, Chernov AV, Butakova MA (2013) The construction of a multi-level intelligent information security system for automated systems of railway transport. Trudy SPIIRAN 30:7–25
Kumar V, Srivastava J, Lazarevic A (eds) (2006) Managing cyber threats: issues, approaches, and challenges, vol 5. Springer, Berlin
Levy-Bencheton C, Darra E (2015) Cyber security and resilience of intelligent public transport: good practices and recommendations. ENISA, Heraklion
Lin HY, Tzeng WG (2012) A secure erasure code-based cloud storage system with secure data forwarding. IEEE Trans Parallel Distrib Syst 23(6):995–1003
Marston S, Li Z, Bandyopadhyay S, Zhang J, Ghalsasi A (2011) Cloud computing—The business perspective. Decis Support Syst 51(1):176–189
Masson É, Gransart C (2017) Cyber security for railways–a huge challenge–Shift2Rail perspective. In: International workshop on communication technologies for vehicles. Springer, Cham, pp 97–104
Matt B (2006) Introduction to computer security. Pearson Education India
Nagurney A, Daniele P, Shukla S (2017) A supply chain network game theory model of cybersecurity investments with nonlinear budget constraints. Ann Oper Res 248(1–2):405–427
Nowakowski W, Bojarczak P, Łukasik Z (2017) Performance analysis of data security algorithms used in the railway traffic control systems. In: International conference on information and digital technologies (IDT), 2017. IEEE, pp 281–287
Priscoli FD, Giorgio AD, Esposito M, Fiaschetti A, Flammini F, Mignanti S, Pragliola C (2017) Ensuring cyber-security in smart railway surveillance with SHIELD. Int J Crit Comput Based Syst 7(2):138–170
PROTECTRAIL (2014) Key Lessons for the Railway Sector on PROTECTRAIL Security Architecture, White Paper
Sandhu RS, Samarati P (1994) Access control: principle and practice. IEEE Commun Mag 32(9):40–48
SECRET (2015) Security of railways against electromagnetic attacks, White Paper
SECUR-ED (2014) SECured URban transportation–European Demonstration, White Paper
Shi H (2014) Railway information sharing platform security requirements analysis. In: ICLEM 2014: system planning, supply chain management, and safety. pp 1116–1121
Smith M, Szongott C, Henne B, Von Voigt G (2012) Big data privacy issues in public social media. In: 6th IEEE international conference on digital ecosystems technologies (DEST), 2012. IEEE, pp 1–6
Söderholm P, Karim R (2010) An enterprise risk management framework for evaluation of eMaintenance. Int J Syst Assur Eng Manag 1(3):219
Thales (2016) Cybersecurity for rail: not a single-shot approach, applying the NIST approach to rail transportation, White Paper
The Local (2017) https://www.thelocal.se/20171012/swedish-transport-agencies-targeted-in-cyber-attack. Accessed 11 Jan 2018
Thomas RK (1997) Team-based access control (TMAC): a primitive for applying role-based access controls in collaborative environments. In: Proceedings of the second ACM workshop on role-based access control 1997. ACM, pp 13–19
Thomas RK, Sandhu RS (1998) Task-based authorization controls (TBAC): a family of models for active and enterprise-oriented authorization management. Database security XI. Springer, Berlin, pp 166–181
Tolone W, Ahn G, Pai T, Hong S (2005) Access control in collaborative systems. ACM Comput Surv (CSUR) 37(1):29–41
Wegner A, Graham J, Ribble E (2017) A new approach to cyberphysical security in industry 4.0. In: Thames L, Schaefer D (eds) Cybersecurity for industry 4.0. Springer, Berlin, pp 59–72
Wijesekera D, Jajodia S (2003) A propositional policy algebra for access control. ACM Trans Inf Syst Secur (TISSEC) 6(2):286–325
Willett KD (2008) Information assurance architecture. CRC Press, Boca Raton
Yu S, Wang C, Ren K, Lou W (2010) Achieving secure, scalable, and fine-grained data access control in cloud computing. In: proceedings IEEE Infocom, 2010. IEEE, pp 1–9
Zhang X, Liu C, Nepal S, Pandey S, Chen J (2013) A privacy leakage upper bound constraint-based approach for cost-effective privacy preserving of intermediate data sets in cloud. IEEE Trans Parallel Distrib Syst 24(6):1192–1202
Zissis D, Lekkas D (2012) Addressing cloud computing security issues. Future Gener Comput Syst 28(3):583–592