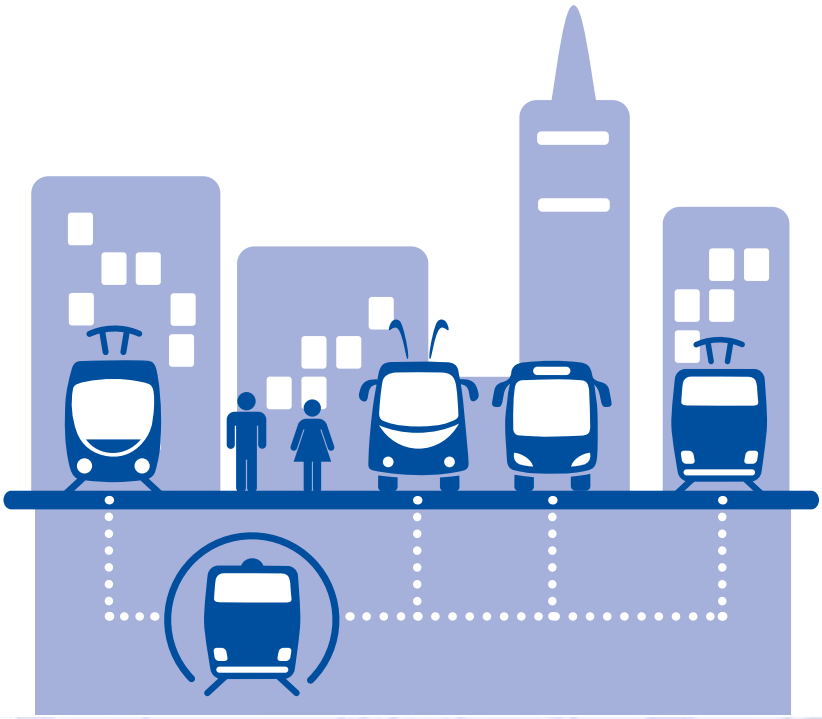


Cyber security for Smart Cities

An architecture model for public transport

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, 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 member states 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 member states 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 (ENISA), 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. Daniel BACHLECHNER (Fraunhofer ISI)
Dr. Michael FRIEDEWALD (Fraunhofer ISI)
Dr. Timothy MITCHENER-NISSEN (Trilateral Research)
Dr. Monica LAGAZIO (Trilateral Research)
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: 978-92-9204-162-5 | doi:10.2824/846575

Contents

Executive Summary

Cyber security in the context of Smart Cities is a hot topic. The objective of Smart Cities is to optimize the city in a dynamic way in order to offer a better quality of life to the citizens through the application of information and communication technology (ICT). The range of areas where cities can become smarter is extensive: it is an evolution of "Connected Cities" with the prevalence of data exchange at a larger scale.

Intelligent public transport (IPT) systems are a key element in Smart Cities. An Intelligent Public Transport operator manages the local public transport by applying ICT to improve the levels of service and efficiency of the transport system. IPT operators also exchange data with other operators in order to provide a better integrated service.

The increase of data exchange controls multiple services and assets leads to a higher degree of automation in the city. As several critical services become interconnected, the need for cyber security surges to protect data exchanges, privacy as well as the health and safety of citizens. However, there is currently no harmonised guideline or standard to model these data exchanges. This leads IPT operators, municipalities, policy makers as well as manufacturers, solution providers and vendors to adopt specific solutions with low scalability and disparate requirements.

Currently, it is not very common for IPT operators to have a cyber security policy in place or to use institutionalised and codified definitions for critical assets. Moreover, knowledge of, and spending for, cyber security in the IPT context appears to be rather low. Nevertheless, several cyber security measures are being implemented by IPT operators. However, measures are very diverse as there are neither widely accepted cyber security standards that aligned with the needs of IPT, nor widely used good practices.

To provide a foundation for the development of cyber security guidelines, this document defines a high level architecture model to understand the key areas to protect from cyber threats. Knowing that cities have different maturity levels, the architecture model focuses on the interactions in Smart Cities from the perspective of IPT operators. It integrates the functional processes and data exchanges between stakeholders.

The specific threats associated with data exchange between IPT operators and other stakeholders, and their potential consequences differ depending on the maturity of the city. Threats appear to be multifaceted and directed against information/data, applications and technology but also organisational structure and the entire infrastructures relevant for IPT. All specific threats discussed in this document are distinguished between threats from intentional attacks and threats from accidents.

The study proposes good cyber security practices for IPT operators to protect against intentional attacks and accidental threats. The study then proposes key recommendations for stakeholders in order to enhance the level of cyber security in Smart Cities:

- Municipalities should support the development of a harmonised cyber security framework
- The European Commission and Member States should foster knowledge exchange and collaboration in cyber security among industry, Member States and municipalities
- IPT Operators should develop a clear definition of their security requirements
- IPT Operators and Municipalities should allocate higher spending on cyber security
- Manufacturers and solution vendors should integrate security in their products

- IPT Operators and Municipalities should define the responsibilities of senior management in cyber security
- The European Commission and Member States should clarify the responsibilities of every actor
- Smart Cities and standard organisations should integrate cyber security in the maturity level of Smart Cities

1. Introduction

This study looks at intelligent public transport (IPT) in Connected Cities (CCs) and Smart Cities (SCs) from a cyber security perspective. CCs and SCs are cities that use information and communication technology (ICT) to meet public needs and to foster their development in a multi-stakeholder environment. CCs are characterised by independent operators that manage one or multiple systems from their own control centre with limited interactions among each other.

SCs extend CCs with data integration and task automation managed by a global decision process. The objective of SCs is to optimize the city in a dynamic fashion in order to offer a better quality of life to the citizens. The range of areas where cities can apply ICT in an attempt to become *smarter* is extensive and includes apart from, for instance, financial management and the management of public safety or energy also the management of public transport. IPT systems apply ICT to improve the levels of service and efficiency in the area of public transport.

Cyber security is concerned with the security of data, and the applications and infrastructure used to store, process and transmit them. It is understood as the process of protecting data and information by preventing, detecting and responding to cyber security events.[1] Such events, which include intentional attacks and accidents, are changes that may have an impact on organizational operations.

1.1 Scope of the study

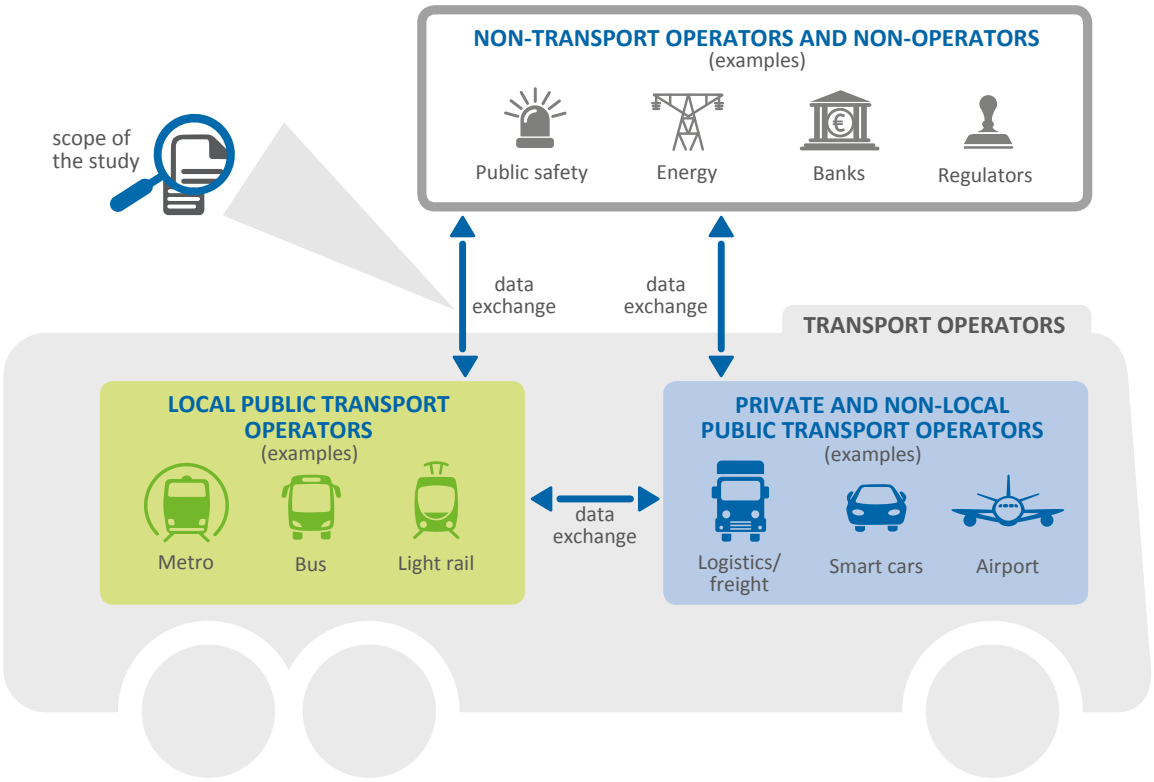
The main objective of this study is to model the architecture of the transport sector in SCs and to describe good cyber security practices of IPT operators. The good practices are put into a relationship with different city maturity levels. This allows representatives of operators and municipalities to quickly assess whether or not they lag behind other cities with the same maturity level in terms of cyber security and, if so, to take appropriate actions. The study is primarily focused on the provision of practical, hands-on guidance.

The scope of the study is illustrated in Figure 1. With respect to cyber security, there is a clear focus on data exchange. Therefore, particular emphasis is put on actors – including IPT operators but also, for instance, banks, safety authorities and energy providers, and other stakeholders with which IPT operators exchange data – and the interactions between them. Both causes and impacts of possible cyber security incidents are looked at as well as control and recovery measures. Particular attention is paid to good practices.

With respect to IPT, the focus of the study is on operators providing local services within a greater city area. Among the IPT operators, particular attention is paid to ones that provide, for instance, metro, bus, tramway/trolley bus or light rail services; smart cars, for instance, are not taken specifically into account. However, it is likely that the architecture model as well as the good cyber security practices presented in this study can be extended to support such cases without great effort.

[1] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cyber security"

Figure 1 Scope of the study



1.2 Target audience

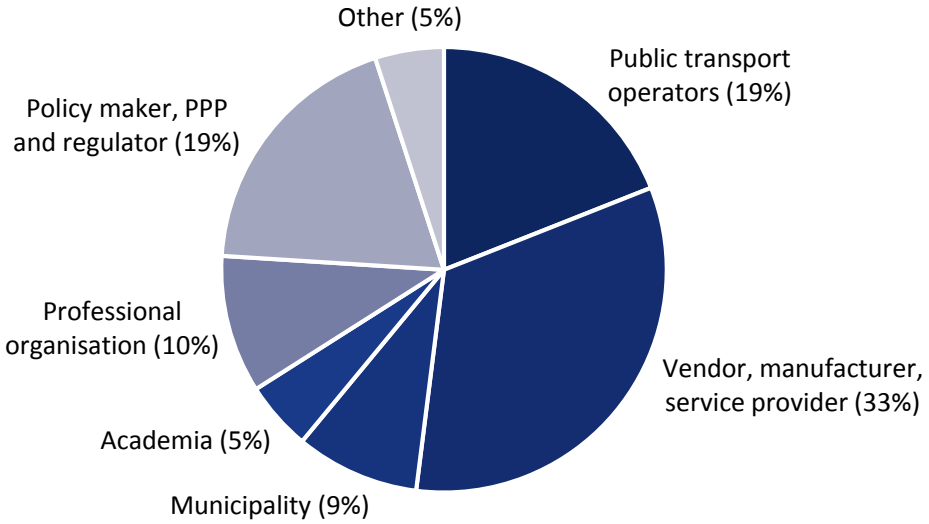
The target audience of the study consists of operators in the area of public transport, municipalities, policy makers as well as manufacturers, solution providers and vendors that supply transport operators.

- **Public transport operators**: This study provides public transport operators with a framework that allows them to better understand cyber security incidents they may face as well as guidance on how to take adequate control and recovery measures.
- **Municipalities:** This study provides municipalities with an overview of common interactions in terms of data exchange between public transport operators and other stakeholders. It allows for the assessment of the local cyber security status against an international benchmark taking different city maturity levels into account.
- **Policy makers:** The overview of common interactions in terms of data exchange between public transport operators and other stakeholders, can also be useful for policy makers. It allows them to gain a clearer understanding of how national and EU policy affects cyber security practices of public transport operators.
- **Cyber security industry:** This study provides manufacturers, solution providers and vendors that supply transport operators with respect to cyber security with a framework that allows them to better exchange views and cooperate with their clients. This includes in particular the exchange of information on possible cyber security incidents. This may allow optimising products and services as well as solutions to better address client needs.

1.3 Methodology

This study is based on desktop research as well as on empirical research. Within the scope of the desktop research, scientific as well as industry and policy material related to IPT was reviewed. A total number of 22 persons participated in the empirical research. Among the participants in an online survey and a series of interviews were, for instance, representatives from municipalities, public transport operators and manufacturers, solutions providers and vendors that supply transport operators as well as policymakers and regulators. Figure 2 shows the distribution of the respondents based upon the sector in which they are employed.

Figure 2 Distribution of respondents based upon the sector in which they are employed



Based upon their geographical location, the respondents were distributed across twelve EU Member States (MSs), namely, Belgium, Denmark, Estonia, France, Germany, Ireland, Latvia, Luxembourg, the Netherlands, Spain, Sweden and the United Kingdom.

1.4 Outline

The study is structured as follows:

- Section 2 describes the SC environment with a clear focus on IPT and cyber security. It pays attention to operators – including but not limited to IPT operators – and other stakeholders as well as interactions in the form of data exchange between public transport operators and other stakeholders.
- Section 3 presents an architecture model of the transport sector in SCs. The architecture addresses the interactions between SC stakeholders, describes data exchange from the perspective of IPT operators and explains how the architecture of the transport sector differs depending on the cities' level of maturity.
- Section 4 builds upon the architecture and adds layers focusing on cyber security. Causes and impacts of incidents as well as incidents themselves are addressed.
- Section 5 also builds upon the architecture but places control and recovery measures at the focus of attention. In essence, cyber security good practices of public transport operators are described.
- Section 6 summarizes the key findings from the empirical research.
- Section 7 proposes recommendations to enhance the level of cyber security in Smart Cities.

2. The Smart City environment

No single definition dominates the SC literature. A multitude of competing definitions have been developed over the last years whose focuses vary considerably.[2] An examination of definitions from policy makers, manufacturers, solution providers, vendors, user groups and standards organisations revealed that individual definitions can be broken down into two general elements:

- **Basic processes** that characterise SCs, such as the extensive use of ICT in general or the application of big data analytics in particular to meet public needs.
- **Specific focus areas** attached to (enabled by) these processes, such as improving mobility or resilience, or addressing environmental challenges

While virtually all definitions integrate the first element, the second element is not always included. In particular, cyber security is typically not prioritized within SC definitions with the exception of definitions provided by vendors and manufacturers whose market activities extend into this realm.

There is no legislation providing a definition of a SC on which a discussion could be anchored. Definitions by municipalities are rather statements of intent or aspiration for driving future activities within that city than an attempt to provide a genuine definition with wider applicability. Usually, there are few restrictions on the formation of definitions beyond the central tenet that a SC is a city that uses ICT to meet public needs and to foster development in a multi-stakeholder environment.

In literature, there is no clear distinction between SCs and CCs; the two terms seem to be used interchangeably. However, the majority of authors tend to prefer the term SC; some even refer to smart, connected cities.[3] In this study, SCs are understood as cities that go beyond or extend CCs in the sense that data integration and task automation is managed by a global decision process. The differentiation is explained in more detail in Section 3.1 where a maturity model for cities that use ICT is introduced.

Intelligent transport is primarily discussed in the context of intelligent transport systems (ITSs) reflecting the interconnected nature of its application. While differences exist between the definitions of ITS, they are much less pronounced than those between the definitions of SCs. This may reflect both the technical nature of ITSs which acts to anchor any subsequent definition as well as the presence of a definition for ITSs within Directive 2010/40/EU. By comparing and combining the definitions available, a concise definition for ITSs could be extracted. Essentially, an ITS is understood as the application of ICT to transport so as to improve levels of service and efficiency. ITSs are discussed in the context of all types of transport including, for instance, private transport, or national and international public transport. This report focuses on ITSs in the context of local public transport.

Definitions of cyber security generally focus on the protection of computer systems and information within cyberspace as well as on the management of their recovery upon incidents but they vary considerably in the level of detail in which

- the elements to be protected,
- the measures used to provide this protection, and

[2] M. Cavada, D. Hunt, C. Rogers, "Smart Cities: Contradicting Definitions and Unclear Measures"
[3] S. Crawford, "Governing the Smart, Connected City", https://hbr.org/2014/10/governing-the-smart-connected-city/

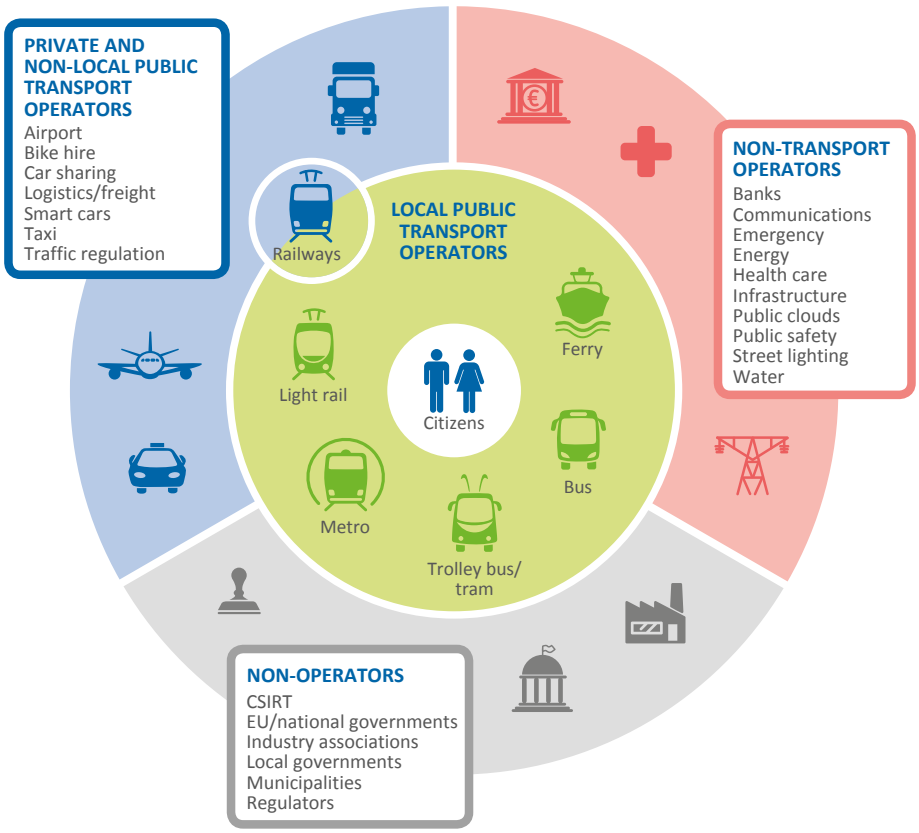
- the nature of the threats

have been expanded. Cyber security in SCs has been defined, for instance, as the protection of data, systems and infrastructure vital to the city's operation and to the stability and the livelihood of its people.[4]

2.1 Stakeholders

This study makes a distinction between different groups of SC stakeholders relevant in the context of IPT. Among them are operators of SC infrastructure and services as well as non-operators. Representatives from the groups of stakeholders are referenced in the architecture model of the transport sector introduced in Section 3. Figure 3 provides an overview of the relevant SC stakeholders.

Figure 3 Overview of SC stakeholders



Local public transport operators (coloured green) that provide public passenger transport services within the greater area of a city (*e.g.* operators providing taxi services, bus services, tram/trolley bus services, metro services, light rail services, local railway services) are distinguished from public transport operators that focus on national or international services (*e.g.* operators of non-local railway services, air services) and transport operators that provide services for private passenger (*e.g.* bike hire or car sharing operators) or freight transport (coloured blue). In addition to transport operators, numerous non-transport operators, which are nonetheless relevant in the context of IPT, operate in SCs (coloured red). Whereas some of them are clearly transport related (*e.g.* operators of street lighting, energy providers, infrastructure providers),

[4] Microsoft, "Developing a City Strategy for Cyber security", October 2014.

the relationship is not so pronounced for others (*e.g.* banks, water and waste utilities, health care providers).

All SC operators increasingly face cyber security issues.[5] A key issue is that a dense web of interconnected sensors, a diverse range of resource-constrained devices and the constant flow of data between them bring the peril of having countless points of entry for attackers seeking to compromise systems. Concurrently, the data that is stored and exchanged by SC operators and access to their systems become increasingly valuable for attackers – due to the increasing dependency on the data and systems, the risk of blackmail grows. Many SCs, for instance, rely on cloud services to store the large amounts of data collected from many geographically disparate sources. If a city fails to ensure that its cloud environment adheres to adequate security standards, it could suffer a data breach that compromises large amounts of sensitive information.[6] The combination of cloud services with existing on-premise infrastructure makes it particularly difficult to maintain a clear overview of all parts of the system. Another related issue is that attacks in SCs may have physical consequences.[7] For instance, the manipulation of traffic data relied on by traffic lights could lead to serious accidents.[8]

In addition to operators, there are several non-operators (coloured grey) in the context of SCs that are relevant for IPT (*e.g.* municipalities, governments, regulators). Particularly relevant in the context of cyber security are Computer Security Incident Response Teams (CSIRTs). Last but not least, citizens (coloured white), no matter if they are passengers or not, are key stakeholders for IPT in particular and SCs in general. They are the primary addressees of all efforts. They are the reason why cities increasingly apply ICT in an attempt to become smarter. Citizens are the actors with whom IPT operators interact most, irrespective of the cities' maturity level.

2.2 Interactions in the form of data exchange

SCs are characterized by a dense web of interconnected field components. Among the field components which are managed by operators are sensors and devices. There is a constant flow of data between field components as well as between field components and the data centres, where the data are processed. In addition to that, IPT operators exchange data with other SC stakeholders. The focus of this study is on interactions in the form of data exchange between SC actors.

2.2.1 Characteristics of the interactions

Collaboration in SCs appears to be common across sectors, between multiple SCs, and even across national borders. The implementation and operation of collaborative applications/systems between IPT and other operators or other SC stakeholders is still unusual, though. The few existing collaborative applications/systems that exist tend to happen between IPT operators, and between IPT operators and citizens. Data exchange with SC stakeholders other than transport operators or citizens tends to be, if it happens at all, more restricted and less coordinated. Overall, data exchange does, by and large, not yet seem to happen on a broad, regular and consistent basis.

---

[5] NIST, "Designed-in Cyber security for Smart Cities: A Discussion of Unifying Architectures, Standards, Lessons and R&D Strategies". http://www.nist.gov/cps/cybersec_smartcities.cfm

[6] ENISA, "Critical Cloud Computing", https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/critical-cloud-computing/at_download/fullReport

[7] C. Cerrudo, "An Emerging US (and World) Threat: Cities Wide Open to Cyber Attacks", White Paper, http://www.ioactive.com/pdfs/IOActive_HackingCitiesPaper_CesarCerrudo.pdf

[8] B. Ghena et al. "Green Lights Forever: Analyzing the Security of Traffic Infrastructure", 8th USENIX Workshop on Offensive Technologies, 2014, https://www.usenix.org/system/files/conference/woot14/woot14-ghena.pdf

Currently, ticket-related and passenger information services (*e.g.* online routes and time schedules, and real time traffic information including location data from GPS systems) are the primary reasons why data is exchanged between actors. The data exchanged between IPT operators, and between IPT operators and citizens varies depending on the context and the maturity of the respective city.

In more mature cities, traffic regulation operators may manage traffic lights and other important functions. Data is then exchanged between all relevant IPT operators and the operator coordinating the traffic. Moreover, IPT operators may provide emergency response agencies and public safety authorities (*e.g.* the police) with emergency and monitoring data, respectively. Energy consumption data may be shared with energy providers, infrastructure condition data with infrastructure operators and cyber security incident data with Computer Security Incident Response Teams (CSIRTs). In return, CSIRTs may provide IPT operators with data on threats. With lower probability, IPT operators may also exchange data with communication service providers, banks, municipalities, national governments, transport industry associations (*e.g.* the UITP) and regulatory bodies.

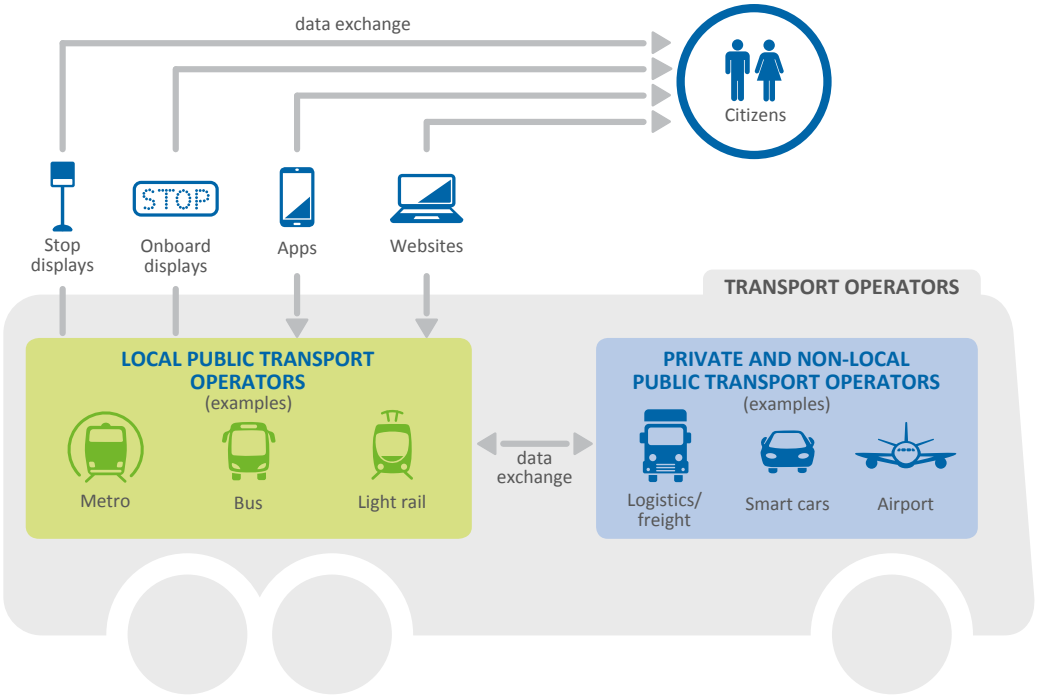
2.2.2 Types of the interactions

From a technical point of view, there are two types of interactions in the IPT context, those between IPT operators and citizens, and those between IPT operators and other stakeholders:

- **With respect to citizens**, there is no direct exchange of data between integrated systems of both the IPT operator and the citizens but data exchange is mediated by websites, apps, stop displays or on-board displays.
- **With respect to other stakeholders**, there may be a direct exchange of data between the respective control centres' systems.

Figure 4 illustrates the difference between the interactions. It shows a SC example were several local public transport operators exchange data with citizens and other stakeholders in an integrated and coordinated from. In CCs, it is more likely than in SCs that individual transport operators communicate with citizens and other stakeholders independently of one another.

Figure 4 A technical view on interactions of IPT operators



The actual transfer of data in a SC environment usually occurs via Machine to Machine (M2M) technologies that allow devices that are connected both through wired and wireless networks to communicate with each other.

Web services are typically used in SCs to realise M2M interaction. The principle of web services is quite simple. A software function provided at a network address is triggered remotely using the Internet and the result is returned to the caller. They typically use HTTP and XML in addition to other Web-related standards. Web services are not only relevant for data exchange between the operation control centres of IPT operators and the control centres of other operators but also for the operation of station and on-board display.

An example for a protocol based on XML to allow distributed servers to exchange real-time information about public transport services and vehicles via web services is the Service Interface for Real Time Information (SIRI).[9] SIRI is based on the TransModel[10] terminology and modelling concepts for public transport information, and used in a number of sites globally. In Europe, for instance, SIRI is used by Transport for London. SIRI has been developed as an evolution and a harmonisation of national standards.

For public transportation schedules, the General Transit Feed Specification (GTFS),[11] is often used as a common format. GTFS feeds allow IPT operators to publish data about their services and developers to

[9] CEN TC 278 Working Group 3 Sub Group, SIRI – Management Overview, http://user47094.vs.easily.co.uk/siri//schema/1.0/doc/Siri%20White%20paper08.zip
[10] CEN, Reference Data Model For Public Transport (EN12896)
[11] General Transit Feed Specification (GTFS), https://developers.google.com/transit/gtfs/

write applications that consume that data. Feeds are typically hosted on the operators' websites. Websites such as GTFS Data Exchange[12] are used to inform developers about new and updated feeds.[13]

Another, more generic standard used is the Constrained Application Protocol (CoAP), which is a software protocol intended to be used in very simple electronics devices such as sensors. The standardisation work with respect to CoAP was mostly done by the Internet Engineering Task Force (IETF). As such devices play a minor role in the context of data exchange between IPT operators and other stakeholder, CoAP is not particularly relevant for this study. The same applies to technologies and standards such as IPv6 over Low power Wireless Personal Area Networks (6LoWPAN), IEEE 802.15.4, HC-06 Bluetooth modules and the Minimum Rank Objective Function with Hysteresis (MRHOF) that are relevant in the context of low-power devices with limited processing capabilities only. Interactions between IPT operators and other stakeholders are usually based on web services and the underlying Internet architecture.

Relevant telecommunications standard development organisations are united on a global scale by the 3rd Generation Partnership Project[14] (3GPP), while the 5G Infrastructure Public Private Partnership[15] (5G PPP) is a joint initiative between the European ICT industry and the European Commission focusing on future communication networks and services.

[12] GTFS Data Exchange, http://www.gtfs-data-exchange.com/
[13] GTFS Data Exchange provided feeds from 962 transport operators all over the world as of 22nd September 2015.
[14] 3GPP, http://www.3gpp.org/
[15] 5GPPP, https://5g-ppp.eu/

3. Architecture of the transport sector in Smart Cities

The architecture of the transport sector in SCs is described from the perspective of stakeholder interactions. To this end, two models are defined:

- a **stakeholder interaction model** focusing on stakeholders (*e.g.* energy operator), functional processes (*e.g.* energy management) and data exchange between stakeholders (*e.g.* exchange of energy consumption data) and
- an **interaction layer model** focusing on the elements that are needed by stakeholders to interact from a business (*e.g.* traffic coordination business), an information/data (passenger information), an application (*e.g.* GTFS), a technology (*e.g.* IEEE 802.15.4) and a physical link viewpoint (*e.g.* radio).

The stakeholder interaction model and the interaction layer model provide the basis for the discussion of causes and impacts of cyber security incidents as well as relevant countermeasures in Section 4 and Section 5, respectively. Illustrations, inspired by data flow diagrams and enterprise architecture descriptions, respectively, are used to make the model easily understandable.

3.1 Maturing from Connected Cities to Smart Cities

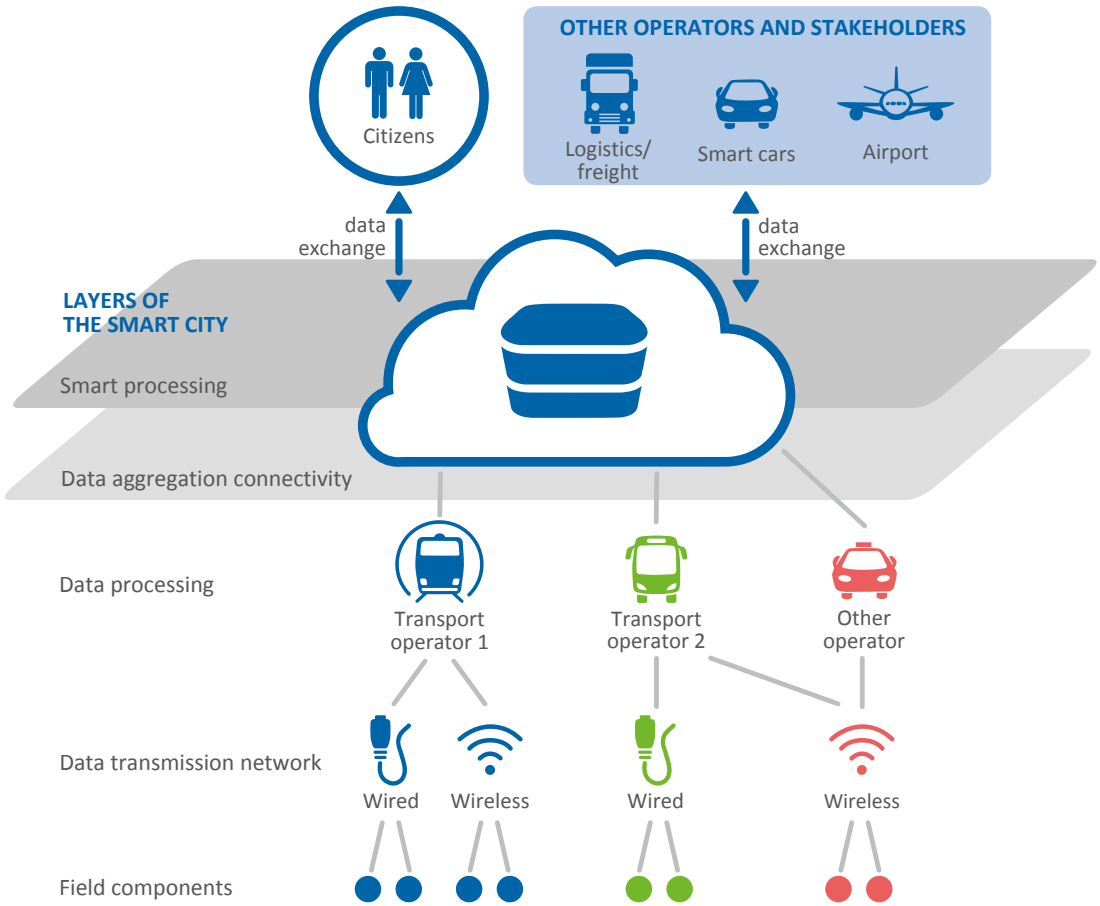
The transport sector differs depending on the maturity of a city. This needs to be taken into account when describing the architecture of the transport sector in smart cities.

To measure the development of SCs, various methods of grading have emerged. These include the development of ranking systems,[16] the holding of annual competitions to reward excellence[17] and the creation of different SC maturity scales that categorise SCs based on their perceived level of development. Together, these methods assist in the identification of frontrunners whose programmes can be adopted by other cities as examples of good practices.

The architecture of the transport sector in cities differs depending on the level of maturity. Figure 5 shows a simplified view of the ICT architecture of SCs.

[16] *e.g.* the European Smart Cities initiative (see http://smart-cities.eu/) and the Annual Smart City Index (see http://www.smart-circle.org/)
[17] *e.g.* the Annual Civitas Awards, and the Intelligent Community Forum's Intelligent Community of the Year.

Figure 5 Simplified view of the ICT architecture of SCs

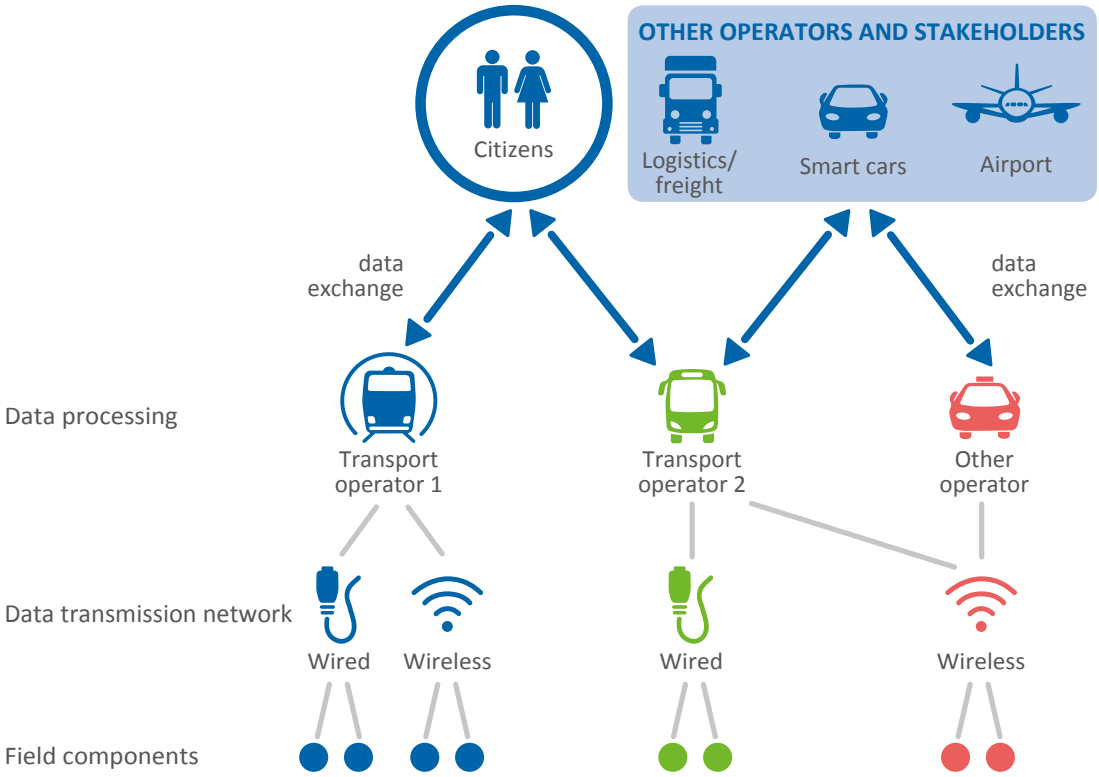


The first three layers describe the ICT architecture in a CC where independent operators – not necessarily IPT operators – manage their systems with limited interactions among each other. Field components are sensors and actuators that interact with the real world. The data transmission network transmits data between field components and the data processing component. Within the scope of data processing, data from field components is integrated in order to allow visualizing the state of the systems.

The SC extends the CC through the aggregation of data and the performance of global decisions – two additional layers became necessary to describe the ICT architecture of the SC. The data aggregation connectivity enables data exchange between operators and the smart processing component. Within the scope of smart processing, data from several sources is aggregated and correlated to lay the foundation for making global decisions.

Data exchange with citizens and other stakeholders may not only happen in SCs but also in CCs but in such cases data from different actors will not be integrated and coordinated. Figure 6 shows a simplified view of the ICT architecture of CCs.

Figure 6 Simplified view of the ICT architecture of CCs



This study distinguishes two levels of maturity:

- **Connected Cities**, in which ICT is used to connect field components via data transmission networks with data centres where the data processing happens taking into account mostly the data of the individual operator
- **Smart Cities**, which are characterised by data aggregation connectivity allowing smart processing of data taking into account data of several related operators and stakeholders

3.2 Stakeholder interaction model

The data exchanged between IPT operators and other stakeholders varies depending on the context and the maturity of a city. It is expected that collaborative applications/systems between IPT operators and other stakeholders will be more common in the future than they are today. This section put the operators and interactions introduced in section 2 into relation.

3.2.1 Interactions in Connected Cities

In CCs, data exchange relevant in the context of IPT is happening mainly among IPT operators and other IPT operators as well as between IPT operators and citizens. There are several other stakeholders with whom IPT operators may collaborate but there have typically not been implemented collaborative applications/systems. Interactions are, if they happen at all, restricted and rather uncoordinated.

Figure 7 IPT-related interactions between operators and stakeholders in CCs

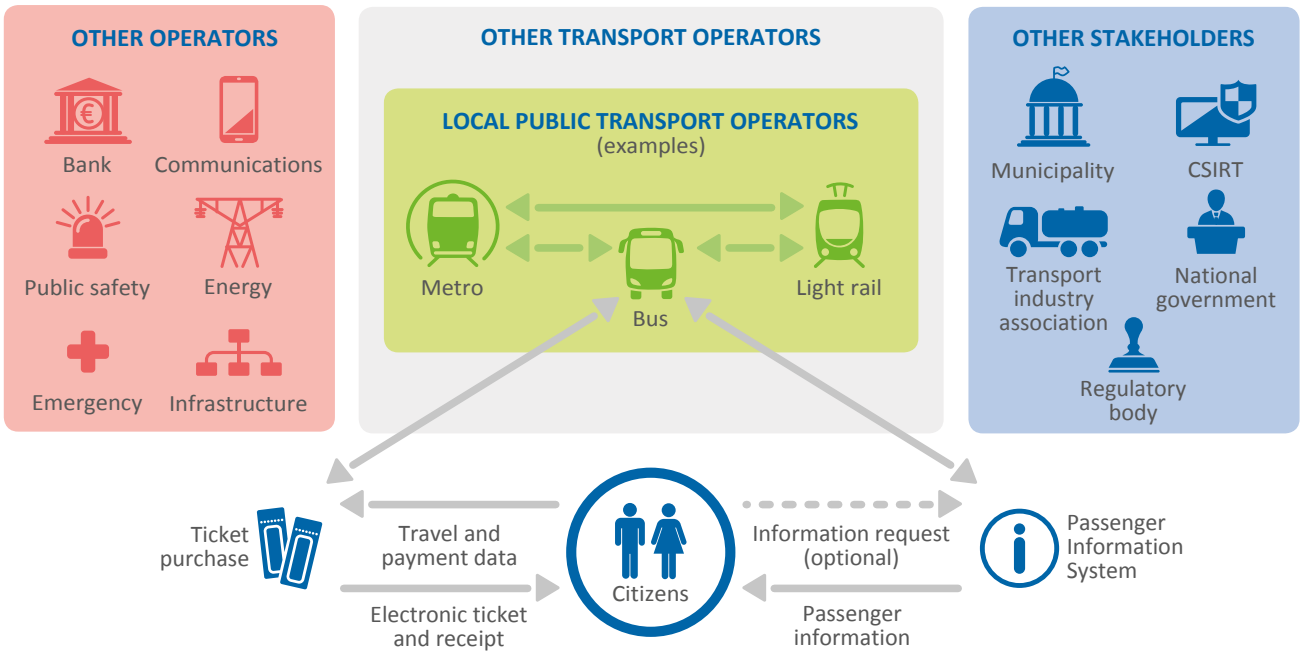


Figure 7 shows an example of how IPT-related interactions in terms of data exchange between stakeholders in CCs may look like. The data exchange between IPT operators and citizens focuses on passenger information and ticket purchase services:

- **Passenger information services** make relevant information (*e.g.* online routes, timetables, real-time traffic information) available to the general public (*e.g.* through stop or on-board displays) or provide specific pieces of information upon request (*e.g.* through a website or an app).
- **Ticket purchase services** receive travel and payment data via the IPT operator's website or a specific app, process the payment, issue the electronic ticket and make the ticket as well as a receipt available to the customer.

Integrity, authenticity, confidentiality and availability are important security requirements in the context of both passenger information and ticket purchase services. Non-repudiation and confidentiality are particularly important in the context of ticket purchase services. Whenever tickets are sold by IPT operators to passengers, it must be ensured that the fare has been paid, especially in the case of smart cards and smartphone applications. Moreover, payment data must be kept confidential at all times. With respect to passenger information services, which concern routes and time schedules as well as real-time traffic data, integrity and authenticity are the key requirements. It needs to be clear who provided the data as well as that it has not been manipulated. Availability is important too but IPT operators won't suffer substantial disadvantages if ticket purchase or passenger information services are temporarily unavailable. Loss of profit should be limited due to fallback options for purchasing tickets and receiving passenger information, and a lack of competing transport offerings.

Apart from communication service providers, banks, energy providers, infrastructure operators, emergency response agencies and safety authorities are regarded as operators relevant for IPT operators to integrate with. With respect to other stakeholders, it may be reasonable for IPT operators to integrate with CSIRTs, the relevant municipality and national government, transport industry associations and regulatory bodies to coordinated transport-related issues.

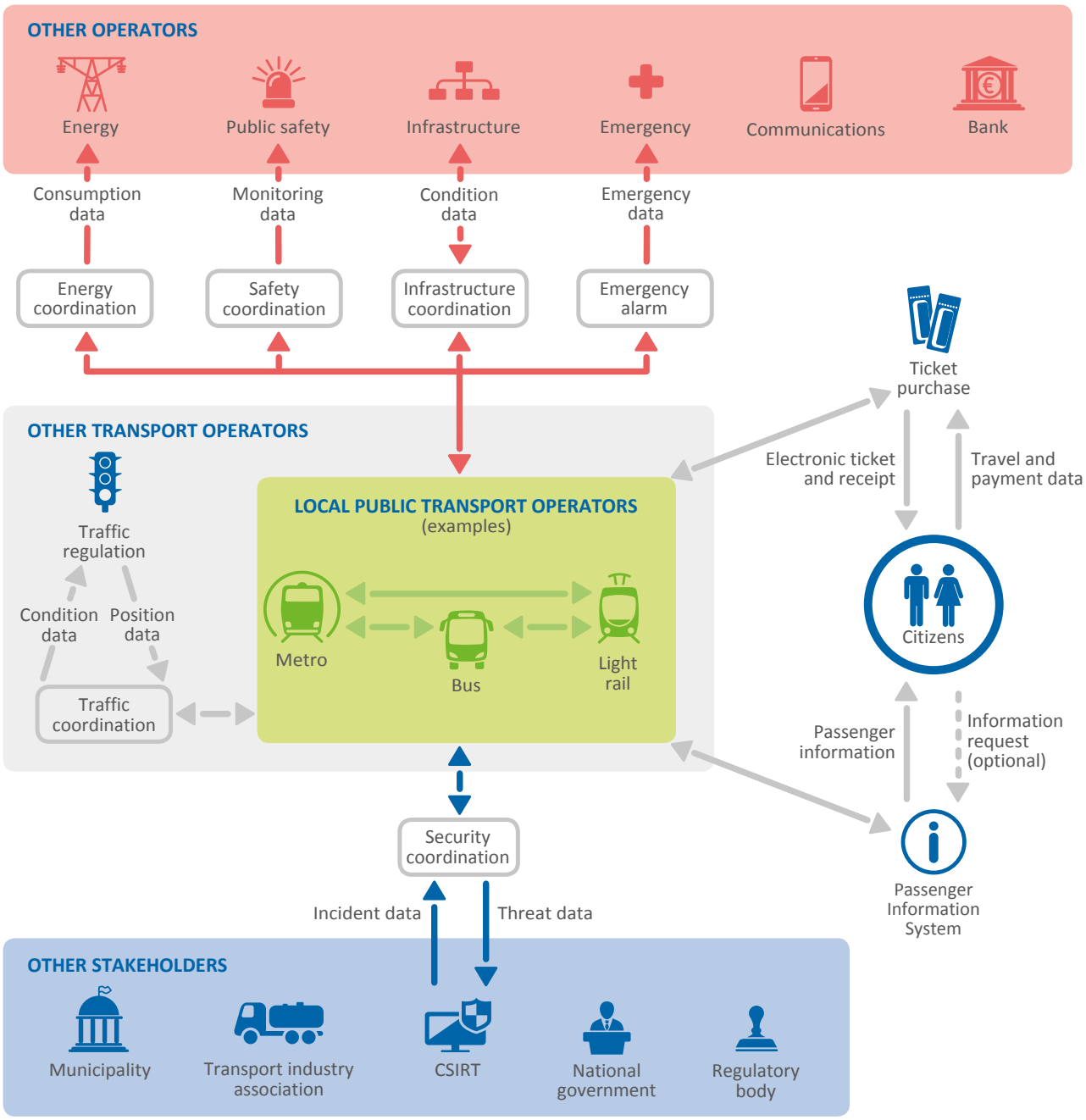
3.2.2 Interactions in Smart Cities

In terms of data exchange, SCs go beyond CCs. Passenger information and ticket purchase service may be more comprehensive as they, for instance, also take into account connections provided by multiple IPT operators in terms of both the issuing of tickets and the information of passengers.

Figure 8 shows an example of how IPT-related interactions in terms of data exchange between operators and stakeholders in SCs may look like. IPT operators in SCs may individually or jointly not only take coordinative actions regarding energy, infrastructure, safety, traffic and security but also provide information about emergencies:

- **Traffic coordination** including, for instance, the management of traffic lights or other important functions is made possible through the exchange of data (*e.g.* location data from on-board GPS systems, real-time traffic information) between IPT operators and a central traffic regulation operator.
- **Energy coordination**, which is relevant in case electrified transport services are provided, is based on the sharing of energy consumption data of IPT operators with energy providers allowing energy providers to manage the grid and resources intelligently.
- **Infrastructure coordination** requires the exchange of data about infrastructure conditions (*e.g.* road conditions) between IPT operators and infrastructure operators but allows the intelligent use of the infrastructure as well as the rapid removal of obstructions.
- **Emergency alarms** and their prompt forwarding by the IPT operator to the right place allow quick reactions through ambulance and similar services in case of emergencies.
- **Safety coordination**, which is relevant, for instance, in relation to criminal incidents, usually requires the sharing of monitoring data of IPT operators (*e.g.* surveillance video recordings) with public safety authorities such as the police.
- **Security coordination** means that IPT operators make data on concrete cyber security incident available to CSIRTs, expert groups that handle cyber security incidents, and receive data on threats they may face in return.

Figure 8 IPT-related interactions between operators and stakeholders in SCs



Generally, IPT operators do not seem to be willing to make information about cyber security public. However, they are open to collaborate and exchange information with CSIRTs and the police. What they expect, however, is proactive two-way information sharing.

With respect to the data exchanged between IPT operators and traffic regulation operators, integrity, authenticity and availability are particularly important. Non-repudiation and confidentiality are less important. It needs to be clear who provided the data as well as that the data has not been manipulated as this could lead to physical consequences in the form of accidents. Availability is in the context of coordination traffic, which includes managing traffic lights and other important functions, more relevant

than it is for ticket purchase and passenger information services but temporary service disruption should be manageable without major impact – possibly with cuts in levels of service and efficiency.

Table 1 describes the interactions between IPT operators and other stakeholders.

Table 1 Interactions and relevant security parameters

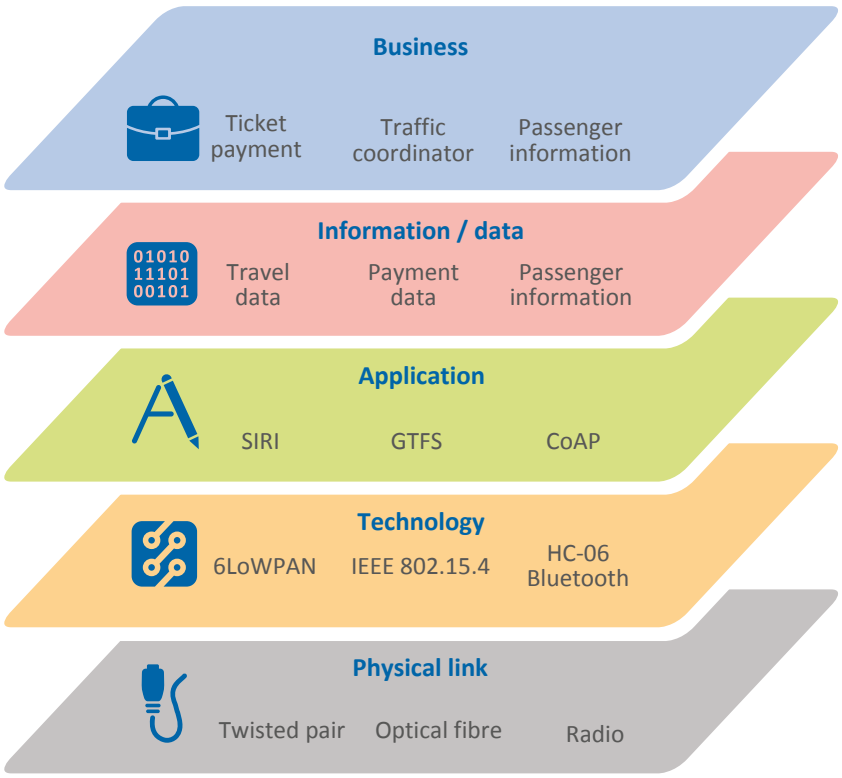
OTHER OPERATORS/STAKEHOLDERS	SECURITY PARAMETERS	DESCRIPTION
Citizen (passenger)	Integrity Authenticity Availability Non-repudiation Confidentiality	Integrity, authenticity and availability are important in the context of both passenger information and ticket purchase services. Non-repudiation and confidentiality are particularly important in the context of ticket purchase services. With respect to passenger information services, integrity and authenticity are the key requirements. Availability is important too.
Traffic regulation	Integrity Authenticity Availability	With respect to the data exchanged between IPT operators and traffic regulation operators, integrity, authenticity and availability are particularly important. Non-repudiation and confidentiality are less important.
Energy	Availability Integrity Authenticity Confidentiality	Information on energy consumption provided by IPT operators can be used by energy suppliers to actively reconfigure the grid in case of temporary and unexpected load conditions.
Infrastructure	Integrity Authenticity Availability	The data that may be exchanged with infrastructure providers, in case it mainly provides infrastructure condition information, appears to be relatively uncritical in terms of cyber security.
Emergency and public safety	Availability Integrity Authenticity	With respect to emergency alarms and safety coordination, availability is particularly important. Both emergency and monitoring data have to be shared without undue delay.
CSIRT	Confidentiality Integrity Authenticity	With respect to the data related to cyber security incidents and threats that may be shared with CSIRTs or the police, confidentiality, integrity and authenticity are of particular importance.

3.3 Interaction layer model

This section describes data exchange from the perspective of an IPT operator referring to the interactions introduced in section 2 into relation.

Figure 9 shows the layers that are considered and gives examples relevant in the context of IPT for each of the layers. This study looks on data exchange in SCs primarily from a business and an information/data perspective but application as well as technology aspects are also be taken into account to some extent.

Figure 9 Data exchange from the perspective of an IPT operator



The business layer describes the processes and activities that use information and data, and that rely on the exchange of data between actors. Processes and activities relevant in the context of IPT are ticket payment, passenger information, traffic coordination as well as energy coordination, infrastructure coordination, raising emergency alarms, safety coordination and security coordination. The business layer is relevant from a cyber security point of view as the processes and activities are what has to be protected and made reliable in the end.

The information/data layer deals with the information or the data that is stored, processed and transmitted using applications. Several types of data and information are relevant in the context of IPT. Among them are not only payment data, travel data and passenger information but also location data, traffic and infrastructure condition data, energy consumption data, emergency and monitoring data, and data on cyber security threats and incidents. The information/data layer is relevant from a cyber security perspective because looking at the data allows an initial assessment of the actual cyber security requirements and appropriate controls.

The application layer, in principle, addresses the applications that run on technology and are used to store, process and transmit information and data. This document does not focus on specific applications used by IPT operators but on protocols and standards relevant for applications. SIRI, GTFS and CoAP are examples for relevant protocol and standards.

The technology layer, in principle, describes the technologies the applications run upon. This document does not focus on the specifics of technologies. In SCs, most data exchange between IPT operators and other stakeholders is based on Internet technology, mostly realised by means of web services. Technologies such as 6LoWPAN, IEEE 802.15.4 and HC-06 Bluetooth are relevant in the IPT context but almost exclusively for data exchange between field components, and between field components and data centres of individual operators. Nevertheless, understanding application and technology aspects is essential for the detailed assessment of cyber security requirements and controls.

The physical link layer represents the actual data transmission medium connecting network nodes. Media may be wired (*e.g.* twisted pair, optical fibre) or wireless (radio). Aspects of the physical link layer are relevant from a cyber security point of view. There are no IPT specifics here though.

4. Threats in Smart Cities

To make reasonable decisions with respect to control and recovery measures, it is important to have a thorough understanding of causes and impacts of cyber security incidents. In this section, threats and their possible consequences are mapped to the architecture of the SC transport sector introduced in section 3.

4.1 Threat modelling

This study is based on an approach to threat modelling which combines a set of threat categories relevant in the context of ITS described by ETSI[18] with a simplified view of the ICT architecture of SCs that was developed after careful analysis of SC characteristics.

The threat categories taken into account are:

- **Availability threats**
- **Integrity threats**
- **Authenticity threats**
- **Confidentiality threats**
- **Non-repudiation/accountability threats**

Threats to the availability and continuous behaviour of an ITS include, for instance, Denial of Service (DoS) attacks. Integrity threats include unauthorized access to restricted information (*e.g.* through masquerade attacks or malware) as well as loss, manipulation and corruption of information. Authenticity is a major challenge in ITS as usually all system stations have the ability to send, receive and replay most types of messages. Threats to the confidentiality of information include, for instance, the illicit collection of data through eavesdropping or the analysis of message traffic. Non-repudiation/accountability is important to ensure that nobody can deny that particular messages were sent or received, or that specific services or data were modified.

The simplified view of the ICT architecture of SCs describes five layers (from bottom to top):

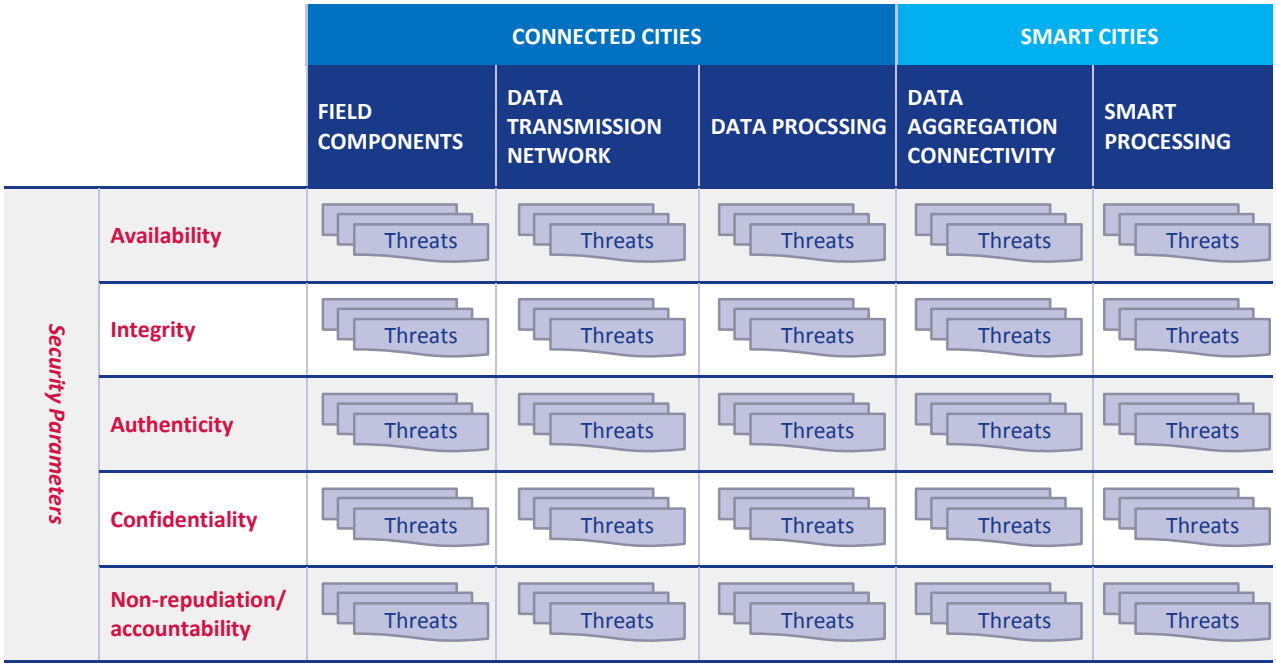
- **Field components**
- **Data transmission network**
- **Data processing**
- **Data aggregation connectivity**
- **Smart processing**

The architecture is in line with the one used within the scope of the introduction of the maturity model in Section 3.1.

The advantage of integrating the two approaches is that the result brings together established threat categories in the context of ITS with ICT architecture components of SCs. Moreover, the differentiation between CCs and SCs provides a simple option to distinguish different levels of maturity. Figure 10 shows a threat matrix based on threat categories as well as the ICT architecture layers.

[18] http://www.etsi.org/deliver/etsi_tr/102800_102899/102893/01.01.01_60/tr_102893v010101p.pdf (p. 38ff)

Figure 10 Threat matrix

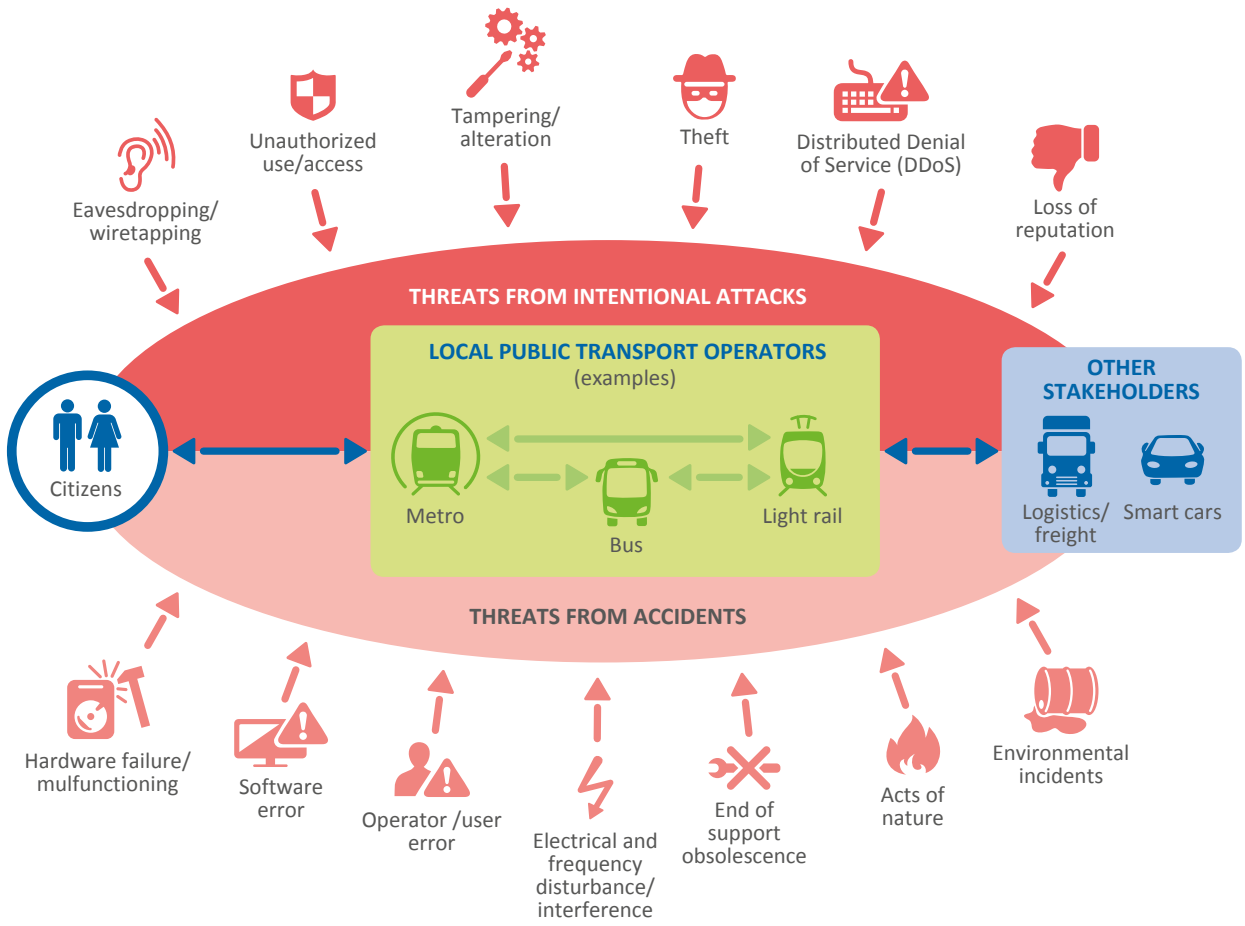


The layers are not independent and cyber security incidents on one specific ICT architecture layer may also affect other layers. As this study focuses on data exchange, the data transmission network and the data aggregation connectivity receive particular attention. Moreover, threats that may lead to incidents cannot necessarily be associated with exactly one threat category only. With respect to incidents, a differentiation is made whether they were caused intentionally or accidentally.

4.2 Specific threats

The specific threats associated with data exchange between IPT operators and other stakeholders, and their potential consequences differ depending on the maturity of the concerned city. Threats appear to be multifaceted and directed against information/data, applications and technology but also organisational structure and the entire infrastructures relevant for IPT. All specific threats discussed in this section are, in principle, relevant for both SCs and CCs, the effect of incidents, however, is often significantly larger in SCs as compared to the less interconnected CCs. Figure 11 provides an overview of the threat landscape in the context of IPT distinguishing between threats from intentional attacks and threats from accidents.

Figure 11 Threat landscape



4.2.1 Threats from intentional attacks

Incidents resulting from threats in this group are caused intentionally. The key threats from intentional attacks are eavesdropping/wiretapping, theft, tampering/alteration and unauthorized use/access.

Eavesdropping/wiretapping is a deliberate act of capturing network traffic and listening to communications between two or more parties without authorisation or consent. Eavesdropping/wiretapping may affect availability, integrity and confidentiality of data and information systems, respectively. Recent experience has shown that wireless and cellular networks are vulnerable to eavesdropping equipment based on standard components. They are the most obvious threats in the context of data exchange and may lead to follow-up attacks since they allow, for instance, tapping credentials or understanding details regarding the configuration of the network including how devices are connected. A network map is a critical piece of information to any attacker who is planning a thoughtful and deliberate attack on systems such as ITSs.[19] The better connected systems are, the more severe follow-up attacks may be. The degree of vulnerability to eavesdropping differs from one type of connection to another. Eavesdropping/wiretapping may lead to the intentional disclosure of proprietary, financial, personal or otherwise sensitive information.

[19] Edward Fox, "An Introduction to Cyber security Issues".

Theft refers to the unauthorised appropriation of information/data or technology. Theft may affect availability and confidentiality. The most common threat to the network connecting field devices in the IPT context remains copper theft. Copper theft is a reason why some operators have chosen to deploy wireless communication technologies, which introduce a different set of problems.[19] With respect to data exchange between IPT operators, and other stakeholders, other forms of theft are more relevant. If it is not properly secured data can be stolen by means of eavesdropping/wiretapping. Theft of cryptographic keys to decentralised ticketing systems, for instance, can cause serious financial and reputational loss. Apart from that, theft of mobile devices of operator employees such as laptops is increasingly happening, where both information/data and technology may be stolen. Stolen mobile devices may reveal credentials or information about the configuration of the network and thus are relevant in the context of data exchange. Theft of credentials or other sensitive information can also be the result of social engineering or shoulder surfing attacks. Theft may lead to follow-up attacks in the sense of unauthorised use/access or tampering. Theft of information/data may allow embarrassing and blackmailing IPT operators.

Tampering/alteration aims at altering information/data, applications or technology with direct and potentially significant effect on availability and integrity. It is also relevant from the perspective of non-repudiation/accountability. Tempering/alteration requires acquiring access to the target assets via several means (*e.g.* information leak, reply attacks, malware, black holes, take over).[20] In the IPT context field devices such as traffic signals, toll tag readers and cameras, for instance, are quite susceptible to tampering. However, besides tapering of technology also alteration of data and applications are on the rise. With respect to data exchange between IPT operators and other stakeholders, active eavesdropping (*e.g.* man-in-the-middle attacks) is particularly relevant, for instance. Any intentional modification, insertion, deletion of data by authorised or unauthorised users, including employees, which compromises the data, is considered data alteration. Alteration might also impact confidentiality and authenticity. For instance, reply attacks in the form of false messages can be sent to the network and deceive users and authorities to make them believe that another node was responsible for sending these messages. In the transport context, several tampering incidents became public recently were portable dynamic message signs (DMS) were used.[21] This shows that IPT operators have to take measures to protect on-board and stop displays. Alteration of websites, which happen relatively often, is certainly not transport-sector-specific but nevertheless something that has to be stopped. Due to the connection of websites with other systems, they have become an important gateway for more serious attacks. Again, the better connected systems are, the more severe such attacks may be. Tampering/alteration may allow embarrassing and blackmailing IPT operators as well as to hiding other nefarious behaviour (*e.g.* theft, illegal access).

Unauthorized use/access can be at the source of other threats. Apart from eavesdropping/wiretapping, theft and tampering/alteration, it may also be that information/data, applications or technology are used/accessed in an unauthorised way. This includes unauthorised connection to a network, data leaks, browsing files, acquiring private data, controlling field components and using resources for personal use. It is relevant in the context of data exchange between IPT operators and other stakeholders, as it may have a direct impact on availability of data, applications and technology.[22] Moreover, unauthorized use/access may affect integrity, confidentiality, authenticity and non-repudiation/accountability as attackers might have obtained comprehensive possibilities. Therefore, follow-up attacks may further affect data exchange.

[20] ETSI, *Intelligent Transport Systems (ITS).*
[21] See: Edward Fox, "An Introduction to Cyber security Issues"; US Department of Transportation, *Intelligent Transportation Systems (ITS).*
[22] See: US Department of Transportation, *Intelligent Transportation Systems (ITS).*

Additionally, unauthorized use/access may cross the borders of individual actors by misusing connections between actors.

Distributed Denial of Service (DDoS) consists in the usage of several sources connecting simultaneously to one destination, with the objective of overflowing the connection. A DDoS usually deprives a target from Internet connectivity; it can also be preliminary to other attacks. With the increase of IP-connected devices, DDoS are a main threat to IPT systems, in particular for devices and services relying on Internet connectivity. The IPT infrastructure is usually targeted by a DDoS but it can also unknowingly take part of a DDoS attack if certain systems are vulnerable.

Loss of Reputation lowers level of trust in the IPT service or in the operator. An intentional cyber attack can target an IPT operator for various reasons, which have an impact on the business. The visible consequences of this attack lead to the loss of reputation (*e.g.* data theft). The reputation of the organisation is perceived lower by citizens, partners, suppliers and municipalities. This threat is transversal as it applies to unprotected system and to personnel.

Further threats from intentional attacks with lower relevance in the context of data exchange are strikes, vandalism/civil disorder and terrorism. They may affect data exchange mostly through outages in electricity and other services and the motiveless or politically motivated destruction or defacement of property and infrastructure. These threats affect almost exclusively availability. Terrorism may go beyond untargeted destruction or defacement and target critical services such as public transport directly. It may even be that terrorisms chose ICT as their preferred attack vector. In this case, the threat may affect all security requirements as described above.

4.2.2 Threats from accidents

Incidents resulting from threats in this group are caused accidentally. The key threats from accidents with varying relevance for data exchange are hardware failure/malfunctioning, software error, operator/user error, end of support/obsolescence, Electrical and frequency disturbance/interruption and environmental incidents.

Hardware failure/malfunctioning can occur due to, for instance, old age, lack of maintenance and overheating. In the IPT context, field components, which are often deployed outside, as well as components critical for the exchange of data between IPT operators and other stakeholders may be affected. In many cases failure/malfunction results in services being unavailable. Failures in network components (*e.g.* router, switch, base station) are sufficient to cause interruptions in the telecommunications between field components and data centres, as well as IPT operators and other stakeholders. In some cases this will be a minor nuisance, for example, being unable to buy tickets or get real-time information at a stop, but in others could result in costly damage, for example, faulty traffic lights leading to significant delays. Impacts will depend on the failure states of the devices and how they are designed to deal with disruption of service, power supply or communication links. Recovery from failure can be complicated by the design of the system. For example, physically remote devices may have to be physically reset or rebooted. Exploiting failure states might also enable intentional attacks.

With respect to their effects, **software errors** are comparable with hardware failure/malfunctioning. Any extraneous or erroneous code in the operating system or an application that result in processing errors, data output errors or processing delays is considered a software error. Software errors mostly affect availability[23] but may also affect integrity. In the IPT context, unexpected system behaviour resulting from

[23] US Department of Transportation, *Intelligent Transportation Systems (ITS).*

software errors could, for instance, affect operations or profitability (*e.g.* a ticket may be delivered without payment). Furthermore, software errors may be exploited within the scope of intentional attacks. Serious vulnerabilities may originate from software errors. With respect to data exchange between IPT operators and other stakeholders, software errors in the components that deal with the actual transfer of data may be particularly threatening.

Operator/user error refers to "an improper or otherwise ill-chosen act by an employee that results in processing delays, equipment damage, or lost or modified data".[23] Operator errors often occur during maintenance when for instance hardware and software are modified and/or updated but also during operation. Configuration errors with respect to applications or software used for data exchange may lead, for instance, to unexpected behaviour of components, which in turn might cause loss of connectivity and slow down or halt of services, or to the creation of vulnerabilities. In case maintenance is outsourced, operators/users may not fully aware of all dependencies and operation requirements.

End of support/obsolescence may lead to serious vulnerabilities. Often, manufactures, solutions providers and vendors stop supporting applications and technology as they become obsolete. It is not uncommon though that obsolete applications and technology, sometimes pursuing a virtualisation strategy, is used together with new applications and technology. Both lack of support and lack of virtualisation know-how may lead to vulnerabilities. Data exchange between IPT operators and other stakeholders is affected in case support is stopped for applications and technology critical for data exchange. Availability and integrity may be directly at risk, other security requirements, if vulnerabilities are exploited for intentional attacks.

Electrical and frequency disturbance/interruption may affect availability. IPT systems require electricity with most field devises and data networking, storage and processing, requiring power. Functionality of these devices will be significantly degraded or stop entirely, with a loss of electricity. In this regard, data exchange between IPT operators and other stakeholders is affected in terms of availability. Furthermore field components and data transmission networks often rely on a Global Navigation Satellite System (GNSS) and cable and/or wireless communication to connect, which can be subject to frequency interference and/or cable cut or involuntary disconnection resulting in loss of connectivity, lower capacity and potentially inability to perform action and services. The SECRET project,[24] for instance, addressed the risks and consequences of electromagnetic attacks on the railway infrastructure. This, however, is less relevant with respect to the specific scope of this study. Similarly to hardware failure and malfunctioning the level of disruption is dependent upon the failure states of the devices and how they are designed to deal with disruption of service, power supply or communication links.

Acts of Nature (including bad weather) is due to unexpected events which impact the service. Such acts of nature include extreme drought or flood, snow, strong wind. Acts of nature usually impact systems which cease to operate. For example, they are one of the main reported cause of outage for telecommunication systems in Europe.[25]

[24] SECRET project, http://www.secret-project.eu
[25] See ENISA, "Article 13a – Annual Incident Report 2014", https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2014

Environmental incidents, such as major electrical failure and liquid leakage (*e.g.* burst or leaking pipes, discharge of sprinklers),[23] are similar to acts of nature and can cause destruction of field components, vehicles and infrastructure. Both environmental incidents and **acts of nature** may affect aspects of IPT including data exchange with other SC actors. The Internet, which is a key infrastructure for the exchange of data between IPT operators and other stakeholders, was constructed with resilience in mind but nevertheless local outages are possible, particularly, in case the stability of power supply cannot be guaranteed. Environmental incidents/acts of nature usually affect availability only.

5. Good cyber security practices

Once threats from intentional attacks and threats from accidents are identified, risk analyses have to be carried out to make reasonable decisions on measures to take. It has to be kept in mind though that the measures taken could themselves be subject to threats.

The presented good security practices provide guidance to IPT operators and municipalities with respect to the assessment of the current measures to control or recover from incidents as well as to the deployment of new measures to manage these incidents. In this section, measures are mapped to the threats and incidents discussed in Section 4 and the architecture of the transport sector introduced in Section 3.

Currently, it is not very common for IPT operators to have a cyber security policy in place or to use institutionalised and codified definitions for critical assets. Overall, knowledge of, and spending for, cyber security in the IPT context appears to be rather low. Nevertheless, several cyber security measures and responses are being implemented by IPT operators. As some of the measures are not fully deployed yet, it seems that cyber security responses are rather new and on the making. Immediate responses to attacks tend to be diverse with the most common reaction being policy and procedure changes and/or deployment of new technologies.

The most used countermeasures include digital access controls to data and networks, implementation of organisational and operational procedures and guidelines, disaster recovery and maintaining back-ups, and monitoring for hardware/software faults while the ones thought to be most effective are staff training, physical access controls and protections, and security by design. Security by design, however, is difficult for IPT operators due to the long life cycles of the equipment used. Many IPT operators, however, do not measure the effectiveness of their countermeasures at all.

Possessing legacy systems is regarded as a constraint for cyber security in IPT. Conversely, key cyber security enablers identified were regulations on cyber security, data privacy and confidentiality requirements, current abilities to maintain the integrity of services/data, and standards specific to security in IPT. Measures and responses are however very diverse indicating there are no widely accepted cyber security standards sufficiently aligned to the need of IPT and/or widely used good practices.

5.1 Good practices to address intentional attacks

There are numerous measures considered useful to address threats from intended attacks. In general, it is considered to pursue a security-in-depth approach, where multiply layers of security measures protect valuable assets. Moreover, it should be acknowledged that attackers will always look for the weakest link; thus, it is not unlikely that attack vectors include not only technology and application but also employees. Therefore, it is not sufficient that technology and application are designed from the ground up to be secure, it is also necessary that employees are aware of cyber security threats and well trained to act properly. Last but not least, close coordination with CSIRTs and public safety authorities (*e.g.* the police) appears to be reasonable.

For more information, Annex 1 provides a detailed overview of the good practices relevant in the context of intentional attacks.

Use of virtual private networks: A virtual private network extends a private network across a public network and allows benefiting from the functionality, security and management policies of the private

network. Virtual private networks offer end-to-end security and can be adapted to specific requirement to protect data exchanges.

Encryption of data: Encryption is the conversion of electronic data into cipher-text which cannot be easily understood by anyone except authorised parties. Sensitive data need to be protected with (preferably strong) encryption at-rest and in-transit. Encryption guarantees data confidentiality as it protects against unauthorized access (*e.g.* wiretapping).

Deploy network intrusion detection systems: (Network) intrusion detection systems inspect all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack. To perform efficiently, network intrusion detection systems shall be configured appropriately (e.g. monitor key data exchange, know authorised connections…)

Deployment of physical protection: Physical protection aims at limiting tampering and unauthorised access to the physical infrastructure. Physical protection measures include locks, alarms, surveillance equipment, sensors, access control systems, etc. It is particularly important to protect equipment not located in a secure location (*e.g.* Field equipment).

Access control: Access controls refer to the methods by which a systems grants/denies access approval to a subject based on the successful authentication. Access control is usually a combination of physical measures (*e.g.* key, lock…) and logical measures (*e.g.* authentication, access-control list…). Access control limits unauthorized access and provides evidences in case of tampering.

Alarms and surveillance: Surveillance refers to the monitoring of behaviour or other changing information. Alarms give a signal when a problem or a specific conditions occurs. Alarms need to be defined according to the security requirements. They monitor key performance indicators and can alert of a threat. For enhanced security, alarms are associated to organizational procedures.

Implementation of an information security policy: Information Security Policy/Framework is implemented to effectively manage information security throughout an organisation. Such policy defines for example the elements to protect, the procedures to follow, the organisation of security… A common example is ISO 270001.[26]

Creation of activity logs: Activity logs, audit trails, and error logging record actions onto a log file. These log offer evidence and analysis capacity in case of an incident. They provide a good indicator of what happened and how a threat materialised effectively.

Maintenance of backups: Maintain backups of data, ideally in secure off-site servers that allow for data recovery in the case of corruption/loss. Proper maintenance of backups ensures that data recovery retains integrity (*i.e.* no loss of data).

Regular auditing: Regular auditing is an inspection or examination of infrastructure (digital or physical) to evaluate or improve its appropriateness, safety, efficiency, or the like. Audits usually provide a report that points out weaknesses/vulnerabilities and proposes remedial actions.

[26] ISO/IEC 27001:2013

Shut-down procedures: Shut-down procedures are methods for either disabling/deactivating a device. Shut-down procedures usually integrate a list of actions to perform before, during and after shut-down. They need to integrate the list of dependencies in order to limit the impacts on the service.

5.2 Good practices to address accidents

The infrastructure of IPT operators is deployed in various environments, indoor but also outdoor in uncontrolled premises. The unavailability of data exchange between IPT operators and other stakeholders culminate can be highly disruptive as it culminates in the unavailability of major transport services.

Good practices intend to protect multiple layers. They integrate from actions to minimise the accidents from occurring (*e.g.* active monitoring of KPIs, hardware redundancy) as well as the effects of a failure (*e.g.* remote deactivation of device capabilities). They encompass the full range of cyber security responses, from technical/engineering solutions (*e.g.* design specifications) through to policy/organisational responses (*e.g.* regular maintenance scheduling, response teams).

For more information, Annex 2 provides a detailed overview of the good practices relevant in the context of accidents.

Monitoring of KPIs: Key Performance Indicators (KPIs) guarantee the respect of security and performance requirements. Monitoring of KPIs (*e.g.* monitoring temperature, output, response, connectivity, etc.) is useful to determine if hardware is operating within accepted parameters, and help identify the early onset of issues.

Hardware redundancy: Redundancy is a system design in which a component is duplicated so if it fails there will be a backup. Proper hardware redundancy also integrates the need for differentiated dependencies (*e.g.* sources of energy).

Shut-down procedures: *c.f.* Shut-down procedures in Section 5.1.

Design specifications: A design specification is a detailed document providing information about the characteristics of a project to set criteria the developers will need to meet. Following the concept of *security by design*, specifications integrate security requirements as soon as the first stages of the design.

Maintenance scheduling: Maintenance scheduling aims at maximum availability and maximum mean time between equipment failures, at the least cost. Indeed, regular maintenance facilitates the early detection of potential malfunctioning or failure.

Response teams: A group of people who prepare for and respond to emergency incidents. Response teams are trained to follow predetermined procedures. Response teams interact with the operational staff and the management to ensure proper recovery of the service (see Response procedures).

Quality assurance: Quality assurance is a way of preventing mistakes or defects in manufactured products and avoiding problems when delivering solutions or services to customers. This includes the definition and application secure coding rules, the vulnerability assessment of new systems, etc.

Reporting procedures: Instructions on how to report incident. Reporting procedures are written not only for the technical staff but for all levels of the organisation. They provide guidance on “what to report”, “who to report to”, and “how to report”.

Debugging procedures: Instructions on how to debug software. They offer a solution for troubleshooting specific errors. They are mostly destined to operational and technical staff. For that purpose, security requirements must specify debugging procedures when required (*i.e.* for specific products and software).

Maintenance of backups: *c.f.* Maintenance of backups in Section 5.1.

Creation of activity logs: *c.f.* Creation of activity logs in Section 5.1.

Regular auditing: *c.f.* Regular auditing in Section 5.1.

Operator/user training: Staff/user training gives knowledge to staff to understand and know how to use cyber security processes. Regular training prepares to handle crisis (*e.g.* using scenario-based training). It also provides inputs to maintain standard operating procedures up-to-date.

Awareness raising: Information on new and emerging threats, destined to staff and management. Awareness raising also contributes to maintain awareness of existing cyber security processes.

Standard operating procedures: Instruction to achieve a desired result with respect to, for instance, incident reporting or response. Defining standard operating procedures requires the participation of the management and the staff from multiple divisions (*e.g.* operations, maintenance, response teams).

Response procedures: Instructions on how to respond to incidents. The procedures usually document the processes to follow (what to do), the reporting chain (who to report to) and define minimum KPIs for service recovery (*e.g.* degraded mode).

Error logs: Error logs collect activity logs, audit trails, and error logging record actions onto one (or several) log file(s). Error logs can be used for diagnostic as part of debugging procedures or for forensics. Error logs need to be backed-up safely (*i.e.* remotely with encryption) at regular interval.

Diagnosis of hardware/software faults: Systematic approach towards the diagnosis of hardware and software faults. Such diagnosis is usually performed during product development (by the developer) but also at testing and commissioning phase (by IPT operators). It can involve vulnerability or penetration testing, fuzzing, etc.

Encryption of data: *c.f.* Encryption of data in Section 5.1.

Access control: *c.f.* Access control in Section 5.1.

Continuous security monitoring: Continuous security monitoring includes methods such as passive network monitoring (*e.g.* IP and hardware address pairing for inventorying and to detect MAC spoofing, IP header analysis, TCP/IP traffic analysis) and active network scanning. The objective is to detect any impact on the security requirements via either a set of predefined rules or real-time analysis.

Implementation of an information security policy: *c.f.* Implementation of an information security policy in Section 5.1.

Incident reporting system: A reporting systems focusing on critical incidents. The system monitors KPIs and triggers alarms when the service or security requirements are not met. Multiple thresholds can be set. It is important to properly integrate dependencies to avoid cascade effect.

Use of open design hardware/software: Open design is the development of physical products, machines and systems through use of publicly shared design information. Using open design hardware/software can prove efficient when the redevelopment of certain functionalities is a security risk (*e.g.* encryption).

Defined terms of support: Support levels are clearly defined as well as the roles of every actor (*i.e.* operator, contractor, etc.). They shall be defined to comply with the security requirements (*e.g.* provision of security patches). The terms of support can also define the level of responsibilities and the liabilities in case of a security incident.

Regular infrastructure upgrade: Infrastructure is upgraded regularly to prevent obsolescence and overcome vulnerabilities found after a risk assessment. Upgrades can be software and/or hardware.

Surge protections: Surge protectors are designed to protect electrical devices from voltage spikes. They are necessary to protect components which are deemed essential to the service.

Increase resilience: Increase resilience by reducing "single points of failure" to critical systems (*e.g.* having alternate power sources available to run critical systems in the event of a power failure in the primary delivery system). Resilience is an integral part of system design, especially when applying the principles of *security by design*.

Remote deactivation of device capabilities: The objective is to mitigate the impact of an incident in case of a failure. Remote deactivate can be done directly at devices level with secure remote access or at the supervisory system level (*e.g.* when the device is not responding to remote control).

Emergency maintenance teams: Emergency maintenance teams address incidents that require immediate action. The objective is to recover a minimum service in a limited time.

Device hardening: Hardening refers to the process of securing a system by reducing its surface of vulnerability. Hardening can be software and/or software.

Enhanced engineering requirements: Enhanced engineering requirements refers to the process of carefully defining, documenting and maintaining requirements. The requirements are drafted within the objectives of the service and with quantifiable key performance indicators. Security is an integral part of these requirements.

Early warning systems/forecasting: Early warning systems need to actively involve the communities at risk, facilitate awareness of risks, effectively disseminate alerts, and ensure there is a constant state of preparedness.

Disaster recovery processes/centres: A disaster recovery plan is a documented process or set of procedures to recover operations in the event of a disaster. The objective is to ensure the recovery of a minimum service in a given time.

Infrastructure threat assessments: Form of assessment to evaluate the risk an infrastructure is exposed to. As threats evolve rapidly, such an assessment aims at understanding the threats applicable to the business. It is a prerequisite to any further action.

6. Key findings

Cyber security in the IPT context is a hot topic. It seems that IPT operators and municipalities have not paid much attention on the topic so far. As a result, there is a need for action. IPT operators are well advised to ensure that they are in line with good practices in terms of cyber security. Otherwise, it won't take long until the next major security incident is made public through the media – it cannot be excluded that an unprepared ITP operator will be at the centre or attention and criticism then.

6.1 Collaboration in Smart Cities is not well defined

Several, interrelated components are regarded as important for making a city smart. The most important components are connectivity and digital networking followed by cyber/network security and a clear vision and objective for the future. Additional components identified as crucial by the respondents are resilience and vision of a city as a system of systems.

SC collaborations across sectors, between multiple SCs and across national borders, appear to be common although awareness is still lacking for some of the respondents. Areas of collaboration include smart streetlight control, smart parking, ticketing and real-time passenger information, tourism activities, water waste, telecom, energy, health, mobility, environment, municipal services, IT security, and web development. Yet, definitions for IPT are not widely used or adopted.

However, these collaborations often do not translate into the implantation and running of collaborative applications/systems on the ground between SC stakeholders and transport operators. When this is in place, it is usually between different transport operators rather than between other SC stakeholders and transport operators. These collaborative applications/systems on the ground tend to focus on ticketing and client services.

Knowledge of legislation is low with the vast majority of respondents either not being aware of, or lacking detailed knowledge of, relevant legislation that applies to IPT.

6.2 Lack of reference architecture for data exchange in Smart Cities

SCs emerged as composed of several key operators and functions.

In order for IPT to operate effectively, telecoms and traffic management are the key areas for integration between IPT operators and other stakeholders, followed by energy and public safety. Additional key areas of integration volunteered by several stakeholders also include interdependencies/cascading-effects analysis, which can take different forms.

Exchange is happening mainly among transport operators and/or transport-related operators as well as between transport operators and citizens. Instead, data exchange among SC operators is more restricted and less coordinated. Furthermore, overall data exchange does not happen on a regular and consistent basis.

Data exchanged among SC operators and between IPT and SC operators varies depending on the context and the maturity of the SC. In more mature SCs this tends to focus on centralised web services to share information with passengers (i.e., availability of self-service cars and bicycles, bus schedules) and surveillance video recording shared with security control centres managed by the police. But this could also include some data exchange with electrified transport systems and energy suppliers; with infrastructure providers, law enforcement and emergency services (and to a lesser extent with local

government, transport industry associations (*e.g.* UITP), and government/regulatory bodies) in relation to criminal incidents and emergency events.

When organisations want to integrate with the SCs to exchange data with operators, there is currently no reference architecture or framework that defines how to do so. However, the components for integration are usually similar (software/applications followed by sensors and other monitor devices and physical infrastructure). This integration leads to interdependencies that may bring cascade effect in case of an incident. Hence, it is necessary to understand how elements integrate as well as the security requirements. This can be answered by the definition of a reference architecture model.

The key elements for an architecture model for SCs and IPT were identified as business, information/data, applications, technology, physical infrastructures together with integration and security as transversal elements and customers as the underlining environment.

6.3 Awareness for cyber security in Smart Cities is low, yet needed

Understanding and use of cyber security policy and critical assets are poor. The majority of respondents do not have a cyber security policy in place and do not use institutionalised and codified definitions for critical assets, either in business or societal critical terms. However, more mature organisations (particularly SC operators), tend to have a more formalised approach towards critical assets.

Business critical appears to refer to any elements which can directly impact the execution and the sustainability of the business in the long run. This includes; business revenue, service provision, business operations, and/or the brand/image of an organisation. Societal critical concerns any elements affecting the quality of life of the citizens, including their daily experience of transport, the transport environment and privacy.

In relation to business critical functions, the following were selected as the three most critical: (1) transportation safety and security, (2) traffic and vehicle management, and (3) sales, fees and charges.

Critical business assets appear to be diverse and dependent on context. The most critical were data and data storage, networking/communication, payment systems and identity management. An additional asset volunteered by the respondents that requires special attention is safety systems.

A clear distinction was made between safety and security with safety regarded as more critical than security. Safety must be maintained at a consistently high level.

In relation to societal critical functions the followings were selected as the three most critical: (1) safety and security, (2) data protection and privacy, and (3) sustainable urban mobility. An additional function volunteered by the respondents was energy management.

While organisations tend not to codify and officially identify lists of societal critical assets they recognise the societal importance of IPT. Critical societal assets tend to be less diverse and context dependent than business critical assets. The most critical were safety systems and trained staff, followed by vehicles and physical infrastructures. An additional asset volunteered by the respondents that required special attention are operational control centres.

6.4 Lack of transversal information sharing on threats and incidents

Threats appear to be multifaceted and directed against IT systems, data, infrastructure but also organisational structure (i.e., mismanagement) and the entire IPT infrastructures. The more mature the SC and IPT operators, the more encompassing the assessment of the threats. Several respondents stressed that threats are real and likely to happen.

Key threats range from disruption/interruption of electrical supply/frequency, distributed denial of service (DDoS) attacks, and the manipulation/failure of hardware and software, to terrorism/state sponsored attacks and acts of nature/environmental incidents. As transport and SC operators lean more towards threats affecting both physical and digit assets, resulting incidents have potential consequences health and safety.

The lack of information sharing limits threat awareness and harmonisation in incident response among the SC operators. Indeed, an information sharing platform on threat and incidents provides a tool for operators to enrich their knowledge by exchanging on the threats they faced and the measures they deploy to prevent and respond to incidents. With such platform it becomes easier to harmonise preparedness and incident response within the SC (or beyond, for example at national level).

6.5 Knowledge of, and spending for, cyber security in IPT is very low

Overall, organisations are not so willing to exchange information about cyber security, probably because of the reputational costs and other indirect losses related to cybercrime. Furthermore respondents indicated a low awareness of any collaboration/information-sharing pertaining to cyber security being carried out within their organisations. However, of the different categories of stakeholders interviewed/surveyed both SC and IPT operators are open to collaborate and exchange information with CSIRTs and law enforcement agencies (LEAs).

CSIRTs can be valuable trusted allies for addressing cyber security, providing they engage in proactive two-way information sharing.

6.6 Adoption of cyber security measures has been slow

Several cyber security measures and responses appear to be implemented by transport and SC operators following their level of maturity with some of the measures not fully deployed yet, which indicates that cyber security responses are rather new and on the making.

The current lack of guidelines and good practices regarding cyber security limits the dissemination and acquisition of knowledge. Thus, cyber security concerns remains limited to experts while their understanding shall apply to all operators of the SC.

Measures and responses are however very diverse indicating there are neither widely accepted cyber security standards sufficiently aligned with the needs of IPT, nor widely used good practices.

The most used measures include digital access controls to data and networks, implementation of organisational and operational procedures and guidelines, disaster recovery and maintaining back-ups, and monitoring for hardware/software faults, while the ones thought to be most effective are staff training, physical access controls and protections, and security by design.

However, the majority of organisations do not measure the effectiveness of their measures.

Immediate responses to cyberattacks tend to be diverse with the most common reaction being policy and procedure changes and deployment of new technologies.

6.7 Cyber security can be improved by raising awareness

Several gaps were identified by the different categories of respondents. These gaps tend to refer to several aspects: organisational gaps (*e.g.* governance for security, training, insider threats); policy and standardisation gaps (*e.g.* both EU standards and a coherent and recognisable EU cyber security strategy, tailored to the specific needs of SCs and IT – that are not generic in nature but specific to the contexts of IPT and enable consistency among operators), enabling technologies (*e.g.* identity management in complex trusted and entrusted environments, regular routine testing and penetration analysis), and more comprehensive approaches (*e.g.* guideline on how to improve security, security by design, awareness and understanding of the full range of cyber threats and cyber security, applicable risk assessment methodologies).

A recurring theme is the need for not confusing safety with security as they are quite different and require different approaches.

Possessing legacy systems is regarded as a constraint for cyber security in IPT. Conversely, key cyber security enablers identified were regulations on cyber security, data privacy and confidentiality requirements; current abilities to maintain the integrity of services/data; and standards specific to security in IPT.

Opinions on the prominence of cyber security are split with IPT and SC operators belonging to the more positive group. Other stakeholders, mainly security experts and policy-makers, belong to the less positive grouping. Overall, the message is that while cyber security has become more dominant within organisations, there is still a lot to do, although things are moving in the right direction.

Barriers against a more dominant role of cyber security in IPT are centred on the lack of a full understanding of specific cyber security threats relevant for IPT and the lack of a clear strategy for dealing with cyber security in IPT.

7. Recommendations

This section proposes recommendations to enhance the level of cyber security within Smart Cities. They are directed towards different groups of stakeholders.

7.1 Municipalities should support the development of a harmonised cyber security framework

The development of a harmonised cyber security framework will allow Smart Cities operators to implement common guidelines. Such frameworks need to be supported by municipalities, which would act as a coordinator between its stakeholders (operators, manufacturers, etc.). Harmonisation is important to ensure a consistent level of safety and security for any service of the city.

This framework could integrate relevant security standards and existing risk management approaches, while taking into account the particularities of the city (*e.g.* societal aspects, ICT architecture, etc.). For that reason, it is important to understand existing approaches used in the Industry and by operators, as they know their security needs and the relevant standards. Moreover, Smart Cities with a lower maturity level may find interest in frameworks developed by more advanced municipalities.

This recommendation aims at resolving findings 1, 2 and 4.

7.2 The European Commission and Member States should foster knowledge exchange and collaboration in cyber security among industry, Member States and municipalities

Several sectors beyond Intelligent Public Transport have already started investigating cyber security. As various initiatives start being deployed across Europe, it is important to foster knowledge exchange and collaboration from these sectors. This information exchange shall allow a better overall security within Smart Cities, where stakeholders would be able to benefit from more mature ones. It is also important to exchange what works and what does not work.

It is recommended that IPT Operators collaborate within and across sectors to such a platform to understand the threats and the risks, share good practices, and converge their approaches in cyber security. Moreover, it is recommended that municipalities participate to such platform in order to gain awareness and knowledge on good security practices.

This recommendation aims at resolving findings 1, 3, 4 and 7.

7.3 IPT operators should develop a clear definition of their security requirements

As IPT operators usually procure their products and services via third-party providers, the security requirements need to be expressed clearly and formally. It is recommended that IPT operators follow the concepts of *Security and Privacy by Design* by integrating their security requirements at the earliest stage of the conception of a new system. Moreover, when integrating a new system or service, the security requirements need to consider the integration of this element in the existing system.

In order to clarify the security requirements, IPT operators can define among other the technical characteristics (*e.g.* security protocols), the secure integration in their system (*e.g.* interface with other systems, access control), the support and maintenance (*e.g.* patching), the testing phase of the security functions, staff training, etc. Doing so shall lead third-party provider to propose secure products.

This recommendation aims at resolving finding 6 and have a positive impact on finding 7.

7.4 Manufacturers and solution vendors should integrate security in their products

It is recommended that manufacturers and solution vendors take the initiative to integrate security and resilience in their products, by following the principle of *Security by Design*. Manufacturers and vendors following this recommendation should be more prepared when it comes to being compliant with security requirement expressed by IPT operators.

It is recommended to take stock of existing good practices from other domains instead of redeveloping new security functions. Moreover, vendors and manufacturers are encouraged to validate their security via testing or other methods (*e.g.* certification). They can also propose added-value services around security (*e.g.* support, training).

This recommendation aims at resolving findings 5 and 6.

7.5 IPT operators and municipalities should define the responsibilities of senior management in cyber security

Senior management has several responsibilities in an organisation. It is recommended that IPT operators and municipalities define the responsibilities of their senior management in cyber security. The objective of this recommendation is to enhance the readiness level against cyber threats and their consequences.

These responsibilities shall cover the roles, duties and obligations of every manager, their reporting chain, as well as additional actions (*e.g.* coordination between different units, preparation, etc.). Defining responsibilities could also become an incentive to enhance the level of cyber security in the organisation.

This recommendation aims at resolving findings 3, 5, 6 and 7.

7.6 The European Commission and Member States should clarify the responsibilities of every actor

With the integration of cyber-physical products in Smart Cities, cyber threats can have real consequences on the safety of citizens. It is important that the European Commission and Member States clarify the responsibilities of every actor is case of a cyber incident.

It is recommended to clarify the responsibilities for all actors involved in Smart Cities (*i.e.* IPT operators, municipalities, manufacturers, integrators and end-users) in regard to data collection, exchange and processing. This recommendation should bring a better knowledge of the rights and duties of everyone to protect data and ensure safety in Smart Cities.

This recommendation aims at resolving findings 2 and 6 and have a positive impact on finding 3.

7.7 IPT operators and municipalities should allocate higher spending on cyber security

Cyber security has a cost that integrates technical and non-technical solutions. It is recommended that IPT operators and municipalities invest allocate higher budget on cyber security, in particular to raise awareness, provide training, develop expertise, etc. for all staff as well as senior management.

Moreover, this recommendation should facilitate the acquisition of third-party solutions in compliance with the security requirements.

This recommendation aims at resolving findings 5 and 6 have a positive impact on findings 4 and 7.

7.8 Smart Cities and standard organisations should integrate cyber security in the maturity level of Smart Cities

Several ranking systems exist to classify Smart Cities according to their level of maturity. Although resilience is sometimes part of the indicators used to establish a ranking, cyber security is not always considered.

With the increase in connectivity and data exchanges in Smart cities, it is recommended that existing standards and ranking systems integrate cyber security as one of the key indicator of the maturity level. Doing so shall help more mature cities explain their security measures and bring incentive to less mature cities to enhance their cyber security.

This recommendation aims at resolving findings 2 and have a positive impact on findings 1 and 6.

Annexes

A.1 Mapping of good practices in the context of intentional attacks

Measures to address eavesdropping/wiretapping are the use of Virtual Private Networks (VPNs), encryption of data to prevent this threat and the deployment of Network Intrusion Detection Systems (IDS) to detect it.

Theft can include a range of targets from infrastructure (*e.g.* copper cabling) to technology (*e.g.* laptops) to data and intellectual property. This range of diverse targets requires the implementation of very different protection measures, if thefts are to be prevented. Such defences range from:

- Physical measures to prevent access to restricted areas and the removal of infrastructure and technology (*e.g.* secure and monitor access to premises through, for instance, alarms or authorised personal).
- Measures to reduce the value of stolen objects such as encryption of data.
- Digital measures to prevent access such as secure storage (*e.g.* for cryptographic keys), firewalls and authentication systems.
- Policy based procedures such as implementing an information security policy.
- Post-theft tools including activity logs and backups.

Measures to address tampering/alteration are deployment of physical protection, access control, alarms and surveillance, implementation of an information security policy, creation of activity logs, regular auditing, and maintenance of backups. Similar to theft, tampering/alteration of information/data, applications or technology can be targeted with very different protection measures. Measures to address this threat must be tailored to the target. Such defences range from: physical measures to prevent access to restricted areas and the use of tamper-proof designs; measures to make tampering/alteration easier to detect, such as measures to mitigate the in transit manipulation of messages travelling between systems or actors; digital measures to prevent access such as firewalls and authentication systems; policy based procedures such as implementing an information security policy; and post-event tools including activity logs, audits and backups.

Measures to address unauthorized use/access are deployment of physical protection, access control, alarms and surveillance, shut-down procedures, creation of activity logs, and use of Network Intrusion Detection Systems. Information/data, applications or technology can used/accessed in an unauthorised way by both external attackers and insiders. Depending on the motivation of the attacker, this unauthorised use/access may result in outcomes covered in other threat-groups discussed above. Measures for protecting against unauthorised use/access cover the full range from physical/digital protections through to procedures for remotely disabling the capabilities of compromised devices, and activity logs and network IDSs for detecting these attacks.

Addressing threats such as strike, vandalism/civil disorder and terrorism, is difficult from a cyber security perspective. Measures may only avoid the threat of damage occurring (*e.g.* through physical protections, security by camouflage), reduce the vulnerability of components to damage (*e.g.* by using tamper resistant designs), and mitigate the expected consequences of a successful attack (*e.g.* with disaster recovery units, contingency planning). If terrorists target ITSs specifically attacks will manifest as the other threats identified and, as such, the protection measures identified for these various threats will apply. Close

cooperation with CSIRTs and public safety authorities is particularly important for IPT operators and municipalities in such situations.

Table 2 provides an overview of the good practices relevant in the context of intentional attacks.

Table 2 Good practices relevant in the context of intentional attacks

GOOD PRACTICES	THREAT ADDRESSED	LAYERS TARGETED	DESCRIPTION
Use of virtual private networks	Eavesdropping/wiretapping	Data transmission network Data aggregation connectivity	A virtual private network extends a private network across a public network and allows benefiting from the functionality, security and management policies of the private network.
Encryption of data	Eavesdropping/wiretapping Theft	Data transmission network Data processing Data aggregation connectivity	Encryption is the conversion of electronic data into cipher-text which cannot be easily understood by anyone except authorised parties.
Use of network intrusion detection systems	Eavesdropping/wiretapping Unauthorized use/access	Data transmission network Data processing Data aggregation connectivity Smart processing	(Network) intrusion detection systems inspect all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack.
Deployment of physical protection	Theft Tampering/alteration Unauthorized use/access	all	Physical protections to protect physical infrastructure, including locks, alarms, surveillance equipment, sensors, access control systems, etc.
Access control	Theft Tampering/alteration Unauthorized use/access	all	Access controls refer to the methods by which a systems grants/denies access approval to a subject based on the successful authentication.
Alarms and surveillance	Theft Tampering/alteration Unauthorized use/access	all	Surveillance refers to the monitoring of behaviour or other changing information. Alarms give a signal when a problem or a specific conditions occurs.
Implementation of an information security policy	Theft Tampering/alteration	all	Information Security Policy/Framework is implemented to effectively manage information security

GOOD PRACTICES	THREAT ADDRESSED	LAYERS TARGETED	DESCRIPTION
			throughout an organisation. A common example is ISO 270001.
Creation of activity logs	Theft Tampering/alteration Unauthorized use/access	Data transmission network Data processing Data aggregation connectivity Smart processing	Activity logs, audit trails, and error logging record actions onto a log file.
Maintenance of backups	Theft Tampering/alteration	Field components Data processing Data aggregation connectivity Smart processing	Maintain backups of data, ideally in secure off-site servers that allow for data recovery in the case of corruption/loss.
Regular auditing	Tampering/alteration	Data transmission network Data processing	Regular auditing is an inspection or examination of infrastructure (digital or physical) to evaluate or improve its appropriateness, safety, efficiency, or the like.
Shut-down procedures	Unauthorized use/access	Field components	Shut-down procedures are methods for either disabling/deactivating a device.

A.2 Mapping of good practices in the context of accidents

Measures to address hardware failure/malfunctioning are monitoring of KPIs, hardware redundancy, shut-down procedures, design specifications, maintenance scheduling, and response teams. The physical infrastructure of IPT operators is deployed in inhospitable environments. Individual components will be subject to the effects of weather, constant use, vibration, rough handling and heavy loads, and may be deployed for many years. This may not be the case for most components relevant with respect to data exchange between IPT operators and other stakeholders but nevertheless, hardware failure/malfunctioning is an issue to be addressed. Given the potentially high disruptive impact of hardware failures in an ITS, culminating in the unavailability of major transport services, multiple layers of protection measures are available. These cyber security measures range from actions to minimise malfunctions/failures occurring (*e.g.* active monitoring of KPIs, hardware redundancy), through to protections which minimise the effects of any failure (*e.g.* remote deactivation of device capabilities). They encompass the full range of cyber security responses, from technical/engineering solutions (*e.g.* design specifications) through to policy/organisational responses (*e.g.* regular maintenance scheduling, response teams).

Measures to address software error are quality assurance, monitoring of KPIs, reporting procedures, debugging procedures, maintenance of backups, activity logs, and regular auditing. Similar to hardware failure/malfunctioning, software errors cannot be completely eliminated given the complexity of individual pieces of software as well as the exponential number of interactions between multiple applications. Cyber security responses focus on identifying as many of these errors as possible before or during implementation (*e.g.* quality assurance by means of beta testing) as well as monitoring, error logging, auditing and debugging procedures to address errors as they arise during operation. Data backups and activity logs assist in returning a system to a pre-error state as well as in mitigating the damage caused by errors.

Measures to address operator/user error are operator/user training and awareness raising, quality assurance, standard operating procedures, reporting procedures, response procedures, maintenance of backups, activity logs, error logs, regular auditing, monitoring of KPIs, diagnosis of hardware/software faults, encryption, access controls, continuous security monitoring, information security policy, and incident reporting system. As this category is not focussed on malicious actions by users/operators, rather genuine errors, responses focus on reporting of incidents, training and the implementation of standard operating procedures to mitigate the likelihood of their (re)occurrence, as well as activities to assist a network to recover from any damage caused. Applications of common standards, training, and quality assurance (*e.g.* testing of systems) can be measures to mitigate the risk of configuration errors occurring. However, given the complexity of ITSs, with their multitude of different interconnects elements, it is impossible to completely preventing the occurrence of all such errors. Hence, system monitoring and the (automated) diagnosis of software/hardware faults are required. To avoid accidental disclosure of information protection measures centre around software-based solutions and operational processes and awareness raising, to minimise the risk of such accidents occurring. Software-based measures include encryption of transmitted and stored data, access controls to minimise access of stored data by unauthorised personal, and continuous security monitoring systems.[27,28] Operational processes include the implementation of an information security policy, training, incident reporting systems and processes for recovering disclosed data.

[27] Microsoft, Developing a City Strategy for Cyber security, 2014
[28] Das et al, Handbook on Securing Cyber-Physical Critical Infrastructure.

Measures to address end of support/obsolescence are use of open design hardware/software, defined terms of support, and regular infrastructure upgrade. As technology progresses, hardware and software will become outdated and eventually obsolete. Additionally, manufacturers, solutions providers and vendors may either cease trading or reach a point where they are no longer supporting older hardware/software. This can have implications for IPT operators and municipalities, especially when updating infrastructure depends on political decisions and financial constraints/priorities. Ultimately, IPT operators may have little leverage to influence decisions to cease supporting/upgrading of products. Options open to them include using open design products over proprietary platforms to minimise becoming reliant on a single provider and defining support terms in procurement contracts.

Measures to address electrical and frequency disturbance/interruption are surge protections, increase resilience (remote deactivation of device capabilities), response procedures, maintenance of backups, and emergency maintenance teams. Electrical and frequency disturbance/interruption can arise from many different initiators, including, among others, accidents and acts of nature but also deliberate attacks cannot be excluded. Security responses seek to mitigate the vulnerability of systems by building in surge protections to address overloading, and alternate power supply avenues to address lack of supply. Maintaining data backups and having response teams to repair supply issues promptly go to reducing the expected impact of such incidents.

Measures to address environmental incidents/acts of nature are device hardening, enhanced engineering requirements, early warning systems, disaster recovery processes/centres, maintenance of backups, hardware redundancy, and infrastructure threat assessments. Given the diverse range of acts of nature, it is beyond the scope of this research to perform an individual assessment of protection measures that are specific for each different act. However, by adopting a higher-level approach and looking at cyber security measures that cross multiple acts a reasonably comprehensive coverage of this category of threats can be provided. Acts of nature (with the possible exception of some flood protections) cannot be influenced or prevented, and threat mitigation measures are unavailable. Hence, cyber security measures must focus on either mitigating the vulnerability of a system to an occurring act of nature (*e.g.* device hardening, enhanced engineering requirements), and mitigating the consequences expected to arise from such an act (*e.g.* early warning systems, disaster recovery processes, maintenance of backups, hardware redundancy). Environmental incidents have similar effects; though potentially on a smaller scale. As opposed to acts of nature, however, it is possible to mitigate the risk of environmental incidents occurring. Measures such as infrastructure threat assessments are considered a useful tool in this regard.

These numerous measures are considered useful to address threats from accidents. Section 5 provides an overview of the good practices relevant in the context of accidents.

Table 3 Good practices relevant in the context of accidents

GOOD PRACTICES	THREAT ADDRESSED	LAYERS TARGETED	DESCRIPTION
Monitoring of KPIs	Hardware failure/malfunctioning Software error Operator/user error Environmental incidents/acts of nature	all	Active monitoring of Key Performance Indicators (KPIs): monitoring temperature, output, response, connectivity, etc., to determine if hardware is operating within accepted parameters, and help identify the early onset of issues.
Hardware redundancy	Hardware failure/malfunctioning Environmental incidents/acts of nature	all	Redundancy is a system design in which a component is duplicated so if it fails there will be a backup.
Shut-down procedures	Hardware failure/malfunctioning	Field components	See Table 2.
Design specifications	Hardware failure/malfunctioning	Field components	A design specification is a detailed document providing information about the characteristics of a project to set criteria the developers will need to meet.
Maintenance scheduling	Hardware failure/malfunctioning Environmental incidents/acts of nature	all	Maintenance scheduling aims at maximum availability and maximum mean time between equipment failures, at the least cost.
Response teams	Hardware failure/malfunctioning	Field components	A group of people who prepare for and respond to emergency incidents.
Quality assurance	Software error Operator/user error	all	Quality assurance is a way of preventing mistakes or defects in manufactured products and avoiding problems when delivering solutions or services to customers. This includes the definition and application secure coding rules.
Reporting procedures	Software error Operator/user error	all	Instructions on how to report incident.
Debugging procedures	Software error	all	Instructions on how to debug software.

GOOD PRACTICES	THREAT ADDRESSED	LAYERS TARGETED	DESCRIPTION
Maintenance of backups	Software error Operator/user error Electrical and frequency disturbance/interruption Environmental incidents/acts of nature	all	See Table 2.
Creation of activity logs	Software error Operator/user error	all	See Table 2.
Regular auditing	Software error Operator/user error	all	See Table 2.
Operator/user training	Operator/user error	all	Staff/user training gives knowledge to staff to understand and know how to use cyber security processes.
Awareness raising	Operator/user error	all	Inform staff of new and emerging threats. Maintain awareness of existing cyber security processes.
Standard operating procedures	Operator/user error	all	Instruction to achieve a desired result with respect to, for instance, incident reporting or response.
Response procedures	Operator/user error Electrical and frequency disturbance/interruption	all	Instructions on how to respond to incidents.
Error logs	Operator/user error	all	Activity logs, audit trails, and error logging record actions onto a log file.
Diagnosis of hardware/software faults	Operator/user error	all	Systematic approach towards the diagnosis of hardware and software faults.
Encryption	Operator/user error	Data transmission network Data processing	See Table 2.
Access controls	Operator/user error	Data transmission network Data processing	See Table 2.

GOOD PRACTICES	THREAT ADDRESSED	LAYERS TARGETED	DESCRIPTION
Continuous security monitoring	Operator/user error	Data transmission network Data processing	Continuous security monitoring includes methods such as passive network monitoring (*e.g.* IP and hardware address pairing for inventorying and to detect MAC spoofing, IP header analysis, TCP/IP traffic analysis) and active network scanning.
Information security policy	Operator/user error	Data transmission network Data processing	See Table 2.
Incident reporting system	Operator/user error	Data transmission network Data processing	A reporting systems focusing on critical incidents.
Use of open design hardware/software	End of support/obsolescence	all	Open design is the development of physical products, machines and systems through use of publicly shared design information.
Defined terms of support	End of support/obsolescence	all	Support levels are clearly defined.
Regular infrastructure upgrade	End of support/obsolescence	all	Infrastructure is upgraded regularly.
Surge protections	Electrical and frequency disturbance/interruption	all	Surge protectors are designed to protect electrical devices from voltage spikes.
Increase resilience	Electrical and frequency disturbance/interruption	all	Increase resilience by reducing 'single points of failure' to critical systems (e.g. having alternate power sources available to run critical systems in the event of a power failure in the primary delivery system).

GOOD PRACTICES	THREAT ADDRESSED	LAYERS TARGETED	DESCRIPTION
Remote deactivation of device capabilities	Software error Hardware failure/malfunctioning Environmental incidents/acts of nature Electrical and frequency disturbance/interruption	all	Deactivate the capabilities of a services to limit the impact of a failure on the service.
Emergency maintenance teams	Electrical and frequency disturbance/interruption	all	Emergency maintenance teams address incidents that require immediate action.
Device hardening	Environmental incidents/acts of nature	all	Hardening refers to the process of securing a system by reducing its surface of vulnerability.
Enhanced engineering requirements	Environmental incidents/acts of nature	all	Enhanced requirements engineering refers to the process of carefully defining, documenting and maintaining requirements.
Early warning systems/forecasting	Environmental incidents/acts of nature	all	Early warning systems need to actively involve the communities at risk, facilitate awareness of risks, effectively disseminate alerts, and ensure there is a constant state of preparedness.
Disaster recovery processes/centres	Environmental incidents/acts of nature	all	A disaster recovery plan is a documented process or set of procedures to recover operations in the event of a disaster.
Infrastructure threat assessments	Environmental incidents/acts of nature	all	Form of assessment to evaluate the risk an infrastructure is exposed to.

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, Greece

TP-01-15-954-EN-N

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

ISBN: 978-92-9204-162-5
doi:10.2824/846575