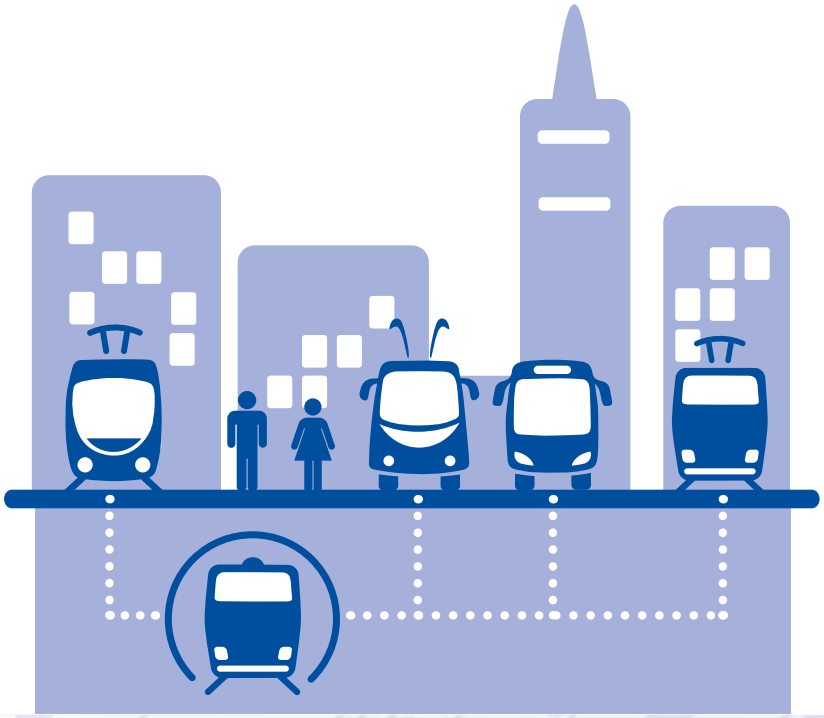


Cyber Security and Resilience of Intelligent Public Transport

Good practices and recommendations

DECEMBER 2015

www.enisa.europa.eu European Union Agency For Network And Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its Member States (MS), the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU MS in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU MS by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

Dr. Cédric LÉVY-BENCHETON, Ms. Eleni DARRA (ENISA)

Contact

For contacting the authors please use resilience@enisa.europa.eu.
For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

Dr. Timothy MITCHENER-NISSEN (Trilateral Research)
Dr. Monica LAGAZIO (Trilateral Research)
Dr. Daniel BACHLECHNER (Fraunhofer ISI)
Dr. Michael FRIEDEWALD (Fraunhofer ISI)
Mr. Antonio KUNG (Trialog)

ENISA would like to acknowledge all participants to the study. In particular, ENISA would like to thank the following experts for their contribution (in alphabetical order):

Mrs. Lindsey BARR MANCINI (UITP)
Ms. Luana BIDASCA (European Transport Safety Council)
Mr. Carl-Johan BOSTORP (Stockholm Public Transport)
Mr. Leon BRAIN (DG MOVE)
Mr. Daniele CATTEDDU (Cloud Security Alliance)
Mr. Patrick CHAMBET (Métropole Nice Côte d'Azur)
Mr. Gino CORMONS (Regione Autonoma Friuli Venezia Giulia)
Mr. Christopher J. COX (Metroselskabet I/S)
Dr. Alexander DIX (German Data Protection Agency)
Mr. Ignasi FONTANAL (Opticits)
Mr. Sergey GORDEYCHIK (Securing Smart Cities / Kaspersky Lab)
Ms. Michele HANSON (Transport for London – TfL)
Eng. Francois HAUSMAN (UNIFE)
Ms. Alena HAVLOVÁ (CER)
Mr. Thomas KRITZER (Wiener Linien)
Mr. Mariano LAMARCA LORENTE (Barcelona City Council – BCN.cat)
Mr. Joe PICHLMAYR (Cyber Security Austria)
Mr. José PIRES (International Union of Railways – UIC)

Mr. David PRIOR (Xuvasi Ltd.)
Ms. Stefanie PROOST (De Lijn)
Mr. Maxime RAPAILLE (STIB - MIVB Brussels public transportation)
Mr. Luis RODA (Empresa Municipal de Transportes de Valencia – EMT)
Mr. Bernardo RODRIGUES (London's European Office)
Mr. Jean-Luc SALLABERRY (FNCCR)
Mr. Stephen SMITH (ECSA)
ir. Andre SMULDERS, CISSP (Senior Business Consultant Security, TNO)
Ms. Andrea SOEHNCHEN (UITP)
Mr. Frank VAN STEENWINKEL (Fidecity)

ISBN: 978-92-9204-146-5 | doi:10.2824/778225

Table of Contents

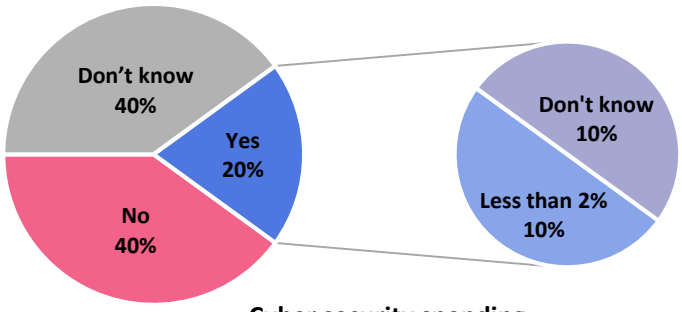
Executive Summary

The concept of "Smart Cities" revolves around the interconnection of different operators from domains of activity such as public transport, energy… These operators rely on Information and Communication Technology (ICT) systems to retrieve, process, and exchange data in order to improve their services and the quality of life of citizens.

In this context, public transport operators have an important role to enable this smartness. They contribute to the life of the city, to the economy and ensure the resilience of the Smart City. The integration of several ICT systems enables "Intelligent Public Transport" (IPT), where cyber-physical devices, communication networks and central servers optimise the transport service up to a certain degree of automation.

While this fusion of cyber technology, physical infrastructures and mass transport vehicles creates new opportunities for improving services and functionality, it also has the effect of introducing cyber security risks into transport networks that have not historically been susceptible to such risks. Moreover, IPT becomes a natural target for emerging cyber threats that will have an impact not only on the operations of the transport service but also on the whole economy and potentially on the health and safety of citizens.

For that reason, it is important to consider security for Intelligent Public Transport to protect the operators, the economy and the life and safety of citizens. However, IPT faces several challenges in this direction: there is currently no EU policy on cyber security for transport, the awareness level is low and it is difficult for operators to dedicate budget to this specific objective of cyber security (see picture on the right).



Cyber security spending

This study proposes a pragmatic approach that will highlight the critical assets of Intelligent Public Transport systems. It gives an overview of the existing security measures (good practices) that could be deployed to protect these critical assets and ensure security of the IPT system, based on a survey and interviews of experts from the sector, municipalities, operators, manufacturers and policy makers.

The good practices propose a first step toward actionable security and a better protection of the transport ecosystem. Good practices go beyond technical security measures; they also integrate policies, standards, operational and organisational measures. For example, transport operators can use this study in support of their risk assessment in order to understand which critical assets to protect, and how.

In spite of the fact that security becomes a concern for all actors of Intelligent Public Transport, additional efforts are still needed to improve the current situation. Following that direction, the study proposes recommendations to three stakeholders groups that need to enhance the status of cyber security for IPT. For that purpose:

Decision makers in the European Commission and in Member States should:

- Promote public/private collaboration on IPT cyber security at national level and EU-wide
- Promote and facilitate the development of a common EU approach to IPT security
- Develop a comprehensive EU strategy and framework for cyber security in IPT
- Integrate and converge security efforts made in other sectors of activity
- Foster the development of harmonised cyber security standards for IPT

Intelligent Public Transport operators should:

- Integrate cyber security in their corporate governance
- Develop and implement an integrated corporate strategy addressing holistically cyber security and safety risks
- Implement risk management for cyber security in multi-stakeholder environments including external contractors and dependencies
- Clearly and routinely specify their cyber security requirements
- Annually review organisational cyber security processes, practices and infrastructures

Manufacturers of IPT systems and solutions should:

- Create products/solutions that match the cyber security requirements of IPT end-users
- Collaborate in the development of IPT-specific standards and apply them to IPT solutions
- Develop a trusted information sharing platforms on risks and vulnerabilities
- Provide security guidance for your systems, products and solutions

1. Introduction

Transport networks are designated as *critical infrastructure* within the European Union (EU) and are essential for maintaining the health, safety, security, and social and economic well-being of citizens within EU Member States (MS).[1] Yet the effective operation of these transport networks is vulnerable to the increasing levels of traffic, which also contribute to rising energy consumption and environmental and social problems.[2] These negative symptoms are strongly felt in European cities which draw together large concentrations of citizens within relatively small geographic areas.

To help manage and mitigate increases in traffic congestion, cities rely upon effective public transport networks as efficient mobility solutions. However, when seeking to expand and improve these public transport networks it is not enough to count solely upon the traditional measure of simply increasing the physical road and rail infrastructure. Rather technological innovation has a major role to play here in the creation of appropriate solutions, and the realisation of this fact is directly connected with the rise of *Intelligent Transport Systems* (ITS) integrated into *Smart Cities*.[3]

ITS integrates information and communication technology (ICT) with transport engineering so as to plan, design, operate, maintain and manage transport systems, which in turn significantly contribute to improving the efficiency and operation of such networks.[2] The application of these technologies to public transport systems produces *Intelligent Public Transport* (IPT).

However, this process of increasing the incorporation of ICT into public transport through both the introduction of networked devices and the expansion of remote access and control capabilities, coupled with the linking together of different operators within a single Smart City network (creating a *system-of-systems*), all acts to increase the cyber threat exposure of traditional transport networks. While current transport operators and engineers possess a wealth of knowledge and experience in ensuring their networks and products are designed with *safety* in mind, they have less experience in ensuring the cyber *security* of their networks and products.

This increase in the cyber security risks for IPT produces new objectives that need to be met. These include the identification of critical IPT assets and the associated threats that target them, as well as the identification of good practices in cyber security that can address these threats and increase the cyber resilience of IPT operators. Such outcomes need to be coupled with a coherent strategic and policy approach that encompasses all of the stakeholders linked to IPT within the Smart City environment.

[1] See Council Directive 2008/11/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, specifically Art.2 and Annex I
[2] See Directive 2010/40/EU of the European Parliament and of the Council on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport.
[3] Smart Cities are cities that integrate ICT to meet public needs and foster development in a multi-stakeholder environment. It is anticipated this integration of cyber-physical technologies and infrastructures creates environmental and economic efficiencies while improving resident's quality of life (see US Dept. of Homeland Security, "The Future of Smart Cities: Cyber-Physical Infrastructure Risk", August 2015).

1.1 Scope of the study

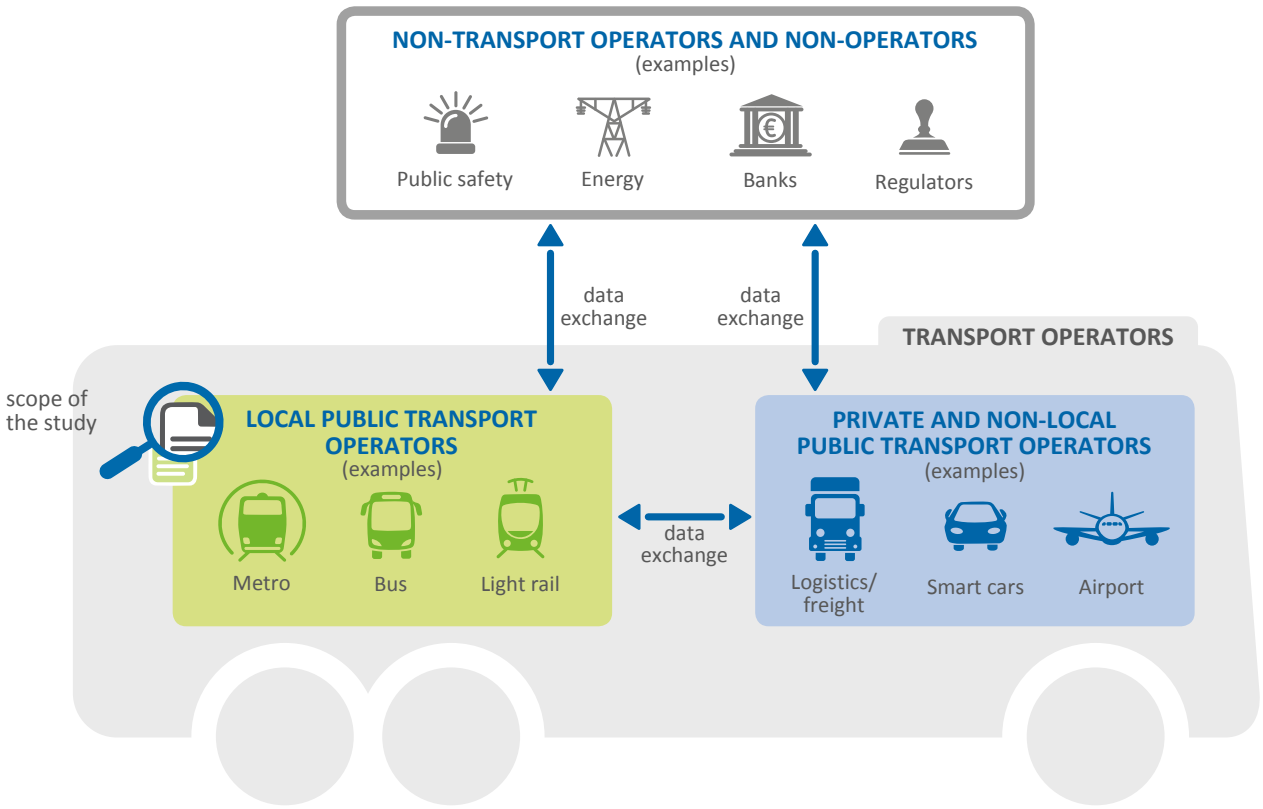
This study focuses on the protection of the assets critical to Intelligent Public Transports in the context of Smart Cities. These assets are considered critical as they contribute to the normal operation of local public transport networks, including metro, buses, light rail and other modes of mass public transport found in Smart Cities.

For that purpose, this study identifies these critical assets from a business and societal point of view. It highlights good security practices against cyber threats. The objective is to enhance the resilience of IPT. From the point of view of Smart Cities, these assets can be considered "internal" to IPT operators.

Figure 1 defines the scope of the study by focusing on the critical assets of local public transport operators (displayed in the green box). The scope does not consider a specific architecture but rather a comprehensive list of assets owned by an IPT operator.

The protection of critical assets for other transport operators (private and non-local), operators from other sectors and non-operators fall out of the scope of this study. The protection of data exchange between IPT operators and other stakeholders is also out of scope of this study. ENISA study "Cyber Security for Smart Cities - an architecture model for public transport"[4] focuses on the protection of this data exchange and its associated assets.

Figure 1: Scope of the study



[4] ENISA, "Cyber Security for Smart Cities - an architecture model for public transport", December 2015. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/smart-infrastructures/intelligent-public-transport/architecture-model-transport-smart-cities

1.2 Target audience

The interconnected network of actors facilitates the operation of IPT within a Smart City environment. Hence, the task of developing secure and resilient IPT systems falls on multiple actors, requiring the cooperation of both public and private stakeholders working together to enhance cyber security. Given this fact, the target audiences of this study are drawn from a number of sectors (see Figure 2):

Figure 2: Target audience groups

- **Operators:** they cover a wide range of actors; both those directly involved in operating different public transport modes (metro, bus, tram/trolley-bus, light rail, ferry) and an interconnected network of operators within the Smart City (energy, infrastructure, public & private clouds, communications, banks and payment systems, etc.).
- **Manufacturers:** Covering the full spectrum of manufacturers including physical transport infrastructure, providers, vehicle manufacturers, developers of ICT networks, hardware and software engineers, etc.
- **Service Providers:** Including risk managers, cloud providers, ICT network providers, security providers, etc.
- **Policy Makers:** Different levels of government (local, national, EU), regulators and law enforcement agencies involved in IPT.

1.3 Methodology

This study is based on a combination of desktop research as well as empirical research (*i.e.* survey and interviews) with the results validated through a stakeholder workshop. Initial data gathering scoped the development of the study, including the current key policies and legislation. Critical societal and business assets for IPT were identified by integrating the desktop and empirical findings, and a comparative approach was employed (*i.e.* between threats, risks, vulnerabilities, good practices, and challenges and gaps) focussing on enhancing cyber security within IPT.

Results of the desktop research were further developed, and good practices identified, through an online survey[5] and series of interviews involving a total of 22 respondents drawn from different stakeholder groups.[6] While this is sample size is limited it nevertheless represents a good starting point for conducting research into IPT. These respondents were based in the following EU MS:

- Belgium
- Denmark
- Estonia
- France
- Germany
- Latvia
- Luxembourg
- Netherlands
- Republic of Ireland
- Spain
- Sweden
- United Kingdom

[5] See Annex 5 for the survey questions.
[6] See Section 1.3 of ENISA, "Cyber Security for Smart Cities - an architecture model for public transport", December 2015, for a distribution of respondents based on sector.

The findings and recommendations of this study were validated through a final workshop of IPT operators, Smart City municipalities and policy makers.

1.4 Outline

This study is structured as follows:

- **Section 1 – Introduction**: introduces the topic and provides an outline of the study, the target audiences and the methodologies employed.
- **Section 2 – The Intelligent Public Transport environment**: provides the contextual environment for IPT, including the key legislative environment, critical business and societal functions for IPT, and key assets.
- **Section 3 – A need to secure IPT**: identifies and organises the key cyber threats affecting the critical assets of IPT operators. The cyber threat vulnerabilities inherent to IPT are identified and discussed, and an initial analysis of risks is conducted.
- **Section 4 – Good practices for securing Intelligent Public Transport**: good practices for securing IPT networks from cyber threats are presented here, as identified through both desktop research and the interviews/surveying of IPT operators.
- **Section 5 – Gap analysis**: The identification and analysis of existing gaps in securing IPT (arising from existing policies, legislation, operational practices and employed technologies) identified throughout this research via a comparative analysis of previous findings.
- **Section 6 – Recommendations**: Sets out nine key recommendations for policy makers, IPT operators, manufacturers and solution providers on enhancing the security and resilience of IPT.

2. The intelligent public transport environment

This section provides an overview of the IPT environment. It defines terms commonly used within this sector, outlines the current legal and policy environment within which IPT operates, places IPT within the wider smart environment, sets out the critical functions and assets for IPT operators, and finally it explains why cyber security is so fundamentally critical in the physical-digital fusion that is IPT.

2.1 Definitions

Many of the common concepts within intelligent transport are the subject of multiple definitions provided by different stakeholders, each with differing perspectives and agendas. These have been distilled here to produce a single set of definitions describing how these concepts are approached within this study. Table 1 defines the terms employed throughout this study.

Table 1: Key definitions employed within this study

TERM	DEFINITION
Intelligent Transport	The application of information and communication technologies to transport so as to improve levels of service and efficiency.
Intelligent Public Transport[7] ***(IPT)***	The application of information and communication technologies to public transport networks so as to improve levels of service and efficiency.
Intelligent Transport Systems (ITS)	The application of information and communication technologies to the real-time management of vehicles and networks involving the movement of people and goods.[8] [9] [10]
Smart City	A city that uses ICT to meet public needs and foster development in a multi-stakeholder environment.
Business critical (as applied to IPT)	Any elements which can directly impact the execution and sustainability of a business in the long-term, including business revenue, service provision, business operations, and/or the brand and image of an organisation.
Societal critical (as applied to IPT)	Any elements affecting the quality of life of the citizens and their daily experience of transport, which includes the environment, their safety and security and their privacy.
Critical Infrastructure (as applied to the EU)	An asset, system or part thereof located in MS which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a MS as a result of the failure to maintain those functions.[11]

[7] Intelligent Public Transport is not a term widely used or adopted, rather it is a term coined for this study.
[8] EC,16.12.2008 COM(2008) 886 final, "Action Plan for the Deployment of Intelligent Transport Systems in Europe".
[9] EC, 20.3.2009 COM(2008) 886 final/2, "Corrigendum to Action Plan for the Deployment of Intelligent Transport Systems in Europe".
[10] Federal Ministry for Economic Cooperation and Development (Germany), "Intelligent Transport Systems", p.2.
[11] As defined within Article 2a of Directive 2008/114/EC. For more details on critical infrastructure see ENISA, "Methodologies for the identification of Critical Information Infrastructure assets and services", February 2015.

TERM	DEFINITION
Cyber security	Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.
IPT Cyber security	For IPT, cyber security is the protection of data, systems, infrastructure and end-users vital to the transport network, its operation and stability.

2.2 EU policy context

At the EU regulatory level, Regulations and Directives have yet to be specifically drafted to govern the form and operation of IPT. Instead, what currently exists are a number of Directives whose broader remits are, to differing degrees, applicable to IPT. These existing Directives cover the protection of personal data,[12] the processing of personal data in the electronic communications sector,[13] the promotion of clean and energy-efficient road transport vehicles,[14] creating interoperability of national rail systems across the European Community,[15] and the deployment of intelligent transport systems in the field of road transport.[16] Individual analyses of these Directives is provided in Annex 1.

Collectively these Directives demonstrate that while there is currently no piece of EU legislation focussing specifically on the operation of IPT at the EU level, there are elements of IPT operations that are still subject to a level of regulation. Despite this fact, when it comes to either cyber security protections, requirements and/or guidance specific to IPT, these Directives have very little to say beyond a cursory mention of general *security* and the need to protect *in-vehicle communications* in Directive 2010/40/EU,[17] and the need to protect the data privacy rights of citizens in Directives 1995/46/EC and 2002/58/EC.[18] There is the proposed Network Information Security (NIS) Directive[19] which, if enacted, will place a duty on

https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/Methodologies-for-identification-of-ciis

[12] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:l14012

[13] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1440673681836&uri=CELEX:32002L0058

[14] Directive 2009/33/EC of the European Parliament and of the Council of 23 April 2009 on the promotion of clean and energy-efficient road transport vehicles. http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1440673932348&uri=CELEX:32009L0033

[15] Directive 2008/57/EC of the European Parliament and of the Council of 17 June 2008 on the interoperability of the rail system within the Community. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008L0057

[16] Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport. http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1440674103143&uri=CELEX:32010L0040

[17] Art.2(1), Directive 2010/40/EU

[18] Art.10, Directive 2010/40/EU

[19] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union (COM/2013/048 final - 2013/0027 (COD)). http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52013PC0048

operators of critical infrastructures (including transport) *to manage the risks posed to the security of the networks and information systems which they control and use in their operations*.[20] While this Directive will apply to IPT operators, the level of impact is uncertain as again it is not primarily focussed on the operation of IPT.[21]

At the national level, while Member States need to ensure these Directives are incorporated into their respective legal systems, they are free to go beyond existing EU legislation by establishing additional national measures to promote IPT and cyber security.[22]

Running parallel with these Directives are a number of important EU policy documents acting to drive the future development of IPT. These have appeared with regularity since the late 2000's focussing on *Intelligent Transport* and its integration within *Smart Cities*, and they indicate the importance being assigned to these topics at the EU level. These policy documents include the following:[23]

- **Action Plan for the Deployment of Intelligent Transport Systems in Europe**: This Action Plan aims to accelerate and coordinate the deployment of Intelligent Transport Systems (ITS) in road transport, including interfaces with other transport modes.[16]
- **Internet of Things - An action plan for Europe**: Sets out 14 "Lines of Action" regarding the future design of objects/systems falling under the Internet of Things (IoT).[24]
- **A Digital Single Market Strategy Europe**: Sets out the Commission's strategy for creating a Digital Single Market whereby the free movement principles of goods, services, people and capital are translated and implemented into EU cyber space.[25]
- **European Innovation Partnership on Smart Cities and Communities: Strategic Implementation Plan**: Presents the Strategic Implementation Plan for creating Smart Cities produced by the High Level Group of the European Innovation Partnership for Smart Cities and Communities.[26]
- **Roadmap to a Single European Transport Area – Towards a competitive and resource efficient transport system**: Focus is on how to remove barriers and bottlenecks so as to complete the *internal market for transport* by creating a competitive and sustainable transport market within the EU.[27]

---

[20] Art.14(1), Proposed NIS Directive

[21] When multiple operators (including IPT operators) are integrated into the architecture of a Smart City it is uncertain to what extent they *control* any shared network and information systems. Additionally the scope assigned to *transport* as critical infrastructure within the proposed Directive as currently drafted in Annex II of the draft NIS Directive does not clearly apply to road-based IPT operators (*i.e.* busses).

[22] For example, it was noted during the final validation workshop that the French Agence nationale de la sécurité des systèmes d'information (ANSSI) is working with Vital Importance Operators such as public transport and railways to establish laws related to cyber security.

[23] See Annex 1: Key EU legislation and policy/strategy documents affecting IPT, for more details on these documents.

[24] Internet of Things - An action plan for Europe - COM(2009) 278 final. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0278:FIN:EN:PDF

[25] A Digital Single Market Strategy for Europe - COM(2015)192 final. http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_en.pdf

[26] European Innovation Partnership on Smart Cities and Communities: Strategic Implementation Plan. http://ec.europa.eu/eip/smartcities/files/sip_final_en.pdf

[27] Roadmap to a Single European Transport Area – Towards a competitive and resource efficient transport system - COM(2011) 144 final. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:tr0054

- **Rolling plan for ICT Standardisation**: This Rolling Plan provides a multi-annual overview of the needs for preliminary or complementary ICT standardisation activities to undertake in support of EU policy activities.[28]
- **Smart Cities and Communities – European Innovation Partnership**: These are partnerships across the areas of energy, transport and information and communication with the objective to catalyse progress in areas where energy use, mobility and transport, and ICT are intimately linked.[29]

What is most telling is that many of the EU policy and strategy documents within IPT have moved beyond simply seeking to educate the reader about IPT and/or justifying the development of this capability, and on to promoting concrete actions and outcomes through the use of action plans and/or the setting of specific objectives. This represents the level of acceptance IPT has achieved within the EU.

However, an EU policy specific to the development and security of IPT as a whole is still lacking. Instead the focus of these documents is primarily to promote the uptake and development of ITS, IoT, ICT, Smart Cities. Yet, there is no related policy on the cyber security requirements for the operators of such systems.

2.3 Critical business and societal functions and assets for intelligent public transport

2.3.1 Asset groups

In order to identify the key IPT assets, based on the field work we have extrapolated key functions and their relevant specific assets from a business and societal prospective. Successfully managing an IPT business requires identifying and protecting those functions that are critical to the effective, continued operation of that business: *i.e. business critical functions*. Given the role and importance of IPT networks to citizens and societies, there are also functions that are critical from a societal perspective; *i.e. societal critical functions*. Within each of these business and societal functions are individual *assets* related to the provision of that function. Through the survey, interviews as well as desktop research covering key documents, the following five business and five societal functions were identified.

Business functions:

- **Traffic and vehicle management** defines IPT through the use of ICT, and underlies its goals of increasing efficiencies and productivity through the linking of systems and employing data. As a result this function contains a long list of related assets covering the full digital-physical spectrum. This mirrors the societal function “sustainable urban mobility”.
- **Transportation safety and security** focuses on ensuring the effective cyber/physical security and safety of IPT infrastructures (including both physical and digital entities) attached to the business operations of the IPT operator. As such the assets range from cyber protection measures (*i.e.* ensuring the confidentiality, integrity and availability of data and communications) to access controls to both physical and digital assets.
- **Sales, fees and charges** are essential to the continuing financial viability of an IPT operator, whether privately or publically owned. Protecting the payment system assets is therefore of fundamental importance.

[28] Rolling plan for ICT Standardisation. https://ec.europa.eu/digital-agenda/en/news/rolling-plan-ict-standardisation-0

[29] Smart Cities and Communities – European Innovation Partnership - COM(2012) 4701 final. http://ec.europa.eu/eip/smartcities/files/ec_communication_scc.pdf

- **Resilient management structure** allows an IPT operator to respond effectively to, and overcome, the range of threats IPT networks are subject to, including: acts of nature, cyber attacks, physical attacks, energy supply problems, etc. Staff and business reputation are important assets here.
- **Energy and environment** concerns have a direct impact on the operation of IPT networks. Operators need to ensure the sufficient and continuous supply of energy to meet their network's needs. While at the same time they must manage energy usage to control costs and mitigate any negative environmental impacts arising from their transport network. This function also mirrors the societal function "sustainable environment".

Societal functions:

- **Sustainable urban mobility** networks are fundamental to the efficient operation of a city, providing a wealth of social and economic benefits. Incorporating ICT into the operation of traditional mobility networks to create IPT acts to maximise the efficiency, operation and sustainability of these mobility networks. This is fundamental in differentiating IPT from the traditional silo-based model of an urban public transport system. This infusion of ICT into the physical infrastructure and assets of different operators enables the integration of wider systems and processes. The critical assets to this function now include the digital infrastructure and integrated systems as well as physical infrastructures.
- **Passenger safety and security** focuses on ensuring the effective cyber/physical security and safety of passengers using urban public transport networks. Achieving acceptable levels of safety and security are fundamental prerequisites for passengers to trust and willingly choose to use such networks. Providing the safety and (cyber) security of passengers on IPT networks requires a range of assets, from technological safety systems and surveillance (CCTV) capabilities, through to trained staff and the real-time ability to communicate with passengers.
- **Data protection and privacy** are digital rights valued by societies, as well as representing EU legal requirements which apply to the operation of IPT networks (see Section 2.2). Mature IPT operators recognise that the *data/information* they hold constitutes one of their most valuable assets.
- **Sustainable environment** recognises the impact of traffic networks on the wider city environment through vectors including; air quality, noise pollutions, traffic flow, user safety, sustainable energy grids, and the economic impact for both end-users and local businesses.[30]

Because of the different nature and focus of these two viewpoints (*i.e.* business and societal), business assets tend to focus more on individual components of IPT, while societal assets tend to be concerned more with integrated and broader elements of IPT systems cutting across several operators.

2.3.2 Main critical assets for intelligent public transport

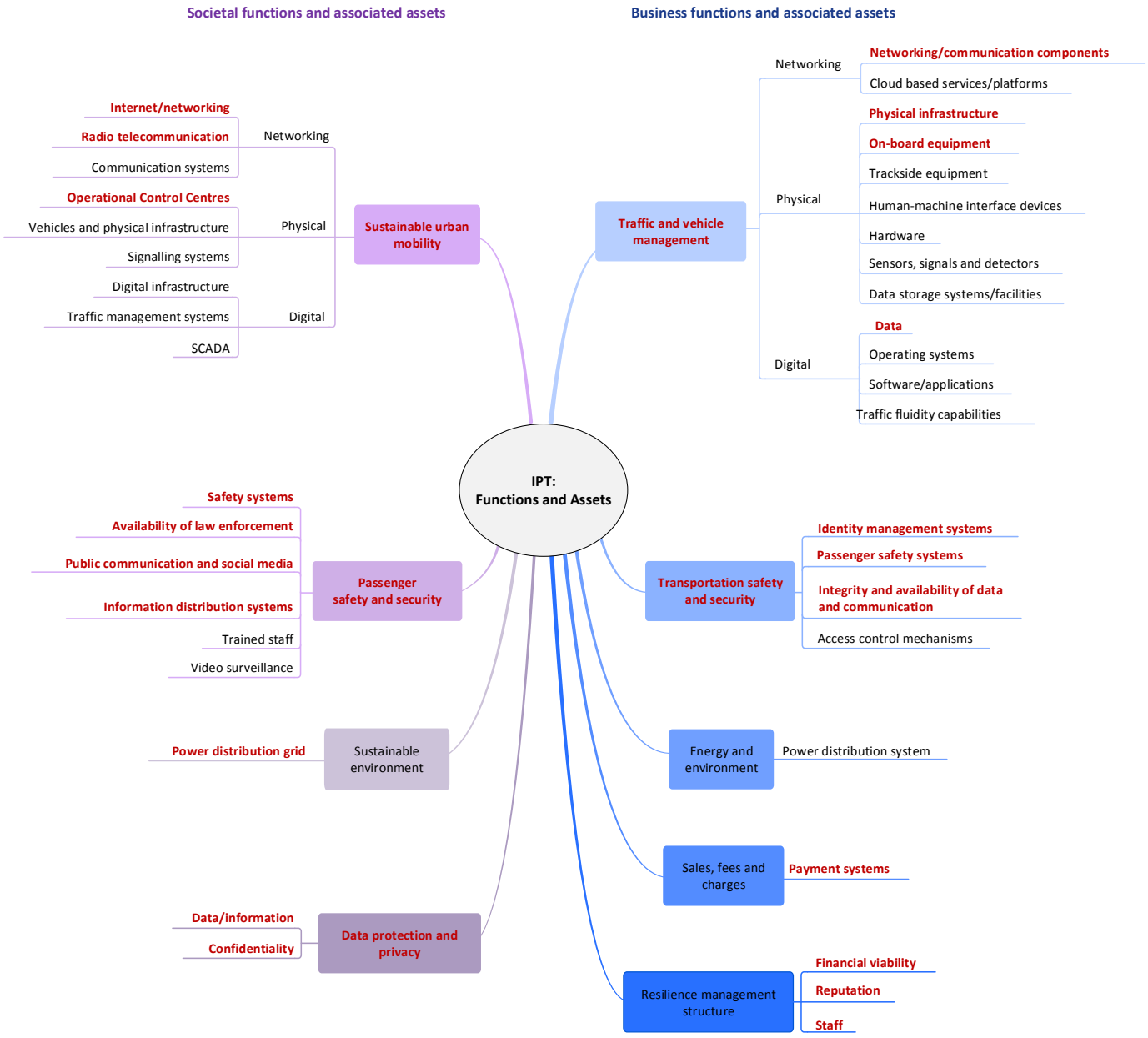
Figure 3 below set out the business and societal functions grouped together with associated assets as identified through the survey, interviews and desktop research of related documents.[31] These were also evaluated to identify those that are *critical*. The resulting five critical functions and 21 critical assets are

[30] Scottish Government, "Smart Cities Maturity Model and Self-Assessment Tool", January 2015

[31] Key documents here included: EC, COM(2011)144 final, "Roadmap to a Single European Transport Area", March 2011. EC, COM(2012) 4701 final, "Smart Cities and Communities. European Innovation Partnership", July 2012. European Innovation Partnership on Smart Cities and Communities, Strategic Implementation, October 2013. EC, COM(2009) 278 final, "Internet of Things. An Action Plan for Europe", June 2009. EC, COM(2010) 245 final, "A Digital Agenda for Europe", May 2010. Ericsson, "Smart communication + Accurate information = Intelligent Transport users", 2014.

presented in bold and highlighted red in Figure 3. In addition, Annex 2 provides an easily referable table listing those functions, assets and threats identified as critical.

Figure 3: Critical functions and assets for IPT



Assessing the nature and distribution of those assets prioritised within IPT, which act to connect IPT to the wider Smart City networks, produces key insights into both the "physical-digital" nature of those assets distributed throughout an IPT network, as well as their security requirements. Three key insights on the nature of IPT assets and security requirements are set out below.

2.3.3 Three key insights on the *nature of* intelligent public transport assets

- **Individual IPT assets combine multiple components**: IPT assets are more complex than similar assets in traditional silo-based transport systems, as they combine multiple assets into one. For example, a bus is no longer just a public transport vehicle – it is also a data collection and recording system, an information dissemination asset, mobile Wi-Fi hub, and a source of real-time intelligence for optimising the transport network. This is especially true for those assets linked to societal functions.
- **The cyber/physical divide disappears within IPT assets:** IPT assets fuse together both physical and digital components. The resulting assets are now cyber-physical hybrids.
- **IPT assets are linked together to form individual systems and systems-of-systems shared amongst multiple stakeholders:** Through the use of ICT, the individual assets of a traditional silo-based transport network are linked together to form a transport operators IPT system. A Smart City links these assets further by integrating the systems of multiple operators and/or other stakeholders and providers, forming a system-of-systems.

2.3.4 Three key insights on *security for* intelligent public transport assets

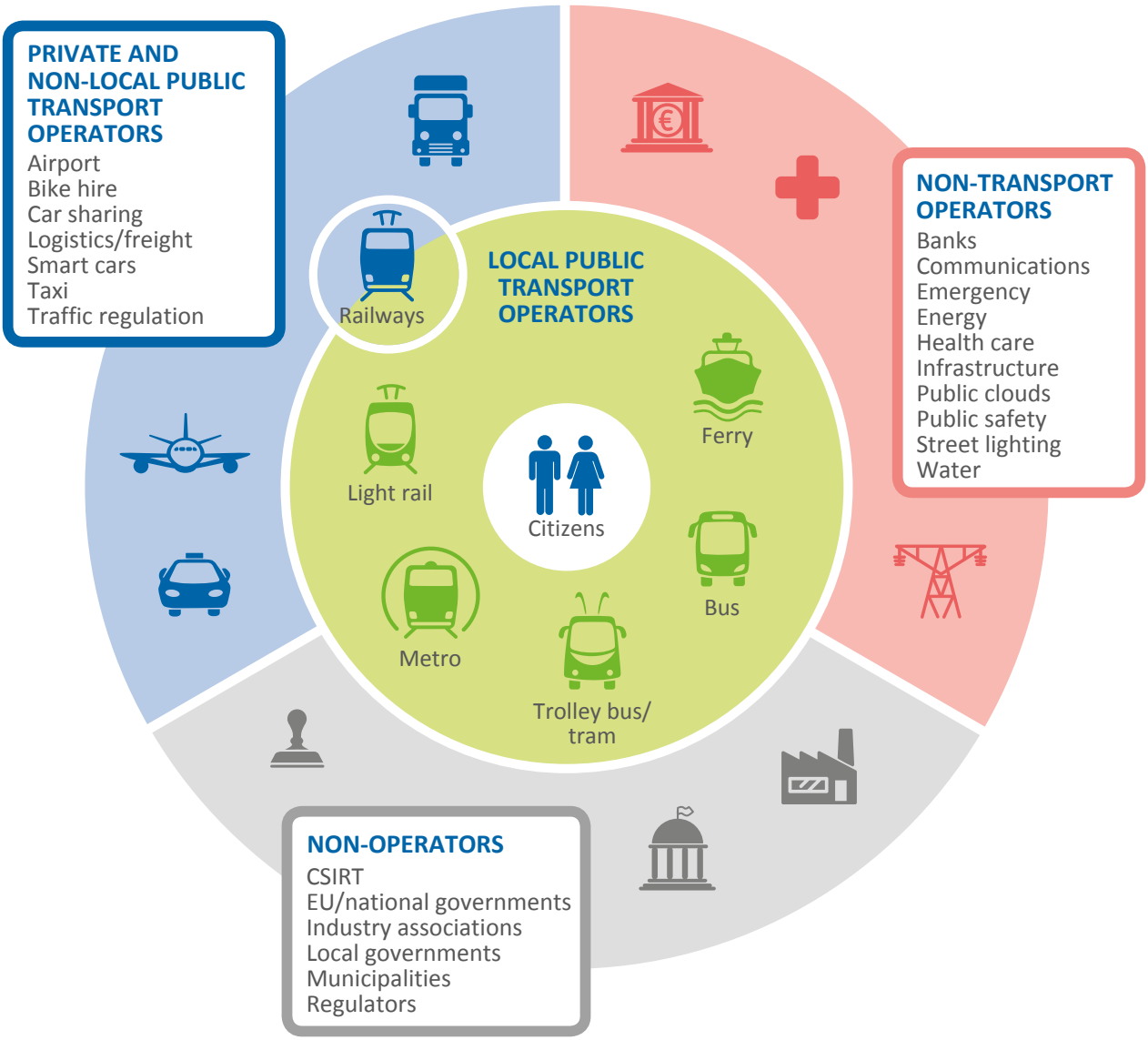
- **IPT assets are subject to a greater range of security threats:** When assets become cyber-physical hybrids, they become susceptible to both physical attacks *and* cyberattacks.
- **Cyber security and physical safety can no longer be treated as separate concerns:** When attackers can affect the physical operation of ICT-enabled vehicles or other physical assets,[32] network cyber security and physical safety become interdependent.
- **Determining where an IPT operator's (security) responsibilities end is no longer clear:** By integrating IPT into the wider Smart City through the sharing of assets, data and ICT networks with 3rd parties, the boundary of the transport operator's network is no longer clear. If an organisation cannot accurately map the network they control, this has important implications for how they conduct their network risk assessments.

[32] Chris Valasek and Charle Miller, *Adventures in Automotive Networks and Control Units*, 2014. http://www.ioactive.com/pdfs/IOActive_Adventures_in_Automotive_Networks_and_Control_Units.pdf

2.4 Intelligent public transport environment and elements

In order to discuss IPT it makes sense to place it in the urban context that both justifies the need for developing IPT systems, as well as provides the necessary cyber-physical infrastructure that enables public transport to become *intelligent*. This environment is the *Smart City*. Producing IPT systems (as opposed to *traditional* public transport systems) within this Smart City environment requires the successful integration of cyber-physical technologies and urban infrastructure. This entails the linking and integration of (physical) infrastructures and (digital) processes which are not always well connected.[27, 33] Figure 4 depicts the different stakeholders operating within Smart Cities[34] that can be integrated into the networks and cyber-physical architecture of IPT operators.

Figure 4: IPT within the Smart City content



[33] US Dept. of Homeland Security, "The Future of Smart Cities: Cyber-Physical Infrastructure Risk", August 2015.
[34] See ENISA, "Cyber Security for Smart Cities - an architecture model for public transport", December 2015.

3. A need to secure intelligent public transport

This section focuses on the *threats*, *vulnerabilities* and *risks* that are faced by IPT networks and operators and their impact on both businesses and society. To this end we employ the following definitions[35] when discussing these terms.

- **Threat:** is the potential cause of an incident that may result in harm to an IPT system or IPT organisation.
- **Vulnerability:** is a weakness within an IPT asset that can be exploited by the threats.
- **Risk:** is the potential that a given threat will successfully exploit vulnerabilities within an IPT asset and thereby result in harm to the businesses and/or society as a whole.
- **Challenges:** are current limitations faced by stakeholders on the security status of IPT (as expressed during the survey and the interviews).

3.1 Threats

3.1.1 Threat model

For the purpose of this study, a practical IPT based threat-taxonomy has been developed. The threats included in the suggested threat model are all applicable to the IPT assets presented in the previous section. The presented threat taxonomy covers mainly cyber-security threats; that is, threats applying to information and communication technology assets. Additional non-IT threats have also been included in order to cover threats to physical assets that are necessary for the operation of the considered ICT-assets. Threats appear to be multifaceted and can be directed against specific assets, ranging from IPT systems to data, through to broad organisational structures and entire IPT infrastructures. Furthermore, due to IPT assets blurring the lines between digital and physical layers (see Section 3.2), IPT operators lean more towards multifaceted threats affecting complex assets having both physical and digital characteristics.

This threat taxonomy draws upon the key findings from the survey, interviews and desktop research. Previous ENISA studies have also been employed as a basis for the taxonomy (*e.g.* ENISA *Threat Landscape and Good Practice Guide for Internet Infrastructure 2015,*[36] *ENISA Threat Landscape* 2013[37] and the *Smart Grid Threat Landscape and Good Practice Guide*).[38] In order to keep a practical focus we propose a threat model that regroups threats into *seven threat categories*. These groups define the origin of the threat with each category having its own implications over the security of IPT. However, it must be noted that these seven threat categories represent a generalised model. The threats each IPT operator must address will vary depending on multiple factors, including the size of the operator and the contextual nature of their

[35] These are contextually modified definitions of those from ETSI TS 102 165-1 V4.2.3 "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and preforms for Threat, Risk, Vulnerability Analysis", March 2011. http://www.etsi.org/deliver/etsi_ts/102100_102199/10216501/04.02.03_60/ts_10216501v040203p.pdf

[36] ENISA, "Threat Landscape and Good Practice Guide for Internet Infrastructure". https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-thematic-landscapes/threat-landscape-of-the-internet-infrastructure

[37] ENISA, "ENISA Threat Landscape 2013: Overview of current and emerging cyber threats". http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats

[38] ENISA, "Smart Grid Threat Landscape and Good Practice Guide". http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/sgtl/smart-grid-threat-landscape-and-good-practice-guide

operating environment. As such it is essential IPT operators conduct individualised risk assessments to identify the specific threats that they need to address.

The identified seven threat categories are as follows:

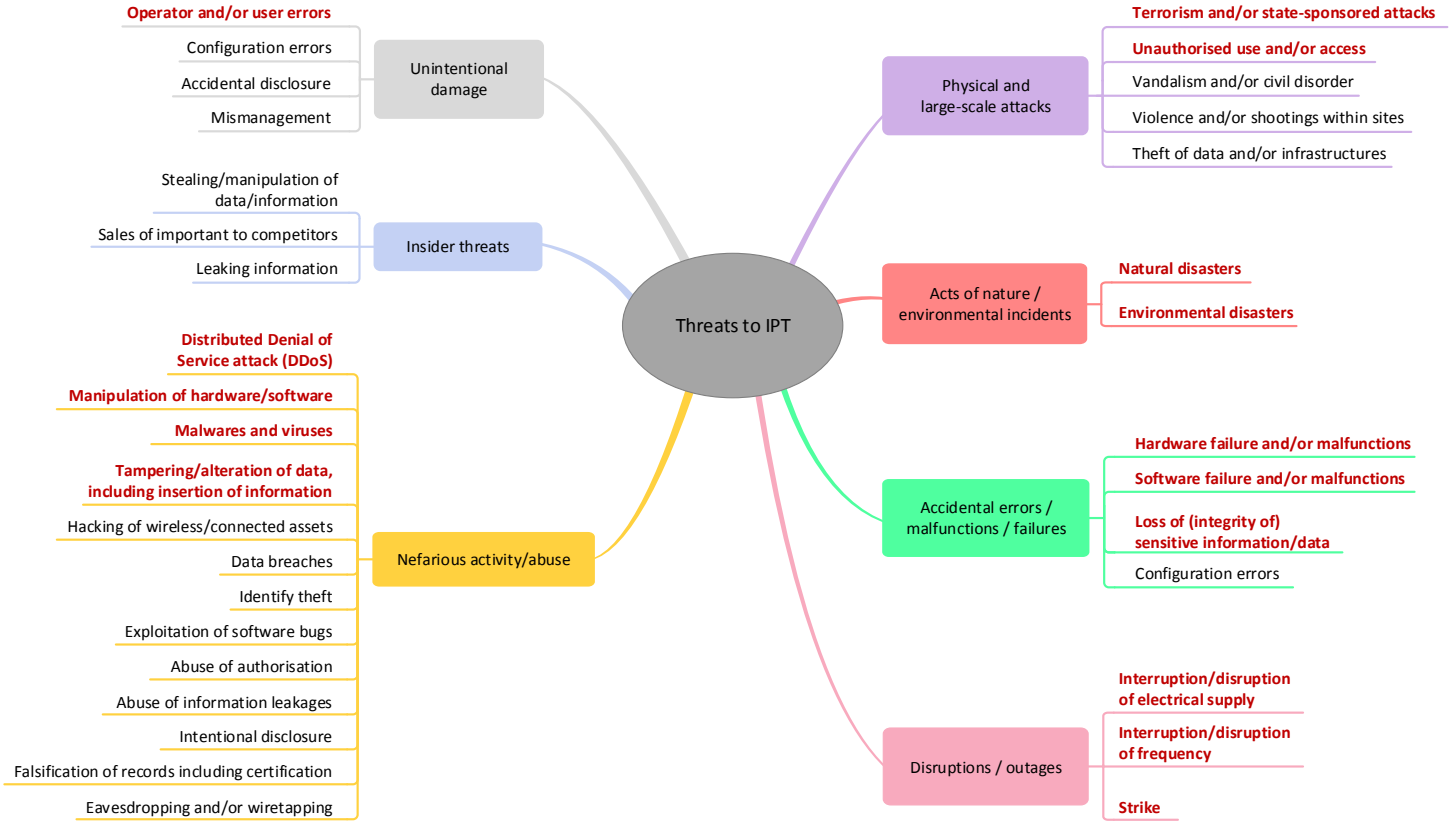
- **Physical and large scale attacks** are intentional offensive actions, which aim to achieve maximum distraction, disruption, destruction, exposure, alteration, theft or unauthorised accessing of assets such as infrastructure, hardware, or ICT connections. This threat group has general application, thus covers the entire spectrum of cyber-physical infrastructure.
- **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. These threats apply to assets in general, hence also to IPT infrastructures. Typical threats include: earthquakes, floods, wildfires, pollution, dust and corrosion.
- **Accidental errors/malfunctions/failures** are related to the condition of not functioning and/or insufficient functioning of any IT infrastructure assets. Examples include; failures or disruptions of network devices or systems, software bugs, and configuration errors.
- **Disruption and/or outages** are unexpected disruptions of services or significant decreases in expected quality, and can affect all kind of IPT assets. Disruption and outages may be triggered by a range of different reasons.
- **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. This group contains those common threats generally referred to as cyber attacks, but also related actions that do not have a digital asset as a direct target.
- **Unintentional damage** refers to the destruction, harm, or injury of property or people by accident. Damage includes both physical and non-physical damage.
- **Insider threats** are similar to nefarious activities, but originate from within the organisation being attacked or targeted. The perpetrator is often an employee or officer of an organisation or enterprise. An insider threat does not have to be a present employee or stakeholder, but can also be a former employee, board member, or anyone who at one time had access to proprietary or confidential information from within the organisation.

3.1.2 List of threats to public transport

This section presents the most relevant threats to IPT structures based on the desktop research, survey and interviews, and arranges them according to the categories described in Section 3.1.1. Respondents to the survey and interviews further evaluated these threats to identify those they consider to be *critical*. The top 15 they identified are highlighted red and presented in bold in Figure 5.[39]

[39] On the importance of operators and user errors see: Michael G. Dinning, "Introduction to Cyber Security Issues for Transportation", T3 Webinar, December 7, 2011. On the importance of terrorism/state sponsored attacks see: Gendron Angela and Martin Rudner, "Assessing cyber Threats to Canadian Infrastructures", CSIS publication, March 2012. On the importance of manipulation of hardware/software, tempering, unauthorised use and access and malware and viruses see: ETSI, "Intelligent Transport Systems (ITS)"; Edward Fok, "An Introduction to Cybersecurity issues in Modern Transportation Systems", *ITE Journal*, July 2013. On the importance of DDoS see: ETSI, "Intelligent Transport Systems (ITS)". On the importance of hardware failure, software failure and loss of integrity of sensitive information see: Trond Foss, "Safe and secure Intelligent Transport Systems (ITS)", Transport Research Arena, Paris, 2014; US Department of Transportation, "Intelligent Transportation Systems (ITS)". On the importance of natural and

Figure 5: Key threats to IPT identified by respondents



3.1.3 IPT assets exposure to cyber threats

In this section, first ideas on the threat exposure of IPT assets are presented. The list of threats is non-exhaustive and could be complemented at a later date by a more in-depth study. The association between the threats (both threat groups and individual threats) from Figure 5 and the top asset types from Figure 3 is established through Table 2 below (see Annex 3 for a more detailed table showing all the asset types). As such, Table 2 shows the relationship between the identified critical threats and the asset types/functions to which these threats apply.

This information is important for identifying countermeasures that will reduce the exposure surface of assets. This threat-to-assets association is made on the basis of the field work and initial assessment done within the project. Since IPT assets tend to blur the lines between digital and physical layers, the same threat can affect multiple assets. The association performed in this study is non-exhaustive and subject to refinements, according to particular transport and threat environments.

environmental disasters see: US Department of Transportation, "Intelligent Transportation Systems (ITS)". On the importance of interruption/disruption of electrical supply and frequency see : CRO Forum, "Power Blackout Risks. Risk Management Options. Emerging Risk Initiative", *Position Paper*, November 2011; US Department of Transportation, "Intelligent Transportation Systems (ITS)". On the importance of strike see: US Department of Transportation, "Intelligent Transportation Systems (ITS)".

Table 2: Association between IPT threats and assets

THREAT TYPES	BUSINESS ASSET TYPES/FUNCTIONS	SOCIETAL ASSET TYPES/FUNCTIONS
Physical and large scale attacks		
Terrorism and/ or state sponsored attacks	All	All
Unauthorised use and/or access	Traffic and vehicle management, Transportation safety and security	Sustainable urban mobility, Passenger safety and security, Data protection and privacy
Vandalism and/or civil disorder	Traffic and vehicle management, Transportation safety and security	Sustainable urban mobility, Passenger safety and security
Violence and/or shooting within sites	Traffic and vehicle management	Passenger safety and security
Theft of data and/or infrastructures	Traffic and vehicle management, Transportation safety and security	Sustainable urban mobility, Passenger safety and security, Data protection and privacy
Acts of nature / environmental incidents		
Natural disasters	All	All
Environmental disasters	All	All
Accidental errors/malfunctions/failures		
Hardware failure and /or malfunctions	Traffic and vehicle management, Transportation safety and security	Sustainable urban mobility, Passenger safety and security
Software failure and/or malfunctions	Traffic and vehicle management, Transportation safety and security	Sustainable urban mobility, Passenger safety and security
Loss of (integrity of) sensitive information/data	Traffic and vehicle management, Transportation safety and security	Data protection and privacy, Sustainable urban mobility
Configuration errors	Traffic and vehicle management, Transportation safety and security	Sustainable urban mobility, Passenger safety and security
Disruption and/or outages		
Interruption and/or disruption of electrical supply	All assets (excepting people/living things and exclusively physical infrastructures)	All assets (excepting people/living things and exclusively physical infrastructures)
Interruption and/or disruption of frequency	All assets (excepting people/living things and exclusively physical infrastructures)	All assets (excepting people/living things and exclusively physical infrastructures)
Strike	N/A to the top 15 assets	Sustainable urban mobility

THREAT TYPES	BUSINESS ASSET TYPES/FUNCTIONS	SOCIETAL ASSET TYPES/FUNCTIONS
Nefarious activity /abuse		
Distributed Denial of Service attacks (DDoS)	Traffic and vehicle management, Transportation safety and security	Sustainable urban mobility, Passenger safety and security
Manipulation of hardware and/or software	All assets (excepting people/living things and data)	All assets (excepting people/living things and data)
Malware and viruses	Traffic and vehicle management, Transportation safety and security	Sustainable urban mobility, Passenger safety and security
Tempering and/or alteration of data including insertion of information	Traffic and vehicle management, Transportation safety and security	Data Protection and privacy
Hacking of wireless , connected assets	Traffic and vehicle management, Transportation safety and security	Sustainable urban mobility, Passenger safety and security
Data breaches	Traffic and vehicle management, Transportation safety and security	Data Protection and privacy, Integrated infrastructure and processes
Identity theft	Traffic and vehicle management	Sustainable urban mobility, Data Protection and privacy
Exploitation of software bugs	Traffic and vehicle management, Transportation safety and security	Sustainable urban mobility, Passenger safety and security
Abuse of authorisation	Traffic and vehicle management, Transportation safety and security	Sustainable urban mobility, Passenger safety and security
Abuse of information leakages	Traffic and vehicle management, Transportation safety and security	Data Protection and privacy
Intentional disclosure	Traffic and vehicle management	Data Protection and privacy
Falsification of records including certification	All assets (excepting people/living things)	All assets (excepting people/living things)
Eavesdropping and/or wiretapping	Traffic and vehicle management, Transportation safety and security	Sustainable urban mobility, Data protection and privacy
Insider threats		
Stealing information or manipulation of data	Traffic and vehicle management, Transportation safety and security	Sustainable urban mobility, Data Protection and privacy
Sales of important data to competitors	Traffic and vehicle management, Transportation safety and security	Data protection and privacy
Leaking information	Traffic and vehicle management, Transportation safety and security	Data protection and privacy

THREAT TYPES	BUSINESS ASSET TYPES/FUNCTIONS	SOCIETAL ASSET TYPES/FUNCTIONS
Unintentional damage		
Operator and/or user errors	All assets (excepting people/living things)	All assets (excepting people/living things)
Configuration errors	See configuration errors above	See configuration errors above
Accidental disclosure	Traffic and vehicle management, Transportation safety and security	Data protection and privacy
Mismanagement	All	All

3.2 Vulnerabilities

In this section, initial reflections are provided on IPT 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.[40] Historically, cyber and physical systems have operated fairly independently of one another[41], 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.[42]

3.2.1 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).[43] This also includes vulnerabilities in commercially available mainstream IT products and systems.
- **Wireless and cellular communication:** Wireless communication[44] and cellular services introduce all the typical vulnerabilities in the area of communication conducted between points not connected by an

[40] US Department of Homeland Security, "The Future of Smart Cities: Cyber-Physical Infrastructure Risk", August 2015.
[41] This meant that the impact of a cyber-system disruption was contained within the cyber domain, while physical disruption was contained in the physical domain.
[42] This is mainly because there are not very many such infrastructures that have been operational for a sufficient period such that experiences have been gained, analysed and shared
[43] See: Gideon Mbiydzenyuy, Jan A Persson and Paul Davidsson, "Threat, Vulnerability, and Risk Analysis for Intelligent Truck Parking, a Pre-study", *ETAP III Project Report,* https://www.bth.se/com/intelligent_truck_parking.nsf/attachments/Del_6_Security_pdf/$file/Del_6_Security.pdf ETSI, "Intelligent Transport Systems"*;* and Edward Fox," An Introduction to Cybersecurity Issues in Modern Transportation Systems", *ITE Journal*, July 2013. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.377.199&rep=rep1&type=pdf
[44] It was noted by operators that the threat "Interruption and/or disruption of frequency" identified above is considered as a major risk for transport operators as most of their moving assets are linked to their central equipment via wireless connections. Such connections could be significantly disturbed with few resources (*e.g.* it is quite simple to develop a frequency jammer that could block a major station).

electrical conductor. For example, inadequate security protocols, inadequate authentication mechanisms, energy constrain, poor security and unreliable communication.[45]

- **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. "Increased connectivity, faster speeds, and multi-directional data flows diversify access points into critical infrastructure, changing and stretching the borders that must be secured."[46]
- **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.[46]
- **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. [46]

3.2.2 Specific vulnerabilities

- **Scale and complexity of transportation networks:** This refers to the difficulty of mapping the entire IPT system (*i.e.* due to the loss of visibility for all parts of a 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.[47]
- **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.[48]
- **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. [46]
- **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. [46]
- **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. [46]

---

[45] C.K. Marigowda and Manjunath Shingadi, "Security Vulnerability issues in Wireless Sensor Network: A short Survey", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 7, July 2013

[46] US Department of Homeland Security, "The Future of Smart Cities".

[47] Bertrand Berche, Christian von Ferber, Taras Holovatch and Yurij Holovatch, "Public Transport Networks under Random Failure and Directed Attack", *Workshop NET 2009*, Rome, May 28th-30th, 2009; US Department of Homeland Security, "The Future of Smart Cities".

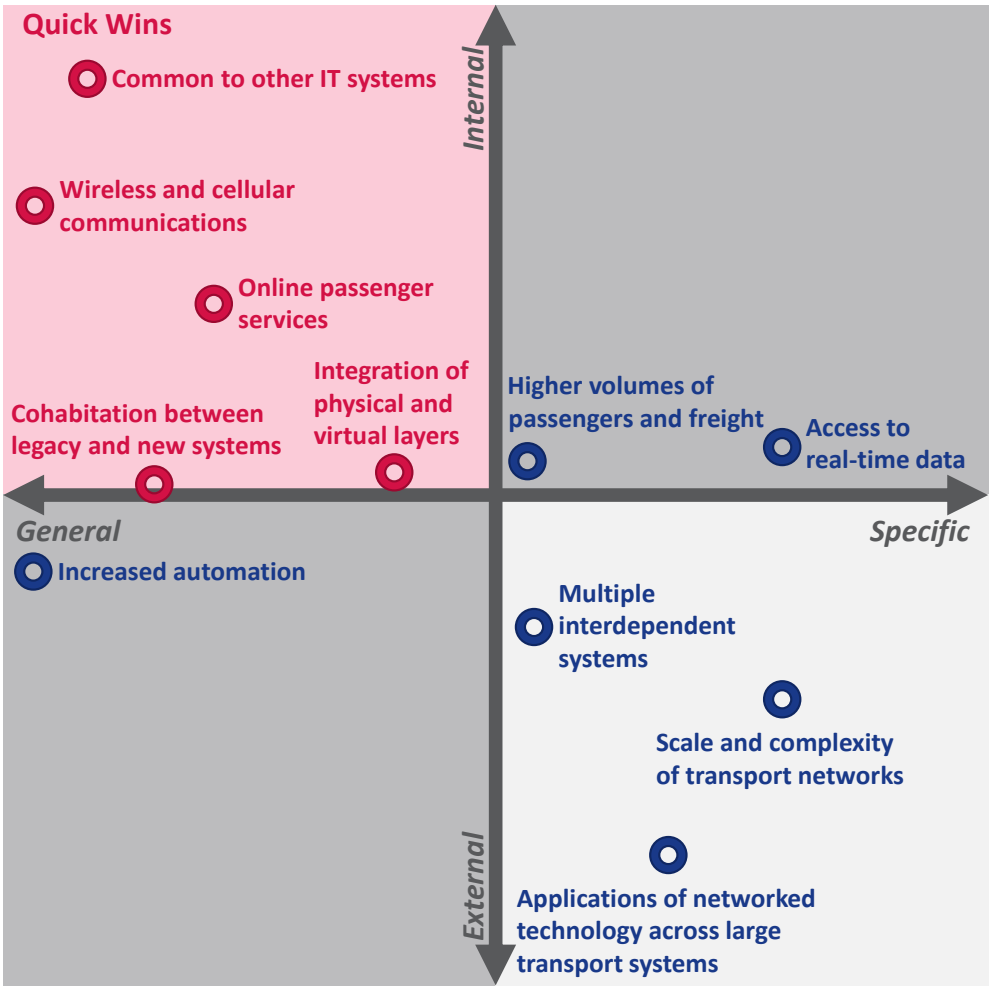
[48] Mulligan, Catherine, "ICT and the Future of Transport", Ericsson, 2014. http://www.ericsson.com/res/docs/2014/ict-and-the-future-of-transport.pdf; and US Department of Homeland Security, "The Future of Smart Cities".

- **Online passenger services:** The online provision of passenger services (such as timetabling, passenger information and ticket booking) that historically have only been available offline, means these functions and now susceptible to all the associated cyber risks.

The inferred vulnerabilities are listed below and presented in Figure 6, whereby these vulnerabilities are mapped (based on the desktop analysis) on an axis system with axes general vulnerabilities (*i.e.* applicable beyond IPT) and specific vulnerabilities (*i.e.* those specific to IPT); and internal vulnerabilities (*i.e.* originating from and controlled by a few operators) versus external vulnerabilities (*i.e.* those originating from operators' interdependence and controlled by multiple operators).

This mapping allows for the identification of "quick wins", defined as improvements that will impart significant benefits to transport operators but are relatively easy and inexpensive to implement. These are vulnerabilities that are internal and hence more likely to be under the direct control of the operator thus allowing for more impactful interventions, and those that are general which imply more affordable solutions (*i.e.* through off-the shelf products and/or greater competition between solution providers).

Figure 6: Matrix of IPT vulnerabilities



3.3 Risks

As defined earlier, risk is the potential that a given threat will successfully exploit vulnerabilities within an IPT asset and thereby produce a negative impact on businesses and/or society as a whole.[49]

Risks exploit several vulnerabilities within an IPT company, but above all those found in the area of: "wireless and cellular communication", "cohabitation between legacy and new system" and "integration of physical and virtual layer".[50]

The risks are divided in two categories:

- **Business risks**, which can be at the source of economic loss and impact normal operations;
- **Societal risks**, which may lead to safety issues and limit service unavailability.

3.3.1 Business risks

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

- **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.
- **Loss of revenue:** In the case of an incident, operations can become limited or suspended, which leads to a loss revenues. Moreover, responsibilities in case of an incident can also lead to loss of revenue (fines…).
- **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.[51]
- **Non-compliance with the regulation on data protection:** The disclosure of personal data, voluntarily or not, is covered by regulation. This risk is usually associated with loss of revenue (due to fines and mitigation action) and loss of trust (from passengers, clients and municipalities).
- **Risks on hardware and software:** Risks related to the manipulation or destruction of IPT components, hardware and software (see Section 3.1 *Threats*) impact the stability and availability of the IPT systems. This can lead to the disruption of services, inferior passenger and freight experience, loss of sensitive data and fraud.[52]
- **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. Using invalid information is a risk as it may limit the quality of the service.

[49] In risk management methodologies risk is interpreted as "the risk factor", which is calculated based upon the likelihood of a particular threat being successful and the impact that a successful threats would have on the system. In this study we do not use risk as a risk factor but instead in more general term as the negative impact produced by a successful threats.

[50] Ahmed Abdel Rahim and Ybette Ochoa "A Framework to Analyze the Survivability and Vulnerability of Intelligent Transportation System Networks", *Journal of Intelligent Transportation and Urban Planning*, Jan 2014, Vol. 2 Issue 1, pp. 22-29

[51] Transport for London , "Strategic Risk Management and Assurance Annual Report 2013/14", July 2013

[52] US Department of Homeland Security , "The Future of Smart Cities".

- **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.[53] Hence, the output of individual vulnerability and risk assessments will depend on the particular mix of components, processes and infrastructure involved in a particular scenario. For example, with the increasing proliferation of mobile devices in traffic systems *mobile security* becomes another important component of the complex traffic infrastructure.
- **Unavailability of a dependency:** The IPT service depends on several internal and external dependencies (*e.g.* power supply, mobile telecommunications…). Hence, the IPT service may suffer from the unavailability of a dependency and become unavailable.

3.3.2 Societal risks

Similarly to business risk, societal risks are mainly triggered by the manipulation and destruction of IPT components (see Section 3.1 *Threats*).[54]

Effective transportation systems are essential to European society: not only do they enable the mobility of citizens and goods, they also have significant impacts on economic growth, social development and the environment.[55] Although the expectation is that IPT will cut costs, improve environmental quality and enhance traditional safety (*i.e.* by reducing road accidents), it could also amplify old and open up new societal risks.[55]

- **Unavailability of the IPT service:** Given the nature of societal assets,[56] 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 for a single IPT operator but also to the unavailability of transport systems (*i.e.* network gridlock) with consequent secondary effects for other sectors, and increases in traffic accidents.[57]
- **Disruption to the society:** The IPT service is used by citizens to carry out their daily lives. 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.
- **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…). Furthermore, the international context has changed in recent years: the sustained threat from terrorism is real and needs to be accounted for when protecting IPT infrastructures.[58]

---

[53] Steven H. Bayless, Sean Murphy and Anthony Shaw, "Connected Vehicle Assessment. Cybersecurity and Dependable Transportation", *Connected Vehicle Technology Scan Series*, 2012-2014.
[54] US Department of Homeland Security , "The Future of Smart Cities".
[55] EC, " Information Society and Transport: Linking European Policy", *DG Information Society and Media publication*, 2006.
[56] See Section 2.3
[57] CGI, "Could Your Security Vulnerabilities Cause Network Gridlock?", *A Discussion Paper for Transportation Information Technology Leaders and Executives,* http://www.cgi.com/sites/default/files/white-papers/transportation-information-technology_security-vulnerabilities-causing-network-gridlock.pdf
[58] Transport for London , "Strategic Risk Management and Assurance Annual Report 2013/14", July 2013.

- **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. For example, vehicles may emit higher pollutants than their expected levels. [59]
- **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. [60]

3.4 Challenges

This section summarises eight identified key challenges facing cyber security within IPT. Challenges are identified based on criticisms and/or shortcomings of the existing status quo that were collected during the survey and the interviews with stakeholders.

While they are numbered 1 to 8 below, these challenges have not been ranked according to any measure of importance.

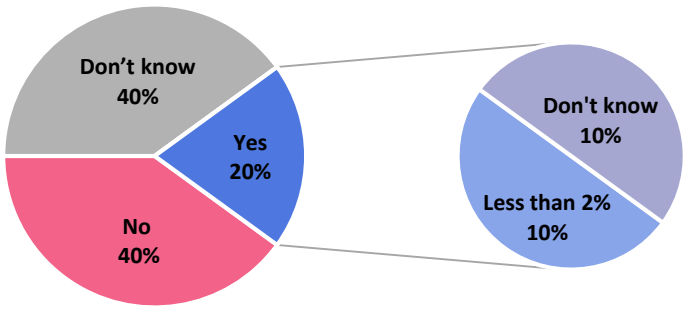
3.4.1 Challenge 1: Difficulties to integrate security for safety

While there is a tendency in other contexts to combine safety and security into a single category, within transport these two concepts are traditionally very separate. Manufacturers and IPT operators usually prioritise 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.

3.4.2 Challenge 2: Inadequate importance and spending being afforded to cyber security

A key finding from the survey and interviews (see Figure 7) indicates that transport organisations 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.

Figure 7: Cyber security spending



3.4.3 Challenge 3: Inadequate checking for countermeasures

The majority of transport organisations do not measure the effectiveness of their countermeasures (see Figure 8 below presenting findings from the survey and interviews).[61] This in turn produces a lack of

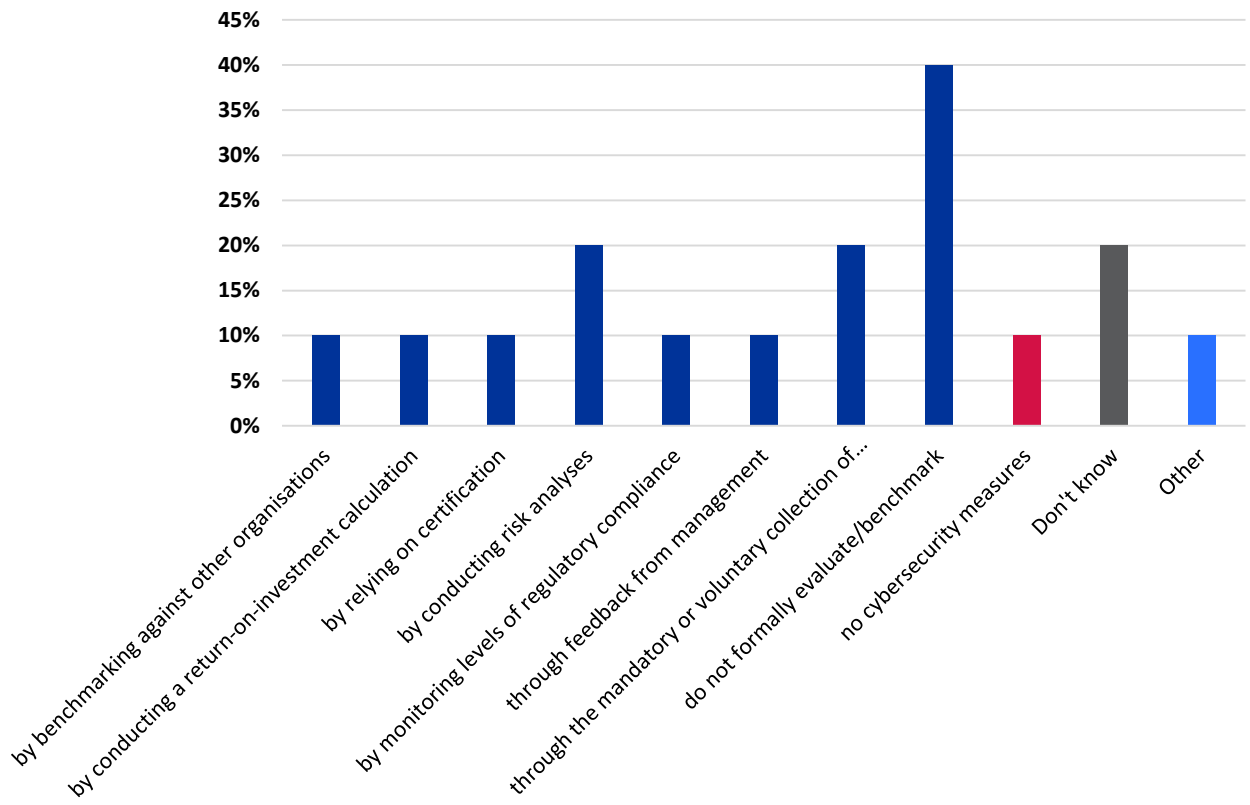
[59] Even though not directly applied to IPT, the Volkswagen emission scandal shows that emission levels of vehicles can be modified by software https://en.wikipedia.org/wiki/Volkswagen_emissions_scandal

[60] Steinfeld, Aaron, "Ethics and Policy Implications for Inclusive Intelligent Transportation Systems", *Second International Symposium on Quality of Life Technology*, 2010.

[61] Please note that the respondents could select multiple relevant answers.

awareness and knowledge in relation to what "works" and what "does not work" in cyber security for IPT. The question of measuring the value of security in a transport organisation is also important when security teams ask the business to invest in security. The inability to answer this question can often explain why the business is reluctant to invest.[62]

Figure 8: Measuring Effectiveness in Cyber security Measures

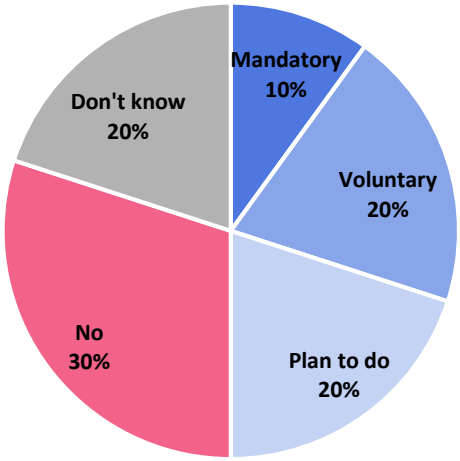


3.4.4 Challenge 4: Unwillingness to collaborate and exchange information on cyber security

Overall, transport organisations 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 and other indirect losses related to cyber crime. Additionally, they may not have implemented the necessary systems/measures to collect the necessary information to be shared (see Figure 9 below presenting finding from the survey and interviews). Furthermore, they also have low awareness of any collaboration and information-sharing activities pertaining to cyber security being carried out within the sector. However, operators are open to collaborate and exchange information with national Computer Security Incident Response Team (CSIRT) and Law Enforcement Agencies (LEA).

[62] Ashford Warwick, "How can businesses measure the effectiveness of their IT security teams to ensure they are getting value?", http://www.computerweekly.com/feature/Security-Think-Tank-How-can-businesses-measure-the-effectiveness-of-their-IT-security-teams

Figure 9: Cyber security Information Exchange



3.4.5 Challenge 5: Slow phasing out of legacy systems

The existence and use of legacy systems can weaken cyber security. Legacy systems have security controls typically focused on the simple necessity of reducing the risk of physical product tampering or theft. 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.[63]

3.4.6 Challenge 6: Inadequate data exchange between IPT and Smart Cities operators

Data exchanges between IPT and different Smart Cities operators (*i.e.* railways, LEA, local government, etc.) tend to be restricted, uncoordinated and ad-hoc. These interactions also vary depending on the context and/or business model adopted by the operators.[64] 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.

3.4.7 Challenge 7: Weak situational awareness of cyber threats

Due to the fast moving and interconnect nature of IPT, transport organisations are struggling to achieve a full awareness of the range of cyber threats and boundaries for securing the IPT landscape.[65]

3.4.8 Challenge 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 (*e.g.* privacy-by-design, building-in redundancy and shut down procedures). 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.

---

[63] Steven H. Bayless, Sean Murphy and Anthony Shaw, "Connected Vehicle Assessment. Cybersecurity and Dependable Transportation", *Connected Vehicle Technology Scan Series*, 2012-2014.

[64] For example electrified transport systems report good integration with energy suppliers. Some data exchanges are happening between infrastructure providers, law enforcement and emergency services (and to a less extent with local government, transport industry associations, *e.g.* UITP, and government/regulatory bodies) in relation to criminal incidents and emergency events yet other stakeholders/elements such as banks and social media are often not well integrated.

[65] US Department of Homeland Security, "The Future of Smart Cities".

4. Good practices for securing intelligent public transport

This section sets out existing good practices for securing IPT networks as identified through both an analysis of existing good practice documentation complemented by interviews with a range of stakeholders, including; transport operators, Smart City municipalities, risk managers and cyber security experts. By *good practices* we are referring to effective security measures that should be implemented if they address weaknesses identified during a risk assessment of your business operation. The inclusion of these good practices reflects our intention that this study should operate as a practical guide for IPT operators, one that will assist in supporting their internal processes.

One point that must be remembered when considering the good practices discussed here is that this section only deals with *existing* good practices as identified during the desktop research and the survey and interviews. *Gaps* in the current suite of existing good practices are not addressed here, but are identified and discussed in Section 5.

This section provides a brief description of each individual good practice identified to secure IPT. They are presented and arranged into three categories according to their inherent nature:

- Technical good practices;
- Policies and standards;
- Organisational, people and processes.

These good practices are effective to counter threats before, during and/or after an attack. For more information, Annex 4 details these good practices by presenting them as a checklist to assist stakeholders in their assessment and implementation.

4.1 Technical good practices

Conduct security-focused risk assessments: Each operator should conduct regular risk assessments covering physical, cyber and information security that entail mapping the scope of their business operations, identifying the critical business functions, and then identifying the assets critical to these functions. Regular risk assessments are required to identify changes in the threat landscape and thereby ensure that the correct threats to the business are identified and efficiently addressed.[66]

Employ appropriate physical security, access controls and protection measures: Physical security is required to protect both the physical and digital assets of an IPT network by preventing unauthorised physical access to sensitive locations, whether deliberate and unintentional. The nature of the physical security employed should be commensurate to the assets being protected[67] (*i.e.* from simple locks for areas designated low risk/value to layered security, such as multi-factor authentication systems potentially combined with guards/CCTV, for high risk/value areas).[68]

[66] See Cristin Goodwin and Paul Nicholas, "Developing a City Strategy for Cybersecurity: A seven-step guide for local governments", October 2014. http://download.microsoft.com/download/1/B/3/1B3C6BE3-8FA4-40BD-9BD6-640FD2F1F648/City%20Strategy%20for%20Cybersecurity.pdf

[67] A Risk Assessment will be required to differentiate between areas of high risk/value and low risk/value.

[68] Ross Anderson, "Security Engineering (2nd Edition)", 2008.

Employ secure digital access controls to networks and data: To complement physical security measures, IPT operators must ensure they employ robust digital access controls to their networks and stored data (whether in local servers or cloud-based) so as to prevent attackers accessing these via ICT due to the prevalent of these attacks on both large and small businesses.[69] [70] Common measures include: firewalls; password controls; multi-factor authentication; use of firewall based VPNs.[71] [72]

Employ alarms/surveillance for protecting physical and digital assets: Closely linked to the monitoring and recording of activity is the need to install alarms and surveillance systems across the cyber/physical network of an IPT operator to secure that network. Alarms and surveillance systems designed to focus the attention of operators on specific locales or events are necessary requirements. This is because the size and complexity of an IPT network distributed across a city demands the implementation of systems enabling a limited security team to effectively monitor the entire network.

Encryption: Operators need to ensure the confidentiality of sensitive data (*e.g.* customer/employee financial details, intellectual property, etc.) that they both hold (either internally or on external servers/clouds) and communicate across networks, due to the prevalence of cyber attacks.[68] In effect, IPT operators should work on the assumption their digital systems will be successfully accessed by attackers. To this end they should employ industry-recognised encryption standards,[73] use VPNs,[74] and if available make use of national cyber security agencies to guide on encryption methods.

Develop secure and private communication networks: Operators need to ensure the security of their communication networks and the privacy of the data traveling across these networks as they represent a target for attacker. As IPT communication networks include both physical and digital elements, a combination of protection methods are required, including; tamper-resistant devices, access controls, firewalled VPNs, encryption, message integrity provisions, network intrusion detection systems, etc.[75]

Employ intrusion detection systems (IDSs): IDSs aid in monitoring a network to inform on internal and external attacks, malicious network communications and usage of computer systems. Common methods include anomaly detection and misuse (signature) detection.[76] IDSs are needed to supplement firewalls

---

[69] HM Government, "2015 Information Security Breaches Survey", June 2015. http://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf

[70] Mariana Carroll and Paula Kotzé, "Secure Cloud Computing: Benefits, Risks and Controls", *Information Security South Africa*, 2011. http://researchspace.csir.co.za/dspace/bitstream/10204/5184/1/Kotze4_2011.pdf

[71] HM Government, "Cyber Essentials Scheme: Requirements for basic technical protection from cyber attacks", June 2014. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317481/Cyber_Essentials_Requirements.pdf

[72] Government of the HKSAR, "*VPN* Security", February 2008. http://www.infosec.gov.hk/english/technical/files/vpn.pdf

[73] See for example: ENISA, "Algorithms, key size and parameters report – 2014", November 2014; ANSSI, "Mécanismes cryptographiques, V2.03" 2014; BSI "Kryptographische Verfahren: Empfehlungen und Schlussellangen: BSI TR-02102-1", February 2015.

[74] Ye Yan, Yi Qian, Hamid Sharif and David Tipper, "A survey on Cyber Security for Smart Grid Communications", *Communication Surveys & Tutorials, IEEE*, Vol.14(4), 2012, pp.998-1010.

[75] Hung-Jen Liao, Chun-Hung Richard Lin, Ying-Chih Lin and Kuang-Yuan Tung, "Intrusion detection system: A comprehensive review", *Journal of Network and Computer Applications*, Vol.36, 2013, pp.16-24.

[76] Chih-Fong Tsai, Yu-Feng Hsu, Chia-Ying Lin, and Wei-Yang Lin, "Intrusion detection by machine learning: A review", *Expert Systems with Applications*, Vol.36, 2009, pp.11994-12000.

and virus scanners as there is no network security measure that will ensure perfect cyber security. Hence IPT operators should employ multiple protection measures through a defence-in-depth approach.

Employ identity management and authentication systems: To secure IPT requires restricting access to both physical spaces and digital networks, such that only authorised individuals can access these spaces. This requires the implementation of measures, such as multifactor (*i.e.* two and three-factor) authentication systems, for confirming that the person seeking access is who they claim to be. Additionally there is the need to link activity within a network to the identity of the actor to prevent repudiation: measures such as digital signatures, access controls, and audit trails should be employed here.[77]

Integrate shut-down procedures/remote deactivation of capabilities, for assets: Malfunctioning, compromised or stolen assets may be in geographically remote locales on a transport network. To enable prompt reactions by IPT operators, the ability to either remotely shut-down or deactivate certain capabilities/functionalities of these assets can minimise damage/loss. Operators can use SCADA systems to issue such supervisory commands to field devices/assets.[78]

Operate in degraded mode of operation: In case of a failure, the system might still operate at with a reduced level of service. In these conditions, the IPT system manages to ensure certain critical functions at a minimum level. For that purpose, IPT operators have to determine which key performance indicators can be relaxed until the normal service is recovered.

4.2 Policies and standards

Employ security by design: Physical/cyber infrastructure should incorporate security requirements upstream during the engineering process to minimise the potential and impact of breaches. As per these requirement, employing security by design improves the security capabilities of products and helps mitigate the likelihood of the costly retrofitting of security protections.[79]

Establish disaster recovery processes and maintain back-ups: It is imperative to develop and establish a disaster recovery processes, and to maintain back-ups of business data preferably in a remote secure location to minimising the likelihood of collateral damage. These actions acknowledge the reality that despite an operator's best security efforts, it is inevitable that incidents will occur,[80] whether through deliberate attacks, user errors, accidents and/or environmental incidents.

Define degraded modes of operation: The definition of degraded modes of operation contributes to enhancing the resilience of the IPT system by ensuring a minimum level of service. One of several degraded modes can be defined in function of the systems impacted and the dependencies identified. For example, degraded modes of operation are applied in air traffic management in order to ensure safety.[81]

---

[77] Thomas Calabrese, "Information Security Intelligence: Cryptographic Principles and Applications", 2004.
[78] Bonnie Zhu, Anthony Joseph and Shankar Sastry, "A Taxonomy of Cyber Attacks on SCADA Systems", Internet of Things (iThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing, pp.380-388, October 2011.
[79] Ann Cavoukian and Marc Chanliau, "Privacy and Security by Design: A Convergence of Paradigms", January 2013. https://www.ipc.on.ca/images/resources/pbd-convergenceofparadigms.pdf
[80] A. Bartoli et al., "Security and Privacy in your Smart City", EU project ICT-258512 EXALTED, December 2011.
[81] Chris Johnsona, Barry Kirwanb and Tony Licuc , "The interaction between safety culture and degraded modes: A survey of national infrastructures for air traffic management", October 2009. http://www.palgrave-journals.com/rm/journal/v11/n3/pdf/rm200910a.pdf

Implement an information security policy: An organisation's information security policy sets their course for information security. It emphasises the need for information security to all staff members, and reflects the commitment of the organisation to operate in a controlled, secure manner and achieve information security.[82] Failure to develop and implement an information security policy undermines the operator's ability to focus their information security activities consistently across their organisation.

Forecasting, early warning systems and risk analysis: IPT operators possess finite security resources, hence it is essential they can direct these resources appropriately so as to maximise their impact. Knowing of, or predicting the risk of, threats in advance of their emergence enables the stakeholder to efficiently allocate their resources and to take pre-emptive steps to mitigate damages.

Separate critical systems from non-critical systems: Critical systems (*i.e.* those controlling steering, braking, etc.) should not be accessible though other non-critical systems installed within the same vehicle (*e.g.* information displays, entertainment systems, etc.). Successful attacks on critical systems in smart vehicles where access was gained through non-critical systems demonstrates the safety and security imperatives of keeping these systems separate.[83] [84] Similarly, networks linking critical systems and/or those essential to the provision of critical services should be separated (either physically or virtually) from networks linking non-critical systems/services.[85]

Enhance physical security protecting critical physical infrastructure: Risk assessments should be used to identify which infrastructure is *critical* to the IPT operator and, enhanced physical protection measures should be implemented as a result.[86] Each operator will have their own unique assets requiring protection, and this two-step process ensures resources are allocated on an evidence basis.

Implement a security control centre with real-time monitoring: A centralised control centre for directing and coordinating security resources to respond to threats as they are identified enables the efficient allocation of resources, and provides a recognisable point of contact for liaising with LEA, CSIRTs and other Smart City stakeholders.

Ensure redundancy for critical systems: Building redundancy into critical systems reduces the likelihood that the failure of a single or small number of components, or an isolated incident within the network, will result in the failure of the entire network. While this good practice is applicable to all critical systems, two specific instances were highlighted by respondents as being particularly critical for IPT, these being; communication systems and power systems.

Create resilient communication systems: Communication systems are essential components of IPT systems with the integration of ICT into public transport defining IPT. At its extreme, the failure of the communication system will halt an IPT network, and these communication systems are susceptible to a multitude of physical and cyber attacks, acts of nature and environmental incidents. Hence it is essential to

---

[82] Karin Hone and J.H.P Eloff, "What Makes an Effective Information Security Policy?", *Network Security*, Vol.6(1), 2002, pp.14-16.
[83] BBC News, "Fiat Chrysler recalls 1.4 million cars after Jeep hack", 24 July 2015. http://www.bbc.co.uk/news/technology-33650491
[84] BBC News, "Car hack uses digital-radio broadcasts to seize control", 22 July 2015. http://www.bbc.co.uk/news/technology-33622298
[85] See Eric D. Knapp and Joel Langill, "Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems (2nd edition)", 2015.
[86] This is not to say that non-critical infrastructure should be unprotected; merely that critical infrastructure should be assessed for additional protections.

build redundancy into IPT communication systems so no single failure will break the network. When public telecommunication networks are used, this resilience can be contractual if specified in the Service Level Agreement established with communication providers.

Create resilient power systems: IPT infrastructure (including some vehicles) require electricity to operate. Nevertheless, these power systems are susceptible to a multitude of physical and cyber attacks, strikes, acts of nature and environmental incidents which can lead to disruptions and outages. Hence it is essential to build redundancy into IPT power networks so that no single point of failure exists. This resilience can be contractual if specified in the Service Level Agreement established with power suppliers.

4.3 Organisational, people and processes

Monitor and record activity: Operators need to implement technologies to monitor and record both physical activity at high value locations (*e.g.* CCTV, authentication logging, etc.) and digital activity (*e.g.* activity logs) on their networks as part of a cohesive Security Management System.[87] These measures are required for multiple purposes including: ensuring safety, providing security, the gathering of forensic evidence, system recovery processes, training purposes, identifying insider threats, data for risk analyses, maintaining system stability, etc.[88]

Define security requirements during procurement processes: During the procurement process "security" needs to be afforded the same importance as "functionality". This enhancing of the status of security at this early stage is to decrease business risks posed by cyber and physical threats, and acts to mitigate the likelihood of the costly retrofitting of security protections.[89]

Coordinate with LEAs and CSIRTs: IPT operators should coordinate with LEAs/CSIRTS. The level of coordination can include sharing threat/good practice information, developing and running online training programmes, and conducting live drills.[90] This level of coordination is necessary as LEA/CSIRTs occupy privileged positions to see emerging and/or applicable threats from other stakeholders outside of IPT.

Raise awareness on cyber threats to all levels of staff including management: Cyber threats keep evolving at fast pace. It is important to raise awareness among staff by informing them periodically about current and top threats targeting IT systems and assets of the organisation. Highlighting security good practices to protect against these threats is also important. In order to improve the awareness level efficiently, all staff including non-technical staff and in particular management shall be informed. In particular, informing management on existing governance models is likely to help integrating cyber security in the organisation.

Engage in staff training: IPT staff are valuable assets for protecting the network against both physical and digital threats. They are also a potential source of threats to the network through accidently introducing viruses and malware, as spearfishing victims, etc. To maximise benefits and minimise risks, pre-emptive training programmes complemented by post-event training (to incorporate "lessons learnt") are essential.

---

[87] Giovanni Bocchetti, Francesco Flammini, Concetta Pragliola and Alfio Pappalardo, "Dependable integrated surveillance systems for the physical security of metro railways", *Third ACM/IEEE International Conference on Distributed Smart Cameras*, 2009.

[88] Preeti Tuli and Priyanka Sahu, "System Monitoring and Security Using Keylogger", *International Journal of Computer Science and Mobile Computing*, Vol.2 (3), March 2013, pp.106-111.

[89] Robert Newby, "Security Think Tank: Procurement and security are uneasy bedfellows", *ComputerWeekly.com*, November 2013.

[90] See Cristin Goodwin and Paul Nicholas, "Developing a City Strategy for Cybersecurity: A seven-step guide for local governments", October 2014.

Develop organisational and operational procedures and guidelines: The development and implementation of operational guidelines and procedures should be integrated into the culture of an IPT via staff training. Without this process, good practices, lessons learnt from prior incidents and corporate knowledge cannot be retained and applied throughout an organisation in a systematic fashion.

5. Gap analysis

This section provides an analysis of the main gaps in relation to cyber security in IPT as identified during the field work. Gaps were elicited from the comparison between the identified threats, vulnerabilities and risk, and good practices.

Gaps to be addressed are widespread and focused not just on technology but also on other areas, such as: organisational gaps, policy and standardisation issues, and the need to develop more comprehensive and integrated tools. This section summaries eight identified key cyber security gaps in IPT. While they are numbered 1 to 8 below, these gaps have not been ranked according to any measure of importance.

5.1 Gap 1: Lack of a common EU approach to Intelligent Public Transport Security

There is currently no common EU approach specific to either intelligent or standard public transport, or related framework that specifically address IPT cyber security needs (see Section 2.2 for an analysis on EU legislation).[91] Potentially the proposed NIS Directive might have an impact on addressing elements of this gap, above all in relation to cyber threat reporting, but may need to be expanded to encompass requirements for IPT cyber security within both urban transport networks and national/international rail networks.

5.2 Gap 2: No integration of security in current EU guidelines for IPT

Although there are EU guidelines on cyber security, very little is specifically designed for intelligent transport.[92] A gap here exists for EU common guidelines that deal more closely with intelligent transport above all in relation to enhancing the cyber security of IPT systems and the implementation of appropriate processes with a suitable cyber security focus.[93] Furthermore, although some initial developments in relation to an EU-wide strategy for intelligent transport have been put in place in recent years, via the action plan for the Deployment of Intelligent Transport Systems in Europe[94] and the Directive 2010/40/EU[95] requiring MS to develop their own strategy for implementing transport, these attempts do not focus on cyber security.[96] Therefore there is still a gap in relation to comprehensive and integrated guidelines or strategies tailored to secure IPT from cyber threats. Such guidelines could define the action of different stakeholders involved on IPT cyber security (*e.g.* coordination, responsibilities…).

5.3 Gap 3: Lack of common definitions and formalised cyber security policies

The field work indicates that definitions for IPT are not widely used or adopted (see Figure 10) within transport organisations. Furthermore, the majority of transport organisations do not have a formalised

[91] While Directive 2008/57/EC is a partial exception here covering the interoperability of EU railways, this Directive also has nothing to say on cyber security needs.
[92] See: ENISA, "Good Practice Guide for Incident Management", 2010; and ENISA, "Technical Guidelines on Security Measures", October 2014.
[93] More mature IPT implies the coordination and cooperation among different operators and users in different countries , hence the EU focus is a paramount.
[94] EC, "Action Plan for the Deployment of Intelligent Transport Systems in Europe - COM(2008) 886 final/2 – CORRIGENDUM", 2008.
[95] EC, "Directive 2010/40/EU on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport", 2010.
[96] In addition they only address road vehicles, therefore other major modes of transportation of IPT are not covered.

cyber security policy in place and/or list of critical assets that need to be protected by cyber threats (see Figure 11). There is need for common definitions and the adoption of more formalised security strategies.[97] This will lead to greater security and collaboration within and among transport organisations.

Figure 10: Use of definition of Intelligent Transport

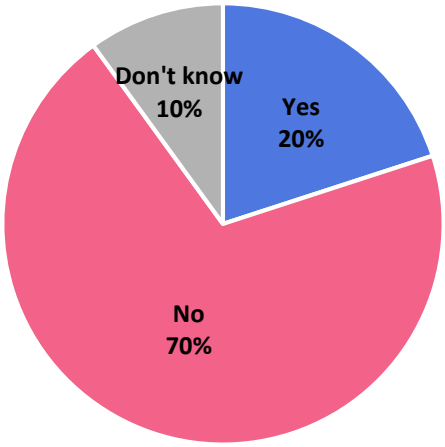
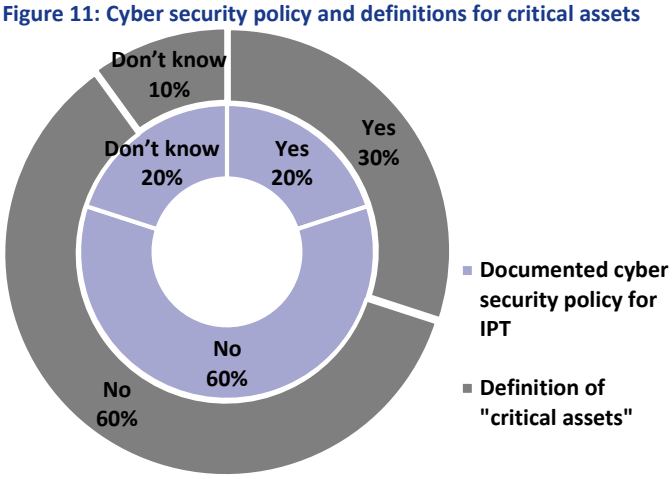


Figure 11: Cyber security policy and definitions for critical assets



5.4 Gap 4: Lack of corporate governance for IPT security[98]

An effective governance framework for IPT security within organisations, setting out clear responsibilities and objectives is still missing.[99] By allocating clear cyber security responsibilities with an organisation, this governance framework (covering common training programmes, the identification and advance warning of threats, support and advice, etc.) would also greatly facilitate cyber security collaboration between IPT and smart city operators on the one hand, and governments, LEA and national CSIRTs on the other.

5.5 Gap 5: No specific security standards for IPT

There is a lack of specific security standards for IPT that can address the specific context and security threats faced by IPT assets. Generic standards, such as the ISO27000 series, are not sufficiently useful for the complex reality of IPT and are poorly related to the security environment within which transport organisations interact and operate today. It is important that standards are able to accommodate new IPT functionalities and concepts as they become relevant, while being able to remain dynamic, extensible and flexible.[100]

5.6 Gap 6: Lack of advanced interdependent analysis tools

Given the highly interconnected and complex nature of transportation networks, there is the need for more sophisticated analysis tools that can capture asset interdependence and cascade-effects among all

---

[97] ISO, "Smart Cities. Preliminary Report 2014", *ISO/IEC publication*, 2015. http://www.iso.org/iso/smart_cities_report-jtc1.pdf

[98] While we have avoided ranking either the identified gaps or challenges, during the validation workshop for this research, practitioners were of the consensus that the lack of corporate governance currently represents the most important gap/challenge facing IPT.

[99] ESADEgeo and Zurich, "Global cyber governance: preparing for new business risks", *Risk Nexus*, April 2015.

[100] The recent work on IPT standards from ETSI and the US Department of Transportation aim at filling this gap at the European and US level. See: http://www.etsi.org/technologies-clusters/technologies/intelligent-transport and http://www.its.dot.gov/standards_strategic_plan/#ID; US Department of Transportation, "Intelligent Transportation Systems (ITS) Standards Program Strategic Plan for 2011–2014 ", *Final report*, April 2011.

the involved assets and different stakeholders. These tools will help capture how interdependencies operate and will heighten impacts in order to develop procedures and policies to improve recovery.[101]

5.7 Gap 7: Lack of advanced risk assessment tools

Risk assessment methodologies that can deal with multiple networked stakeholders working in collaboration need to be developed. This requires a different mind-set for existing risk management approaches, which often begin by scoping a system (*i.e.* defining its borders) prior to a risk assessment based on the individual elements. However, in interconnected systems this clear border does not exist. To address this gap we need to redesign risk management systems/approaches so that they operate from a *stakeholder* perspective rather than *border* perspective.[102] [103]

5.8 Gap 8: Lack of advanced real-time and multi-stakeholder-enabled security technologies

Due to the number of networked technologies applied across the transportation systems, often belonging to different operators and displaying multiple interdependence,[104] [105] there is a need for more advanced security IT infrastructures that allow for multi-stakeholder penetration testing, and provide real-time authentication among both trusted and un-trusted users in a multi-stakeholder environment.[105]

[101] Rae Zimmerman and Carlos E. Restrepo, "Analyzing Cascading Effects within Infrastructure Sectors for Consequence Reduction", Proceedings of the 2009 IEEE International Conference on Technologies for Homeland Security, HST 2009, Waltham, MA.

[102] E. Bekiaris, A. Parkes, A. Stevens and M. Wiethoff, "A Structured Methodology and Preliminary Results of ADAS Risk Assessment, including Technical, Behavioural, Liability and Organisational Risks", 8th WORLD CONGRESS ON ITS, Sydney, Australia, 2001.

[103] See also Riek Joosten and André Smulders, "Networked Risk Management: How to successfully manage risks in hyperconnected value networks", July 2014, TNO. http://publications.tno.nl/publication/34612233/jfvm8m/joosten-2014-networked.pdf

[104] Catherine Mulligan, "ICT and the Future of Transport", Ericsson, 2014. http://www.ericsson.com/res/docs/2014/ict-and-the-future-of-transport.pdf

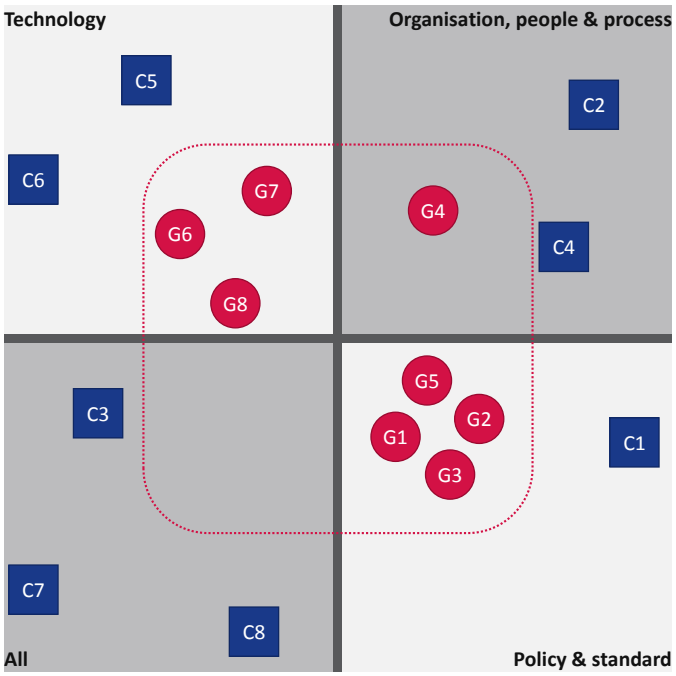
[105] US Department of Homeland Security , "The Future of Smart Cities".

6. Recommendations

This final section of the study provides nine recommendations on how to enhance cyber security within IPT. Recommendations are directed towards different groups of stakeholders, specifically: decision makers; transport operators; and manufactures and solution providers. The recommendations try to accommodate both the rigorous requirements coming from the study and the more practical matters of short-range implementation by practitioners. Each recommendation draws upon the information and analysis presented in earlier sections and has been validated by a range of different stakeholders. Below each recommendation are brief explanatory notes.

Figure 12 summarizes the above mentioned challenges and gaps and allocates them across four areas:

Figure 12: Challenges and gaps



- Gaps and challenges that are mainly related to technology;
- Gaps and challenges that are mainly related to organisation, people and process;
- Gaps and challenges mainly concerning policy and standard; and
- Gaps and challenges concerning a mix of all the previous areas (*i.e.* affecting all the previously mentioned areas).[106]

As the figure indicates, challenges and gaps tend to concentrate in both the *technology and tools* area and *policy and standards* area.

Challenges

C1 Difficulties to integrate security for safety
C2 Inadequate importance and spending being afforded to cyber security
C3 Inadequate checking for countermeasures
C4 Unwillingness to collaborate and exchange information on cyber security
C5 Slow phasing out of legacy systems
C6 Inadequate data exchange between IPT and SC operators
C7 Weak situational awareness of cyber threats
C8 Resistance to security adoption

Gaps

G1: Lack of a common EU approach to IPT
G2: No integration of security in current guidelines or strategies for IPT
G3: Lack of common definitions and formalised cyber security policies
G4: Lack of corporate governance for IPT security
G5: No specific security standards for IPT
G6: Lack of advanced interdependent analysis tools
G7: Lack of advanced risk assessment tools
G8: Lack of advanced real-time and multi-stakeholder-enabled security technologies

[106] The allocation was based on desktop research, survey and interviews

6.1 For decision makers[107]

6.1.1 EC and MS institutions should promote public/private collaboration on IPT cyber security at national level and EU-wide

This requires EC and MS institutions to actively promote greater collaboration, information exchange and knowledge on IPT cyber security across-borders via appropriate measures. For instance, this could take the form of establishing EU multi-stakeholder fora, engaging in regular consultations, conducting awareness campaigns, etc. The objectives of such initiatives will be: to set up cross-border and multi-stakeholder collaboration on cyber security; develop and implement awareness campaigns to educate end-users on risks in smart environments; and share best practices and information about cyber threats, attacks and cyber measures. Regarding this last objective, voluntary reporting of threat incidents to a trusted third party within the EU could be a viable tool for identifying and quantifying threat levels. At the moment in transport there is no real coordination on cyber security across national borders. This recommendation directly addresses challenges C4 and C7 as identified in Figure 12 above, while also having a positive impact on challenges C2, C3, C6 and C8.

6.1.2 EC institutions and agencies should promote and facilitate the development of a common EU approach to IPT security

Relevant EC institutions and agencies (*e.g.* ETSI, CEN, CENELEC, ENISA, DG MOVE) must play an important role in facilitating and promoting integrated industry efforts via open IPT coordination initiatives, whereby standards and common guidelines tailored for cyber security in IPT are produced by interested parties across Europe through a transparent, open and consensus-based process. Transport operators, manufactures and vendors will be consulted in order to gain their support and buy-in for these new standards and guidelines. Existing initiatives on EC standards, led by ETSI, CEN and CENELEC[108], could be further developed and expanded to include wider participation from public and private partnerships, and/or industry stakeholders. In addition, the cross-exchange of knowledge and practices between transport and other sectors (*e.g.* telecommunication, finance, etc.) should be developed to leverage lessons learned and existing good practices. Taken together, these actions would enable the identification of common standards and guidelines for IPT in areas where these are currently less effective and mature (*e.g.* minimum cyber security requirements and good practices that should be in place; implementation of security by design; minimum security requirements for data exchange and collaborative IPT systems among operators, etc.). Such guidelines could be based on the work of ENISA and/or national CSIRTs. This recommendation directly addresses challenges C3-C8 as well as gap G2, while also having a positive impact on gaps G1 and G4-G7.

6.1.3 EC institutions and agencies should develop a comprehensive EU strategy and framework for cyber security in IPT

This suggests that EC institutions should further develop the existing EU cyber security strategy and framework with a greater focus on IPT in order to provide a much more comprehensive, focused and integrated approach to IPT cyber security across Europe. This goes hand-in-hand with efforts to develop an ongoing dialogue with stakeholders to inform on policymaking and to ensure effective implementation of

[107] By "decision makers" we are referring primarily to publically elected/appointed officials with decision-making powers that impact on IPT at both the EU and Member States levels.

[108] These organisations were given a mandate to develop European standards to provide interoperability, compatibility and continuity for the deployment and operational use of ITS (see Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 and Directive 98/34/EC)

the endorsed strategy. The anticipated NIS is an initial step in this direction and a building block for a comprehensive framework. This recommendation directly addresses gaps G1 and G8.

6.1.4 EC and MS should integrate and converge security efforts made in other sectors of activity

IPT operators share similarities with other operators in the usage of systems (*e.g.* ICS/SCADA) and operations. Efforts have already been made in other sectors of activity to enhance their security (*e.g.* Smart Grids). In order to benefit from these existing efforts, Policy Makers from the European Commission and from Member States should assess which measures can be integrated to IPT. Moreover, it is important to converge the efforts when possible, through collaboration and experience sharing. This recommendation directly addresses gaps G1-G3 and challenge C6 and C8.

6.1.5 EC and MS should foster the development of harmonised cyber security standards for IPT

The lack of a dedicated cyber security standard for IPT is an obstacle to the adoption of good security principles by IPT operators, manufacturers and solution vendors. With the support of the EC and MS, the industry (private and public sector) should ensure the development and adoption of harmonised standards adapted to the particularities. One or several completing standards could be developed to cover cyber security from various points of views (*e.g.* technical, organisational, validation of security practices, etc.) as it has been proposed in other domains (*e.g.* Smart Grids). This recommendation directly addressed gaps G1-G3 and challenges C1 and C3.

6.2 For transport operators

6.2.1 IPT operators should integrate cyber security in their corporate governance

This leads transport operators to define the roles and responsibilities of top management as well as the integration of cyber risks into their budgetary, risk and project management operational processes. This does not necessarily mean that transport operators need to develop a new governance framework, but integraty cyber security roles into its current one. The objective is to integrate within the current framework the budget and responsibilities to meet cyber security objectives (*e.g.* training, awareness raising, acquisition, etc.). This recommendation directly addresses challenges C1, C2, C3, C4 and C8, and gaps G3 and G4.

6.2.2 IPT operators should develop and implement an integrated corporate strategy addressing holistically cyber security and safety risks

This requires transport operators develop effective cyber security policies for cyber security in order to start formalising cyber security processes both internally and with the other operators they interact/collaborate with. The policy should also make clear the relationship between security and safety, the minimum security requirements for collaborative IPT initiatives with other operators and the need to report and exchange information and know-how on cyber security with relevant agencies and other operators. If transport operators do not have a clear policy spelling out their objectives for cyber security, and if a senior manager is not clearly responsible for the final outcome within the organisation(s) involved in sharing IPT infrastructures (*i.e.* responsible for management of the cyber risk), then this final outcome will not happen. This recommendation directly addresses challenges C1, C2, C4, C6 and C8, and gaps G6 and G7, while also having a positive impact on challenges C5 and C7.

6.2.3 IPT operators should implement risk management for cyber security in multi-stakeholder environments including external contractors and dependencies

This entails that transport operators should have tailored risk management processes in place for cyber security which involve all the relevant participating operators and are integrated into their corporate risk frameworks. These processes shall also include external contractors that interact with the IPT operators.

This will improve standardisation and consistency on how to manage cyber security risks within all the participant organisations, while supporting managers with cyber security responsibilities in doing their jobs. Transport operators should also think of involving other external stakeholders, such as end-users and civil society, as part of their approach to managing cyber risk. These external stakeholders could bring valuable, external insights and a customer or citizen point of view, which are necessary for the effective management of cyber risks. This recommendation directly addresses challenge C7 and gaps G3 and G4, while also having a positive impact on challenge C4.

6.2.4 IPT operators should clearly and routinely specify their cyber security requirements

This suggests that transport operators should routinely and clearly specify their cyber security requirements for all their transports initiatives and projects as part of their risk management processes. Such activities should not be "one-off events", rather they should be a part of regular cyber security reviews. These cyber security requirements can then be incorporated into the beginning of project-cycles through the use of security by design. They also provide a guide for enhancing the cyber security of future infrastructure developments when planning the phasing-out of legacy systems. This recommendation directly addresses challenges C5 and C8.

6.2.5 IPT operators should annually review organisational cyber security processes, practices and infrastructures

This suggests that transport operators should check and review their internal processes, practices and infrastructures for cyber security every year as part of the organisation's corporate review and performance management procedures. It also feed into the goal of creating/strengthening a cyber security practice knowledge base among IPT stakeholders. This annual review should be done in parallel with the review of overall risk management procedures. Senior managers discuss and assess how well the organisation has performed in relation to its cyber security objectives, and assess whether the implemented cyber security processes, practices, training, infrastructures and tools have been adequate. This review provides a systematic and periodic process for assessing the organisation's cyber security performance in relation to certain pre-established criteria and organisational objectives, while identifying needs for further enhancement and next steps. This recommendation directly addresses challenges C3, while also having a positive impact on challenges C5 and C8, and gaps G3-G5.

6.3 For manufacturers and solution providers

6.3.1 Manufacturers and solution providers should create products/solutions that match the cyber security requirements of IPT end-users

Manufacturers and providers should increase their collaboration with end-users in relation to R&D, while aligning their solutions much more closely to the cyber security requirements, needs and affordability concerns of end-users. Solutions should be specifically tailored to address both existing gaps and the needs of end-users that the end-users themselves have identified via their own risk analyses (examples here may include; the development of advanced interdependent analysis tools, improving real-time capabilities, developing advanced risk assessment tools that can operate in multi-stakeholder environments, and technologies that enable security). Products should also be developed by employing security by design principles including; defence in depth, separation of privilege, securing the weakest link, promoting privacy, etc. At the moment solutions tend to be too general and do not reflect the contextual reality of IPT offerings. This recommendation directly addresses gaps G3-G5.

6.3.2 Manufacturers and solution providers should collaborate in the development of IPT-specific standards and apply them to IPT solutions

This recommends that manufacturers and providers should collaborate in the development of security standards tailored for IPT by participating in open IPT coordination initiatives (see recommendation in Section 6.1.2), while also meeting all applicable EU and international standards in the development of their products and solutions (*e.g.* ETSI, Intelligent Transport Systems (ITS); Security; Security header and certificate formats, 2015 and US government, Federal Information Security Management Act - FISMA, 2002). This recommendation directly addresses gap G2.

6.3.3 Manufacturers and solution providers should develop a trusted information sharing platform on risks and vulnerabilities

A trusted information sharing platform offers the possibility to its participants to exchange knowledge on risks and vulnerabilities. The trust aspect of such platform is necessary to ensure good participation, as it constitutes an incentive to share about incidents and solutions. For Intelligent Public Transports, it is recommended that manufacturers and solution providers participate to the development of such a trusted information sharing platform. The objective is to understand existing vulnerabilities in IPT systems, the risks associated to IPT as well as to promote possible solutions in order to improve the readiness level of the participants. This recommendation directly addresses challenges C4 and C7 as well as gap G3.

6.3.4 Manufacturers and solution providers should provide security guidance for your systems, products and solutions

IPT operators who integrate new systems needs guidance to do it securely. Manufacturers and service providers should provide security guidance to describe proper procedures and parameters for secure configuration, operation and maintenance. Such guidance should lead IPT operators to improve their awareness and clarify liabilities. For instance, one possible guidance regarding patch management could explain the consequences on patching systems in relation to compatibility and availability. This recommendation directly addresses challenges C6 and C7 as well as gaps G6 and G7.

Annexes

A.1 Key EU legislation and policy/strategy documents affecting IPT

Table 3 describes the legislation and policies that combine to form the *legal and policy environment* governing IPT at the EU level.

Table 3: EU legislation and policy documents

EXISTING EU LEGISLATION		
Title	**General Description**	**Impact on IPT**
Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data	Under this Directive, MS shall protect the fundamental rights and freedoms of citizens, and in particular their right to privacy with respect to the processing of personal data, as well as ensuring the free movement of such data between MS.	This Directive (together with Directive 2002/58/EC) sets out rules protecting fundamental rights and freedoms of individuals, specifically in relation to data privacy, security and the re-use of information. This includes passengers on IPT networks.
Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)	Directive 2002/58/EC complements Directive 1995/46/EC. It concerns the protection of privacy with respect to the processing of personal data in the electronic communication sector, as well as ensuring the free movement of such data between MS.	This Directive (together with Directive 1995/46/EC) sets out rules protecting fundamental rights and freedoms of individuals, specifically in relation to consent, privacy, security and the re-use of information. Services provided to the public within IPT networks via electronic communications will need to have regard for this Directive. Use of location data linked to user's devices, provision of security, use of cookies, and recording/storage of data are all possible issues here.
Directive 2009/33/EC on the promotion of clean and energy-efficient road transport vehicles	This Directive requires applicable authorities, entities and operators to take into account lifetime energy and environmental impacts when purchasing road transport vehicles. This includes energy consumption and emissions of CO2 and of certain pollutants.	Directive (2009/33/EC) applies to public transport, including; railways, automated systems, tramways, trolley buses, and buses. However, the focus is very narrow covering only a specific set of environmental vehicle specifications.
Directive 2010/40/EU on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport	This Directive establishes a framework to support the coordinated, coherent deployment and use of Intelligent Transport Systems (ITS) within the EU. It also provides for the development of specifications and necessary standards within areas including; ITS road safety and security, linking vehicles with transport infrastructure, optimal use of data, and continuity of service.	Defines ITS. Enables the EC to adopt specifications necessary to ensure the compatibility, interoperability and continuity for the deployment and operational use of ITS. Also, promotes the development of necessary standards in these areas. Sets out rules on privacy, security and the reuse of information.

Directive 2008/57/EC on the interoperability of the rail system within the Community	This Directive concerns the provisions relating to the interoperability constituents, the interfaces and procedures, as well as the conditions of overall compatibility of the rail systems across the EU, that are required to achieve its interoperability.	This Directive establishes Technical Specifications for Interoperability (TSIs) for the subsystems that comprise the trans-European rail system. No specific mention of ITS, however, the development of interoperability across national rail networks provides a convenient common platform for developers of ITS to utilise and link into.
FUTURE EU LEGISLATION		
Title	**General Description**	**Impact on IPT**
Proposed **NIS Directive**[109] concerning measures to ensure a high common level of network and information security across the Union	The aim of the proposed Directive is to ensure a high common level of network and information security (NIS). This means improving the security of the Internet and the private networks and information systems underpinning the functioning of EU societies and economies.	Operators of critical infrastructures, including transport, will be required to manage cyber security risks and report serious incidents to their national competent authorities.
PRINCIPLE EU POLICY & STRATEGY DOCUMENTS		
Title	**General Description**	**Impact on IPT**
Action Plan for the Deployment of Intelligent Transport Systems in Europe - COM(2008) 886 final/2 – CORRIGENDUM	This Action Plan aims to accelerate and coordinate the deployment of Intelligent Transport Systems (ITS) in road transport, including interfaces with other transport modes.	While the overall focus of this Action Plan is wider than just security and resilience of ITS, specific actions identified within this plan are applicable. These include: the optimal use of traffic/travel data; road safety and security; integration of the vehicle into the transport infrastructure; data security and protection and liability issues; and European ITS cooperation and coordination.
Internet of Things - An action plan for Europe - COM(2009) 278 final	This action plan sets out 14 "Lines of Action" regarding the future design of objects/systems falling under the Internet of Things (IoT) umbrella. Specifically this introduces questions of privacy, the monitoring of individuals, and the storage of personal data. Also issues of design standardisation are raised.	The IoT will become integrated into the ICT networks of Smart Cities and IPT systems. This action plan is useful in that it raises a number of issues yet to be addressed. As the IoT develops and becomes integrated elements of this action plan will take on increased significance.

[109] EC, "EU Cybersecurity plan to protect open internet and online freedom and opportunity - Cyber Security strategy and Proposal for a Directive". http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

Title	General Description	Impact on IPT
A Digital Single Market Strategy for Europe - COM(2015) 192 final	The overall aim is to develop a Digital Single Market across EU cyber space whereby the principle of free movement of people, goods, services and capital is translated and applied online.	This Strategy has the potential to impact the technical operation of ICT networks, create a more joined-up approach to the development of online network security solutions, and boost the development of standards for interoperability in the transport sector.
European Innovation Partnership on Smart Cities and Communities: Strategic Implementation Plan	Presents the Strategic Implementation Plan for creating Smart Cities produced by the High Level Group of the European Innovation Partnership for Smart Cities and Communities.	This plan places strong emphasis on urban mobility (*i.e.* map public transport) and the integration of infrastructure assets and processes across energy, ICT and transport to improve the efficiency and sustainability of cities (*i.e.* creating IPT).
Roadmap to a Single European Transport Area – Towards a competitive and resource efficient transport system - COM(2011) 144 final	Focus is on how to remove barriers and bottlenecks so as to complete the *internal market for transport* by creating a competitive and sustainable transport market within the EU.	While the focus is limited the Roadmap does specifically mention the development of smart mobility systems such as intelligent transport systems, and the need for regulatory frameworks to protect privacy and personal data in parallel with the wider use of information technology tools. Highlights standardisation and interoperability as keys to avoiding the technological fragmentation of the European transport market.
Rolling plan for ICT Standardisation	This Rolling Plan provides a multi-annual overview of the needs for preliminary or complementary ICT standardisation activities to undertake in support of EU policy activities.	Within Intelligent Transport Systems, this document sets out the standards developments that have occurred and the legislation and policy documents at the European and (to a lesser extent) at the MS level.
Smart Cities and Communities – European Innovation Partnership - COM(2012) 4701 final	Covering Smart Cities and Communities European Innovation Partnerships; these are partnerships across the areas of energy, transport and information and communication with the objective to catalyse progress in areas where energy use, mobility and transport, and ICT are intimately linked.	Strong focus on energy efficiency and environmental concerns, this communication does emphasise the need for interoperability of smart technologies. Highlights the lack of standards and the immaturity of the market in truly integrated energy, transport and ICT solutions as market impediments.

A.2 Top critical functions, assets, and threats identified for Intelligent Public Transport

Table 4 below lists the critical societal/business functions, assets and threats identified for IPT during the survey and the interviews. While all of these functions, assets and threats are to be treated as critical they have also been ranked by the end-users who have participated in the stocktaking and may be subjective.

Table 4: Top critical functions, assets and threats

TOP 5 CRITICAL SOCIETAL/BUSINESS FUNCTIONS	TOP 21 CRITICAL ASSETS	TOP 15 CRITICAL THREATS
1 Passenger safety and security	**1** Payment systems	**1** Distributed denial of service attack (DDoS)
= Transportation safety and security	**=** Financial viability	**2** Terrorism and/or state sponsored attacks
3 Data protection and privacy	**3** Internet & networking	**3** Manipulation of hardware and/or software
= Traffic and vehicle management	**=** Networking &communication components	**4** Interruption and/or disruption of electrical supply
5 Sustainable urban mobility	**=** Radio telecommunication	**=** Interruption and/or disruption of frequency
	= On-board equipment	**=** Software failure and/or errors
	7 Operational control centres	**7** Natural disasters
	= Physical infrastructure	**=** Environmental disasters
	= Data	**9** Malware and viruses
	= Power distribution grid	**=** Hardware failure and/or malfunctions
	11 Identity management systems	**11** Unauthorised use and/or access
	12 Safety systems	**=** Loss of (integrity of) sensitive information/data
	= Passenger safety systems	**=** Tampering and/or alteration of data including insertion of information
	14 Integrity and availability of data and communications	**14** Operator and/or user errors
	= Staff	**15** Strike
	16 Reputation	
	= Confidentiality	
	= Data protection and privacy	
	19 Availability of law enforcement	
	20 Public communication and social media	
	= Information distribution systems	

LEGEND	FUNCTIONS AND ASSETS	THREATS
	Societal critical	Unintentional damages
	Business critical	Insider threats
		Nefarious activities/abuses
		Physical and large-scale attacks
		Acts of nature/environmental incidents
		Accidental errors / malfunctions / failures
		Disruptions/outages

A.3 Threats to individual assets

Table 5 below associates the threat groups and individual threats to all assets functions.

Table 5: Complete list of threats

THREAT GROUPS	BUSINESS ASSETS AND FUNCTIONS	SOCIETAL ASSETS AND FUNCTIONS
Physical and large scale attacks		
Terrorism and/ or state sponsored attacks	All	All
Unauthorised use and/or access	Traffic and vehicle management, Transportation safety and security, Sales, fees and charges, Resilient management structure, Energy and environment	Sustainable urban mobility, Passenger safety and security, Sustainable environment, Data protection and privacy
Vandalism and/or civil disorder	Traffic and vehicle management, Transportation safety and security, Sales, fees and charges, Energy and environment	Sustainable urban mobility, Passenger safety and security, Sustainable environment
Violence and/or shooting within sites	Traffic and vehicle management, Resilient management structures	Passenger safety and security
Theft of data and/or infrastructures	Traffic and vehicle management, Transportation safety and security, Resilient management structures, Energy and environment	Sustainable urban mobility, Passenger safety and security, Sustainable environment, Data protection and privacy
Acts of nature / environmental incidents		
Natural disasters	All	All
Environmental disasters	All	All
Accidental errors/malfunctions/failures		
Hardware failure and /or malfunctions	Traffic and vehicle management, Transportation safety and security, Sales, fees and charges, Resilient management structures, Energy and environment	Sustainable urban mobility, Passenger safety and security, Sustainable environment
Software failure and/or malfunctions	Traffic and vehicle management, Transportation safety and security, Sales, fees and charges, Resilient management structures, Energy and environment	Sustainable urban mobility, Passenger safety and security, Sustainable environment
Loss of (integrity of) sensitive information/data	Traffic and vehicle management, Transportation safety and security, Resilient management structures	Data protection and privacy, Sustainable urban mobility

THREAT GROUPS	BUSINESS ASSETS AND FUNCTIONS	SOCIETAL ASSETS AND FUNCTIONS
Configuration errors	Traffic and vehicle management, Transportation safety and security, Sales, fees and charges, Resilient management structures, Energy and environment	Sustainable urban mobility, Passenger safety and security, Sustainable environment
Disruption and/or outages		
Interruption and/or disruption of electrical supply	All assets (excepting people/living things and exclusively physical infrastructures)	All assets (excepting people/living things and exclusively physical infrastructures)
Interruption and/or disruption of frequency	All assets (excepting people/living things and exclusively physical infrastructures)	All assets (excepting people/living things and exclusively physical infrastructures)
Strike	Resilient management structures	Sustainable urban mobility
Nefarious activity /abuse		
Distributed denial of service attacks (DDoS)	Traffic and vehicle management, Transportation safety and security, Sales, fees and charges, Resilient management structures, Energy and environment	Sustainable urban mobility, Passenger safety and security, Sustainable environment
Manipulation of hardware and/or software	All assets (excepting people/living things and data)	All assets (excepting people/living things and data)
Malware and viruses	Traffic and vehicle management, Transportation safety and security, Sales, fees and charges, Resilient management structures, Energy and environment	Sustainable urban mobility, Passenger safety and security, Sustainable environment
Tempering and/or alteration of data including insertion of information	Traffic and vehicle management, Transportation safety and security, Resilient management structures	Data Protection and privacy
Hacking of wireless , connected assets	Traffic and vehicle management, Transportation safety and security, Sales, fees and charges, Resilient management structures, Energy and environment	Sustainable urban mobility, Passenger safety and security, Sustainable environment
Data breaches	Traffic and vehicle management, Transportation safety and security, Resilient management structures	Data Protection and privacy, Integrated infrastructure and processes
Identity theft	Traffic and vehicle management, Sales, fees and charges, Resilient management structures	Sustainable urban mobility, Data Protection and privacy

THREAT GROUPS	BUSINESS ASSETS AND FUNCTIONS	SOCIETAL ASSETS AND FUNCTIONS
Exploitation of software bugs	Traffic and vehicle management, Transportation safety and security, Sales, fees and charges, Resilient management structures, Energy and environment	Sustainable urban mobility, Passenger safety and security, Sustainable environment
Abuse of authorisation	Traffic and vehicle management, Transportation safety and security, Sales, fees and charges, Resilient management structures	Sustainable urban mobility, Passenger safety and security, Sustainable environment
Abuse of information leakages	Traffic and vehicle management, Transportation safety and security, Resilient management structures	Data Protection and privacy
Intentional disclosure	Traffic and vehicle management, Resilient management structures	Data Protection and privacy
Falsification of records including certification	All assets (excepting people/living things)	All assets (excepting people/living things)
Eavesdropping and/or wiretapping	Traffic and vehicle management, Transportation safety and security, Resilient management structures	Sustainable urban mobility, Data protection and privacy
Insider threats		
Stealing information or manipulation of data	Traffic and vehicle management, Transportation safety and security, Resilient management structures	Sustainable urban mobility, Data Protection and privacy
Sales of important data to competitors	Traffic and vehicle management, Transportation safety and security, Resilient management structures	Data protection and privacy
Leaking information	Ditto	Ditto
Unintentional damage		
Operator and/or user errors	All assets (excepting people/living things)	All assets (excepting people/living things)
Configuration errors	See configuration errors above	See configuration errors above
Accidental disclosure	Traffic and vehicle management, Transportation safety and security, Resilient management structures	Data protection and privacy
Mismanagement	All	All

A.4 Reference guide for applying good practices to Intelligent Public Transport

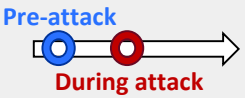
Table 3 provides a reference guide of the current good practices identified for IPT whereby the practices are described according to both the business/societal functions identified in Section 2.3, and the different threat groups identified in Section 3.1.1. In addition these good practices are assessed according to when they should be applied using the following three categories: [110]

- ***Pre-attack good practices:*** Focus is on identifying threats to, and weaknesses within, an IPT network and increasing the preparedness and resilience of that network prior to attacks such that threats can be reduced or even negated.
- ***During attack good practices:*** Focuses on both measures that will enable the operator to identify that an attack is occurring, as well as measures to be implemented once an ongoing attack is detected so as to halt and/or mitigate the consequences of that attack.
- ***Post-attack good practices:*** Focuses on system monitoring practices that will enable the operator to identify that an attack has occurred, returning the network to its pre-attack state, gathering evidence on the nature and perpetrators of the attacks, and identifying lessons-learnt for improving the security of the network to resist future similar attacks.

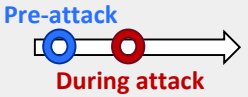
Table 6: Good practice security measures for protecting IPT

GOOD PRACTICE	BUSINESS / SOCIETAL FUNCTIONS	THREAT GROUPS ADDRESSED	WHEN TO APPLY GOOD PRACTICE
Technical good practices			
Conduct security-focused risk assessments	• *Traffic & vehicle management / Sustainable urban mobility* • *Transportation safety and security / Passenger safety and security* • *Energy and environment / Sustainable environment* • *Sales, fees & charge / Data protection & privacy/ Resilient management structure*	• *Unintentional damage* • *Physical & large-scale threats* • *Acts of nature/environmental incidents* • *Accidental errors/malfunctions/ failures* • *Disruptions/outages* • *Nefarious activities/abuse* • *Insider threats*	Pre-attack Post-attack 

[110] This Refers to when the good practice should be engaged so as to address the different threat groups. It does not refer to when the good practice should be developed and implemented by the IPT operator – which will always be "before the threat has manifested itself".

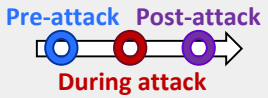
GOOD PRACTICE	BUSINESS / SOCIETAL FUNCTIONS	THREAT GROUPS ADDRESSED	WHEN TO APPLY GOOD PRACTICE
Employ physical security, access controls and protection measures	• *Traffic & vehicle management / Sustainable urban mobility* • *Transportation safety and security / Passenger safety and security*	• *Unintentional damage* • *Physical & large-scale threats* • *Accidental errors/malfunctions/ failures* • *Nefarious activities/abuse* • *Insider threats*	
Employ secure digital access controls to networks and data	• *Traffic & vehicle management / Sustainable urban mobility* • *Transportation safety and security / Passenger safety and security* • *Sales, fees & charge / Data protection & privacy/ Resilient management structure*	• *Unintentional damage* • *Physical & large-scale threats* • *Accidental errors/malfunctions/ failures* • *Nefarious activities/abuse* • *Insider threats*	
Employ alarms/surveillance for protecting physical and digital assets	• *Traffic & vehicle management / Sustainable urban mobility* • *Transportation safety and security / Passenger safety and security* • *Energy and environment / Sustainable environment* • *Sales, fees & charge / Data protection & privacy/Resilient management structure*	• *Unintentional damage* • *Physical & large-scale threats* • *Accidental errors/malfunctions/ failures* • *Nefarious activities/abuse* • *Insider threats*	
Encryption	• *Traffic & vehicle management / Sustainable urban mobility* • *Transportation safety and security / Passenger safety and security* • *Sales, fees & charge / Data protection & privacy / Resilient management structure*	• *Unintentional damage* • *Physical & large-scale threats* • *Accidental errors/malfunctions/ failures* • *Nefarious activities/abuse* • *Insider threats*	
Develop secure and private communication networks	• *Traffic & vehicle management / Sustainable urban mobility* • *Transportation safety and security / Passenger safety and security* • *Sales, fees & charge / Data protection & privacy / Resilient management structure*	• *Physical & large-scale threats* • *Nefarious activities/abuse*	

GOOD PRACTICE	BUSINESS / SOCIETAL FUNCTIONS	THREAT GROUPS ADDRESSED	WHEN TO APPLY GOOD PRACTICE
Employ intrusion detection systems (IDSs)	• *Traffic & vehicle management / Sustainable urban mobility* • *Transportation safety and security / Passenger safety and security* • *Energy and environment /Sustainable environment* • *Sales, fees & charge / Data protection & privacy / Resilient management structure*	• *Unintentional damage* • *Physical & large-scale threats* • *Accidental errors/malfunctions/ failures* • *Nefarious activities/abuse*	
Employ identity management and authentication systems	• *Traffic & vehicle management / Sustainable urban mobility* • *Transportation safety and security / Passenger safety and security* • *Sales, fees & charge / Data protection & privacy / Resilient management structure*	• *Unintentional damage* • *Physical & large-scale threats* • *Accidental errors/malfunctions/ failures* • *Nefarious activities/abuse* • *Insider threats*	
Integrate shut-down procedures/remote deactivation of capabilities	• *Traffic & vehicle management / Sustainable urban mobility* • *Transportation safety and security / Passenger safety and security* • *Energy and environment / Sustainable environment*	• *Unintentional damage* • *Physical & large-scale threats* • *Accidental errors/malfunctions/ failures* • *Nefarious activities/abuse*	
Operate in degraded mode of operation	• *Traffic & vehicle management / Sustainable urban mobility* • *Transportation safety and security / Passenger safety and security* • *Sales, fees & charge / Data protection & privacy / Resilient management structure*	• *Unintentional damage* • *Physical & large-scale threats* • *Acts of nature/environmental incidents* • *Accidental errors/malfunctions/ failures* • *Nefarious activities/abuse*	
Policies and standards			
Employ security by design	• *Traffic & vehicle management / Sustainable urban mobility* • *Transportation safety and security / Passenger safety and security* • *Energy and environment / Sustainable environment* • *Sales, fees & charge / Data protection & privacy / Resilient management structure*	• *Unintentional damage* • *Physical & large-scale threats* • *Accidental errors/malfunctions/ failures* • *Disruptions/outages* • *Nefarious activities/abuse* • *Insider threats*	

GOOD PRACTICE	BUSINESS / SOCIETAL FUNCTIONS	THREAT GROUPS ADDRESSED	WHEN TO APPLY GOOD PRACTICE
Establish disaster recovery processes and maintain back-ups	• *Traffic & vehicle management / sustainable urban mobility* • *Transportation safety and security / Passenger safety and security* • *Energy and environment / Sustainable environment* • *Sales, fees & charge / Data protection & privacy / Resilient management structure*	• *Unintentional damage* • *Physical & large-scale threats* • *Acts of nature/environmental incidents* • *Accidental errors/malfunctions/ failures* • *Disruptions/outages* • *Nefarious activities/abuse* • *Insider threats*	
Define degraded modes of operation	• *Traffic & vehicle management / Sustainable urban mobility* • *Transportation safety and security / Passenger safety and security* • *Sales, fees & charge / Data protection & privacy / Resilient management structure*	• *Unintentional damage* • *Physical & large-scale threats* • *Acts of nature/environmental incidents* • *Accidental errors/malfunctions/ failures* • *Nefarious activities/abuse*	
Implement an information security policy	• *Transportation safety and security / Passenger safety and security* • *Sales, fees & charge / Data protection & privacy / Resilient management structure*	• *Unintentional damage* • *Physical & large-scale threats* • *Accidental errors/malfunctions/ failures* • *Nefarious activities/abuse* • *Insider threats*	
Forecasting, early warning systems and risk analysis	• *Traffic & vehicle management / Sustainable urban mobility* • *Transportation safety and security / Passenger safety and security* • *Energy and environment / Sustainable environment* • *Sales, fees & charge / Data protection & privacy / Resilient management structure*	• *Unintentional damage* • *Physical & large-scale threats* • *Acts of nature/environmental incidents* • *Accidental errors/malfunctions/ failures* • *Disruptions/outages* • *Nefarious activities/abuse* • *Insider threats*	
Separate critical systems from non-critical systems	• *Traffic & vehicle management / Sustainable urban mobility* • *Transportation safety and security / Passenger safety and security*	• *Unintentional damage* • *Physical & large-scale threats* • *Accidental errors/malfunctions/ failures* • *Nefarious activities/abuse* • *Insider threats*	

GOOD PRACTICE	BUSINESS / SOCIETAL FUNCTIONS	THREAT GROUPS ADDRESSED	WHEN TO APPLY GOOD PRACTICE
Enhance physical security protecting critical physical infrastructure	• *Traffic & vehicle management / Sustainable urban mobility* • *Transportation safety and security / Passenger safety and security* • *Energy and environment / Sustainable environment*	• *Unintentional damage* • *Physical & large-scale threats* • *Accidental errors/malfunctions/ failures* • *Nefarious activities/abuse* • *Insider threats*	
Implement a security control centre with real-time monitoring	• *Traffic & vehicle management / Sustainable urban mobility* • *Transportation safety and security / Passenger safety and security* • *Energy and environment / Sustainable environment*	• *Unintentional damage* • *Physical & large-scale threats* • *Acts of nature/environmental incidents* • *Accidental errors/malfunctions/ failures* • *Disruptions/outages* • *Nefarious activities/abuse* • *Insider threats*	
Ensure redundancy for critical systems	• *Traffic & vehicle management / Sustainable urban mobility* • *Transportation safety and security / Passenger safety and security* • *Energy and environment / Sustainable environment* • *Sales, fees & charge / Data protection & privacy/Resilient management structure*	• *Unintentional damage* • *Physical & large-scale threats* • *Acts of nature/environmental incidents* • *Accidental errors/malfunctions/ failures* • *Disruptions/outages* • *Nefarious activities/abuse* • *Insider threats*	
Create resilient communication systems	• *Traffic & vehicle management / Sustainable urban mobility* • *Transportation safety and security / Passenger safety and security*	• *Unintentional damage* • *Physical & large-scale threats* • *Acts of nature/environmental incidents* • *Accidental errors/malfunctions/ failures* • *Disruptions/outages*	
Create resilient power systems	• *Traffic & vehicle management / Sustainable urban mobility* • *Energy and environment /Sustainable environment*	• *Unintentional damage* • *Physical & large-scale threats* • *Acts of nature/environmental incidents* • *Accidental errors/malfunctions/ failures* • *Disruptions/outages*	

GOOD PRACTICE	BUSINESS / SOCIETAL FUNCTIONS	THREAT GROUPS ADDRESSED	WHEN TO APPLY GOOD PRACTICE
Organisational, people and processes			
Monitor and record activity	• *Traffic & vehicle management / Sustainable urban mobility* • *Transportation safety and security/ Passenger safety and security* • *Sales, fees & charge /Data protection & privacy / Resilient management structure*	• *Unintentional damage* • *Physical & large-scale threats* • *Acts of nature/environmental incidents* • *Accidental errors/malfunctions/ failures* • *Disruptions/outages* • *Nefarious activities/abuse* • *Insider threats*	
Define security requirements during procurement processes	• *Traffic & vehicle management / Sustainable urban mobility* • *Transportation safety and security / Passenger safety and security*	• *Unintentional damage* • *Physical & large-scale threats* • *Accidental errors/malfunctions/ failures* • *Nefarious activities/abuse* • *Insider threats*	
Coordinate with LEAs and CSIRTs	• *Traffic & vehicle management / Sustainable urban mobility* • *Transportation safety and security / Passenger safety and security* • *Energy and environment / Sustainable environment* • *Sales, fees & charge / Data protection & privacy / Resilient management structure*	• *Unintentional damage* • *Physical & large-scale threats* • *Acts of nature/environmental incidents* • *Accidental errors/malfunctions/ failures* • *Disruptions/outages* • *Nefarious activities/abuse* • *Insider threats*	
Raise awareness on cyber threats to all levels of staff including management	• *Traffic & vehicle management / Sustainable urban mobility* • *Transportation safety and security / Passenger safety and security* • *Energy and environment / Sustainable environment* *Sales, fees & charge / Data protection & privacy / Resilient management structure*	• *Unintentional damage* • *Physical & large-scale threats* • *Accidental errors/malfunctions/ failures* • *Disruptions/outages* • *Nefarious activities/abuse* • *Insider threats*	

GOOD PRACTICE	BUSINESS / SOCIETAL FUNCTIONS	THREAT GROUPS ADDRESSED	WHEN TO APPLY GOOD PRACTICE
Engage in staff training	• *Traffic & vehicle management / Sustainable urban mobility* • *Transportation safety and security / Passenger safety and security* • *Sales, fees & charge / Data protection & privacy / Resilient management structure*	• *Unintentional damage* • *Physical & large-scale threats* • *Acts of nature/environmental incidents* • *Accidental errors/malfunctions/ failures* • *Disruptions/outages* • *Nefarious activities/abuse* • *Insider threats*	
Develop organisational and operational procedures and guidelines	• *Traffic & vehicle management / Sustainable urban mobility* • *Transportation safety and security / Passenger safety and security* • *Energy and environment / Sustainable environment* • *Sales, fees & charge / Data protection & privacy / Resilient management structure*	• *Unintentional damage* • *Physical & large-scale threats* • *Acts of nature/environmental incidents* • *Accidental errors/malfunctions/ failures* • *Disruptions/outages* • *Nefarious activities/abuse* • *Insider threats*	

A.5 Survey questions

The following are the survey questions used for the initial elicitation of information on cyber security within both IPT and Smart Cities.

Organisational description

1. What organisation are you affiliated with?

2. What is your role within this organisation?

3. Which of the following sectors does your organisation belong to? (select one option and include any additional details if requested)

- Professional organisation (please specify)
- Public transport operator (which mode(s) of public transport: metro, bus, light-rail, tram, other?)
- Vendor (please specify primary area)
- Service provider (please specify service area)
- Manufacturer (what products do you manufacture?)
- EU level organisation/representative (please specify: *e.g.* policy maker, regulator, elected representative, administrative authority, etc.)
- Member State level organisation/representative (please specify: *e.g.* policy maker, regulator, elected representative, administrative authority, etc.)
- Local government (please specify area of control: *e.g.* single-city municipality, district, region, etc.)
- Academia/research (please specify: *e.g.* university, research centre, think-tank, etc.)
- Civil society (please specify)
- Other (please specify)

4. Please state which country your organisation is based in, or if multi-national/EU-wide, please describe this here:

5. Please state the Smart City your organisation operates in/has responsibility over, also indicating the size of that city using the following scale ≤500k = small, 500k<1,000k = medium, 1,000k+ = large. If you operate in multiple Smart Cities, choose up to 5 for inclusion here.

6. What is the size of your organisation?

- 1-9 employees/members
- 10-49 employees/members
- 50-249 employees/members
- 250+ employees/members

General attitudes to Smart Cities and Intelligent Public Transport

7. In your experience how important are each of the following components for making a city "smart"? (please rate all of the following components as either: not-important / low-importance / medium-importance / high-importance / crucial)

- "In-the-field" and physical infrastructures
- Data collection and processing
- Connectivity and digital networking
- Data exchange/collaboration
- Smart applications
- Analytics and new knowledge extraction

- Mobile and virtual technology
- Multichannel platforms
- Cyber/network security
- Human infrastructure
- Social capital
- Integrated services
- Smart services
- Personalised services
- Business-citizen collaboration
- eGovernance activities
- Government smart city policies
- Smart city legislation
- Clear vision/objectives for the future
- Other (please specify the component)

8. Does your organisation engage in and/or enable Smart City collaboration in the following forms (yes/no/don't know):

- Across sectors? (please name the sectors)
- Between multiple Smart Cities? (please name the cities)
- Across national borders (please name the countries)

9. Does your organisation have or use a definition for "intelligent transport"?

- Yes (please provide this definition)
- No
- Don't know

Data flow via Information Technologies in Smart Cities

10. Based on your experience, in order for Intelligent Public Transport to operate effectively within a Smart City which of the following aspects of Smart Cities should be linked with Intelligent Public Transport? (please indicate as many as you consider relevant)

- Financial/banking components
- Energy
- Health systems
- Public safety components
- Logistics
- Retail
- Water/wastewater
- Telecoms
- Traffic lights and other traffic-flow systems
- Other (please specify aspect)
- Don't know

11. Does your organisation either exchange data with other operators, or recommend the exchange of data between operators, to support Smart Cities?

- Yes - If "yes" what data does your organisation exchange/recommend to be exchanged and with whom? Please specify the nature of this data (*e.g.* traffic data, ticketing data, financial transaction data, etc.) and recipient of this data (*e.g.* public transport operators, governments, service providers, etc.)

- No - If "no" what are the key reasons/inhibitors that are preventing your organization from exchanging/recommending the exchange of this data? (for example are they - technological constraints (please specify), financial costs (please specify), legal reasons (please specify), security concerns (please specify), trust concerns (please specify), organisational constraints (please specify), resource constraints (please specify), other (please specify))
- Don't know

12. In relation to the exchanging of data within Smart Cities:

- **Are there specific technology(s) you use or recommend be used to facilitate the exchange of data within Smart Cities?** (please specify what these technologies are)
- **Are there specific process(es) you use or recommend be used to facilitate the exchange of data within Smart Cities?** (please specify what these processes are)
- **Are there specific standard(s) you use or recommend be used to facilitate the exchange of data within Smart Cities?** (please specify what these standards are)

13. From the list provided, which of the following components of a Smart City's architecture would your organisation be most likely to either integrate with, or recommend that they be integrated? (please select as many options as are relevant)

- Data and data storage layer
- Software/applications
- Business processes/service delivery
- System networking
- Sensors and other monitoring devices
- Physical infrastructure
- Operating system
- None - we do not integrate
- Don't know

13.1 Please provide details about the specific nature of any component integration you selected from the list in Q.13 above

14. From the list provided, which of the following components of Intelligent Public Transport would your organisation be most likely to either integrate with, or recommend that they be integrated? (please select as many options as are relevant)

- Data and data storage layer
- Software/applications
- Business processes/service delivery
- System networking
- Sensors and other monitoring devices
- Physical infrastructure
- Operating system
- None - we do not integrate
- Don't know

14.1. Please provide details about the specific nature of any component integration you selected from the list above

Legislation

15. Are you aware of any specific pieces of legislation that apply to Intelligent Public Transport?

- Yes (please list this legislation)
- No
- Don't know

16. Does your organisation either have a documented cyber security policy in place for Intelligent Public Transport, or recommend to others that they should implement one?

- Yes
- No
- Don't know

17. Within the context of Intelligent Public Transport, does your organisation have or use a definition for "critical assets" (either business critical or societal critical)?

- Yes (what is this definition?)
- No
- Don't know

18. Specifically in relation to Intelligent Public Transport, which of the following are critical assets that your organisation either includes in its own cyber security policy/procedures, or recommends others to include in their cyber security policy/procedures? (select as many as are relevant from the list provided)

- Data
- Data storage systems/facilities
- Hardware
- Software/applications
- Operating systems
- Sensors and detectors
- Physical infrastructure
- Networking and communication components
- Human-machine interface devices
- Traffic management applications
- Trackside equipment
- On-board equipment
- Payment systems
- Identity management and authentication systems
- Cloud-based services and platforms
- Others (please specify what these "other" critical assets are)
- Don't know

19. From a societal perspective, what are the critical assets that need to be protected? (please specify up to 10 assets)

20. What are the key threats to cyber security within Intelligent Public Transport your organisation has experienced and/or identified? (Please indicate as many options as are relevant from the list provided)

- Distributed denial of service attacks (DDoS)
- Manipulation of hardware and software
- Manipulation/insertion of information
- Eavesdropping
- Traffic analysis
- Malware and viruses

- Data breaches
- Insider attacks
- Exploitation of software bugs
- Abuse of authorisations
- Generation and use of rogue certificates
- Abuse of information leakages
- Identity theft
- Natural disasters
- Accidental disclosure
- Configuration errors
- Hardware/software failure
- Distribution/disruption problems for electrical supply
- Vandalism/civil disorder
- Other (please specify)

Security measures

21. Does your organisation either allocate, or advise others to allocate, some of their IT budget to cyber security for Intelligent Public Transport

- Yes (What percentage of your organisation's IT budget is spent/recommended for cyber security? Less than 2%; 2-10%; 11-25%; Greater than 25%; Don't know)
- No
- Don't know

22. What would you regard as the main motivators driving cyber security expenditure in the Intelligent Public Transport context? (Please indicate as many options from the list provided as required to answer this question)

- Protecting non-physical assets (Please specify these assets)
- Improving efficiencies/reducing-costs
- Enabling business opportunities
- Protecting intellectual property
- Business continuity in a disaster situation
- Protecting customer information
- Preventing downtime and service outage
- Compliance with regulation/legal requirements
- Protecting an organisation's reputation
- Maintaining data integrity
- Protecting privacy/maintaining confidentiality
- Protecting physical infrastructure
- Other (Please specify)
- Don't know

23. List the key measures either your organisation has implemented, or recommends that others implement, in order to protect Intelligent Public Transport from cyberattacks. *This can include technical measures, processes and policies implements, organisational structures and roles, standards, and any other measures. For each measure listed please rate how effective you believe these measures to be (please list*

your measures and for each rate their effectiveness using the following scale: ineffective; low-effectiveness; high-effectiveness). List as many as appropriate.

24. Does your organisation engage in or regulate the exchange of information related to cyber security?

- Yes, through mandatory reporting regulation (Specify the legislation – or state if not known)
- Yes, on a voluntary basis
- No, but we plan on doing so
- No
- Don't know

25. How does your organisation go about measuring or benchmarking the effectiveness of cyber security measures? (Please select as many responses as are relevant from the list provided)

- By measuring trends in security incident costs
- By benchmarking against other organisations
- By conducting a return-on-investment calculation
- By measuring staff awareness
- By relying on certification
- By conducting risk analyses
- By monitoring levels of regulatory compliance
- Through feedback from management
- Through other formalised processes (Please specify)
- Through the mandatory or voluntary collection of incident data
- By relying on the advice of third-parties such as law enforcement agencies, CSIRTs, etc.
- Through stakeholder feedback
- We don't formally evaluate/benchmark the effectiveness of our cyber security measures
- We do not employ any cyber security measures
- Don't know

26. How has your organisation responded to, or recommended how others should respond to, previous cyberattacks on Intelligent Public Transport (*please select as many responses as are relevant from the list provided*)

- Through additional staff training
- Through additional vetting of staff/contractors
- By changing the nature of business carried out
- By making changes to policies and procedures
- Through the deployment of new technologies
- By taking disciplinary actions
- By undertaking a formalised incident review

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greec

TP-02-15-956-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-146-5
doi:10.2824/778225