Complex Systems Informatics and Modeling Quarterly (CSIMQ)
eISSN: 2255-9922
Published online by RTU Press, https://csimq-journals.rtu.lv
Article 210, Issue 38, March/April 2024, Pages 100–131
https://doi.org/10.7250/csimq.2024-38.04

Information Security and Privacy Management in Intelligent Transportation Systems

Mariia Bakhtina[1]*, Raimundas Matulevičius[1], and Lukaš Malina[2]

[1]Institute of Computer Science, University of Tartu, Narva mnt. 18, Tartu, 51009, Estonia
[2]Department of Telecommunications, Faculty of Electrical Engineering and Communication, Brno University of Technology, Technicka 12, Brno, 61600, Czech Republic

bakhtina@ut.ee, rma@ut.ee, malina@vut.cz

Abstract. With the global digitalization of services, passenger Intelligent Transportation Systems (ITSs) have emerged as transformative components, yet the practical implementation of state-of-the-art measures to ensure information security and privacy presents substantial challenges. In this article, we propose a framework for information security and privacy management. The framework is validated through two empirical studies. First, the framework is used to extract data during the literature review defining state-of-the-art aspects and measures. Second, a survey-based analysis of running passenger ITSs in selected regions of the European Union provides insights into real-life ITS implementations, enabling a thorough comparison with the proposed state-of-the-art measures. The study also showed that the proposed framework depicts some dependencies between measures, and, thus, using its matrix structure for the state of information security and privacy management in the organization helps to cross-check the usage of policies or methodologies by the organization departments. Our findings resulted in recommendations for organizations developing ITSs to enhance their information security and privacy management systems and bridge the gap between research proposals and practical implementation.

Keywords: Information Security Management, Privacy Management, Intelligent Transportation, Survey.

1 Introduction

With the trend of global digitalization of services in both private and public sectors, we observe the appearance of new services delivered by the enabled IT systems connections and enabled digital supply chain. Among such sectors where connectivity takes place are passenger transportation and mobility. The creation of intelligent transportation systems (ITSs), which are systems of systems

* Corresponding author

Reference: M. Bakhtina, R. Matulevičius, and L. Malina, "Information Security and Privacy Management in Intelligent Transportation Systems," Complex Systems Informatics and Modeling Quarterly, CSIMQ, no. 38, pp. 100–131, 2024. Available: https://doi.org/10.7250/csimq.2024-38.04

Additional information. Authors ORCID iD: M. Bakhtina – https://orcid.org/0000-0002-0940-9713, R. Matulevičius – https://orcid.org/0000-0002-1829-4794, and L. Malina – https://orcid.org/0000-0002-7208-2514. PII S225599222400210X. Article received: 13 February 2024. Accepted: 17 April 2024. Available online: 30 April 2024.

(SoS) that not only allow the digitalization of existing services for citizens but also strive to improve mobility and reduce negative impacts of transport usage. As the Spanish minister of transport, mobility, and urban agenda said in [1]: "Intelligent transport systems can save us time, reduce emissions and congestions, and simplify journey planning".

The European Union (EU) encourages countries to implement ITSs, for instance, by adopting the updated ITS directive that provides a framework for deploying Intelligent Transport Systems [2]. ITSs involve processing numerous data of different natures – publicly available traffic data, data about companies' resources, and citizens' data about their identities and mobility patterns. The possibility of accessing such data instances separately may not be a high risk, but manipulating such data instances in tight-connected settings of ITS may cause a chain of security threats and have a high impact on both companies and citizens.

To avoid risks related to the mentioned data leakages and malicious usage, the research community and companies work on defining the measures to ensure the information security and privacy of end-user data. Assuming that the published academic papers (e.g., [3], [4], [5]) depict the latest state of ITS development and support, we consider such measures from the papers as the state-of-the-art measures for protecting information in ITS to meet information security and privacy requirements (from now on, "state-of-the-art measure"). Meanwhile, private and public companies may lag behind and develop solutions not as fast as they are proposed. Such a delay may be caused by the too-idealistic set-up proposed in the literature, too hard-to-implement technologies due to limited resources, infrastructure readiness, or the lack of awareness about state-of-the-art developments.

As ITSs are becoming a part of our everyday life, some questions are yet to be answered for the citizens and companies to understand the situation and potential threats of using ITSs. To the best of our knowledge, there has been no comprehensive study conducted to analyze whether such new ITSs preserve privacy and assure information security. Also, there are no studies showing whether organizations using ITSs do any changes to align its systems with the new landscape. Finally, it is not clear whether organizations update their information security and privacy management systems with the systems shifting to ITSs.

Thus, our study aims to identify the challenges of ensuring the security and privacy of information in the evolving ITS characterized by the gap between state-of-the-art research proposals and real-life usage of them. The main research question (MRQ) of the study is the following: ***What are the challenges in information security and privacy management in ITSs?*** Hereinafter, we refer to information security and privacy management as "InfoSec & PM". To answer MRQ, we divide it into the following sub-questions:

- RQ1. What is the level of ITSs maturity?
- RQ2. In which areas do organizations, that use or maintain ITSs, operate?
- RQ3. What kind of information is being protected in ITSs?
- RQ4. Which information security and privacy management standards support ITSs?
- RQ5. Which information security and privacy management methodologies do the organizations that use or maintain ITSs follow?
- RQ6. Which information security and privacy management technologies are applied by organizations that use or maintain ITSs?

In this study, we consider that an ITS is a (set of) system(s) that consists of advanced technologies and information processing added into transportation infrastructure and vehicles to improve safety, efficiency, and sustainability in transportation systems [6], [7], [8]. ITS utilizes various technologies such as sensors, communication networks, data analytics, and control systems to gather and disseminate real-time information, optimize traffic flow, enhance mobility, and reduce congestion and environmental impact. ITSs are used for freight and passenger transportation and may differ by the transportation modes (e.g., road, rail, water). However, within this study,

we focus on the road passenger transportation systems limiting ITSs to those that deliver the following services – ride-hailing, vehicle sharing, smart parking, electronic toll collection, and vehicle-to-vehicle communication.

To answer the stated questions, first, we review common models guiding information security and privacy management (Section 2) and propose a framework for information security and privacy management (i.e., FISP-ProCOP) (Section 3). Then, we use FISP-ProCOP as a theoretical model for two empirical studies (Section 4). The first study is a literature review that results in the defined state-of-the-art aspects and measures that help to assure information security and privacy in ITSs (Section 5). The second study is a survey-based analysis of the running ITS within the selected region that results in the comparison of the real-life ITS and the used measures for InfoSec & PM with the state-of-the-art measures defined through the literature review (Section 6). As the researched area for the study, we select two regions in the EU – South Moravia in the Czech Republic and Estonia – where ITSs are used and which have market actors specialized in cybersecurity. As a result, the comparison allows us to identify both the challenges of addressing information security and privacy management perceived by the organizations themselves and the identified gaps in using state-of-the-art security privacy measures. To address such challenges, we develop recommendations for the organizations developing, supporting, or using ITSs to improve their InfoSec & PM (Section 7). In Section 8, we review the related work, while Section 9 highlights the limitations of our study and the results. Finally, Section 10 concludes the article and underlines the directions for future work.

2 Background

2.1 Cybersecurity Landscape of Transportation Sector

An overview of the cybersecurity threats landscape in the transport sector has been provided in [9]. The study shows that the majority of attacks on the transport sector target exactly information technology (IT) systems. Thus, IT-enabled components of intelligent transportation systems are primarily under threat in contrast to operational technology systems represented by physical infrastructural components of ITSs like sensors and actuators.

The road transportation industry is primarily confronted with ransomware attacks, with data-related risks and malware following closely behind. Ransomware attacks have particularly targeted automotive producers, including original equipment manufacturers (OEMs) and suppliers, resulting in disruptions to production. Also, one car-sharing company has fallen victim to ransomware attacks [9]. Data-related threats primarily focus on infiltrating IT systems to obtain customer and employee data, along with proprietary information.

2.2 Information Security Frameworks

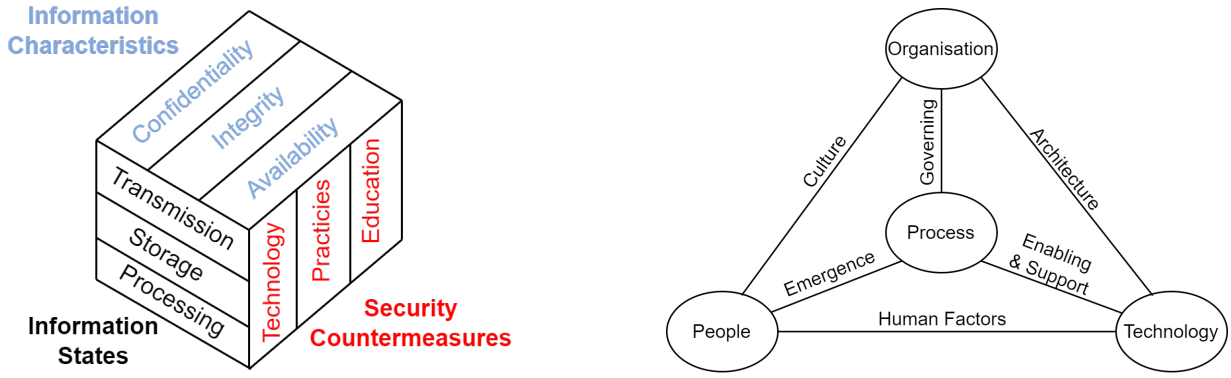
The screening of the literature on information security and privacy management in ITS shows that the proposed measures for securing information vary from the specific protocols for the data transfer and system architectures up to defining new roles of stakeholders and following security related standards. Thus, to understand the whole picture of how organizations are handling InfoSec & PM, we should remember that information security is a multidisciplinary domain. To define how organizations handle it, we should consider multiple aspects of the organizations involved in the InfoSec & PM.

Models and frameworks are abstract ways of describing concepts and their connections to the selected domain and this helps unify the understanding of the domain. Hence, the respective models and frameworks are supposed to guide one in understanding information security and privacy. However, there are numerous of those, and they differ by the level of detail and the purpose: descriptive, which describe the state, e.g., ISACA BMIS [10] and McCumber cube [11] that are depicted in Figure 1, or prescriptive, which prescribe actions to be perfomed (e.g., NIST

CSF [12], HITRUST CSF [3]). Since in our study we want to understand the static view, we consider the descriptive InfoSec & PM models and frameworks as a theoretical background for the data extraction.

McCumber cube. Presented in [11], the McCumber cube is one of the earliest models that guides examining information security. The model proposes to examine security from three dimensions (Figure 1a). First, security principles, which are often referred to as the CIA-triad, describe the properties of information that should be preserved. Second, the model proposes to consider the state in which information can exist within the system, namely storage, processing, and transmission. Third, countermeasures are applied to ensure that critical information properties are maintained while information resides or moves between the states. Countermeasures are primarily based on the technological solutions presented by hardware, firmware, or software. However, the second important building block of information security countermeasures is policy and practice, which describe what are the existing policies to follow using information systems and procedures to employ or to enhance technological security countermeasures. Finally, while the first two countermeasure types enable security-enhanced information systems, the final dimension comprises people. Thus, ensuring that people understand the necessity to protect information and be capable of its maintenance significantly contributes to the overall level of the system's information security.

ISACA business model for information security (BMIS). Proposed by Roessing in [10], BMIS is a framework of business-related elements used to describe information security in an organization. The framework shows the dynamic connections between the four key dimensions where information security and privacy take place and how they affect each other through the depicted interconnections (Figure 1b).



(a) McCumber cube [11] **(b)** ISACA's BMIS [10]

Figure 1. Information security frameworks

Organization refers to "a network of people, assets, and processes which are working together toward a common goal" [10]. Thus, organizational design and strategy describe how the organization's strategy guides the processes based on the strategic objectives, how the organizational design and strategy itself are guided by external factors, and how the organization's strategy drives the architecture of the technical security measures. The people element extends the BMIS model with a non-technical perspective by highlighting the importance of stakeholders' values, beliefs, and behaviors that influence information security and privacy in the organization. The process element describes formal and informal processes that exist in an organization. The processes are governed by the organization's strategy and enable the strategy. The technology

[3] https://hitrustalliance.net/product-tool/hitrust-csf/

element describes the IT solutions that enable and support the processes. This is the key element commonly addressed by information security and privacy management, as most of the proposed security and privacy countermeasures are technological measures. However, the BMIS model highlights the tight connection of the technical solutions with the existing organization governance and objectives, processes, and people, which the IT systems support.

Reference Model of Information Assurance & Security (RMIAS). First proposed in [13], RMIAS is a high-level guide that outlines the key components, relationships, and principles involved in ensuring the confidentiality, integrity, and availability of information assets. Depicted in Figure 2, RMIAS consists of four dimensions: information system security life cycle, information taxonomy, security goals, and security countermeasures. The reference model aims to assist with the development and revision of an information security policy document. The model considers four types of security countermeasures: organizational, human-oriented, technical, and legal.

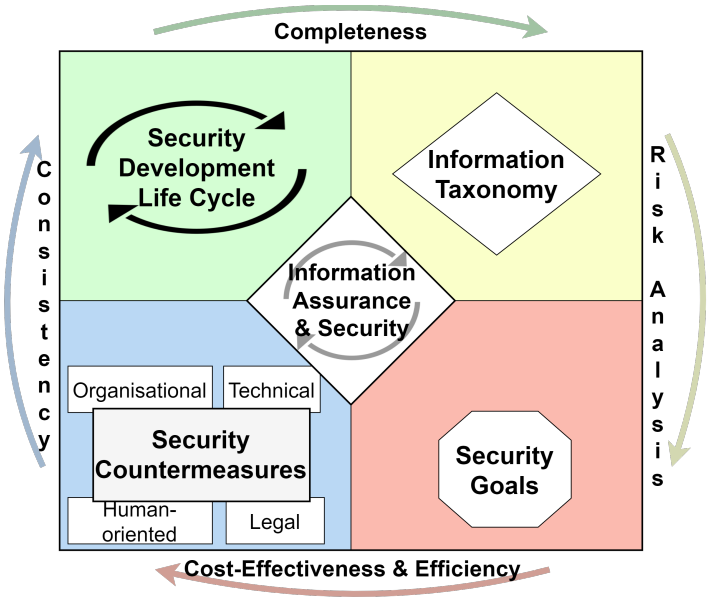


Figure 2. Key elements of a Reference Model of Information Assurance & Security (based on [13])

Industry Standards. Along with the reviewed information security frameworks, several standards, and frameworks are known among industry representatives. **ISO/IEC 27001** is an international standard for information security management systems that provides a framework for organizations to establish, implement, maintain, and continually improve an effective information security management system. The standard also contains a set of security controls for mitigating the selected threats. Having the possibility to be certified against it, ISO/IEC 27001 is a de facto industry-used framework for information security used by established organizations to demonstrate commitment to information security to customers and partners [14]. **ISO/IEC 27701** is another international standard built upon ISO/IEC 27001 and includes requirements for a privacy information management system. Other commonly used recommendations are NIST SP, which are special publications from the American National Institute of Standards and Technology. For instance, **NIST SP 800-39** [15] focuses on managing information security risks from an organizational perspective, and **NIST SP 800-37** [16] provides a structured framework for managing cybersecurity risks within the context of system development and operation. Meanwhile, **NIST SP 800-53** [17] is a catalogue of security and privacy controls that organizations can use to protect their information systems and data. Originating from the American agency, NIST SP are commonly used by U.S. government agencies and are more recognizable by U.S. organizations. While guidelines and frameworks from ISO/IEC and NIST SP are industry best practices and

provide comprehensive recommendations on managing information security, they are proved to be of high complexity [18] and, thus, are resource-intensive, particularly for smaller organizations.

To sum up, the reviewed models complement one another and are useful for summarising the domain knowledge on information security management. Despite that, the models are too general to be used as a theoretical model for data extraction in the empirical study of ITS. While the models explain the dependencies of aspects of information security on one another, they do not have accompanying guidelines on how these models can be instantiated to depict the state of a selected organization. As a result, based on the information security frameworks and models we reviewed and considering the need for a model that would help analyze the state of information security and privacy management on intelligent systems, we developed a new framework for information security and privacy management (FISP).

3 Proposed Framework for Information Security and Privacy Management (FISP-ProCOP)

The proposed framework (see Table 1) is based on BMIS, McCube, and RMIAS models. Assuring the privacy of users' data is directly connected with securing it (e.g., based on GDPR), we consider information security management and privacy management as tightly coupled tasks in our study. Consequently, the proposed framework does not differentiate attributes of the context that affect only one of them (privacy or security) and do not affect the other. The proposed framework is more granular than the reviewed ones and, thus, is more applicable for the purpose of our study – defining the static state of information security and privacy management in the context of intelligent socio-technical systems (e.g., intelligent transportation systems).

Table 1. FISP-ProCOP: Framework for information security and privacy management

Dimension	Category	Attribute
P. People	PA. Actors	Actors, stakeholders, entities
		Goals, tasks, motives
	PR. Relationships	Relationships and dependencies between actors
O. Organization	OS. Strategy	Purpose for the system usage, org. design & strategy
		Challenges to address
	OC. Formal Constraints	Legislation, regulation, standard
	OI. Information Involved	Type of information used
		How the information is manipulated
		Security criteria
		Privacy objectives
C. Sec. & Privacy Countermeasures	CP. Policies & Practices	Policies & practices
	CE. Training & Education	Training & education
	CT. Technology	Architectural measures
		Use case-oriented technological measures
		Cryptographic building blocks
		Others technological measures
Pr. Processes	PrL. System Lifecycle	Security as a part of the system lifecycle
	PrU. Usage of the System	Use cases of the system as a part of the business processes

The FISP describes four key aspects, i.e. *dimensions*, that, from the business point of view, affect the management of information security and privacy assurance – ***Pro****cesses*, *security & privacy* ***C****ountermeasures*, ***O****rganization*, and ***P****eople* (ProCOP). Each dimension contains multiple categories, which are divided by the attributes. Finally, each attribute may have one or more instances of such attribute that correspond to the instantiation of the model to the selected context of the system usage.

- The dimension of *People* aims to answer the question: what are the stakeholders (including physical and legal entities) that have an interest or are involved in the system lifecycle (design, developments, support, or usage)? Thus, the category *Actor* describes (i) who the stakeholders are and (ii) which goals, tasks, and motives they have towards the system. Another category of *Relationships* depicts the relationships and dependencies between the identified actors.
- The dimension of *Organization* aims to answer the question: what are the business goals that guide and restrict the system? The category of *Strategy* describes the internal organizational constraints: (i) the purpose for the system usage, and (ii) the existing challenges faced by the organization. The category of *Formal constraints* describes the goals that affect the system and are set up by the external entities – through (i) legislation and regulations and (ii) standards. The category of *Information involved* describes the goals of manipulating information in the context of the other two categories, namely strategy and formal constraints: (i) the expected types of information to be manipulated with, (ii) how such information is manipulated (e.g., based on which data), (iii) the security criteria to be achieved for the information assets, and (iv) the privacy objectives to be achieved for the information assets.
- The dimension of *Security & Privacy countermeasures* aims to answer the question: which measures are used to ensure information security and data privacy in the context of People and Organisation dimensions? The measures in the dimension are divided into three categories. The category of *Policies & practices* describes the policies and practices in the organization that enable achieving the goals from the Organisation dimension. The category of *Training & education* describes the educational practices used in the organization for the identified actors. The category *Technology* describes the technological solutions that enable ensuring information security and data privacy. The category consists of four attributes: (i) architectural solutions, (ii) use case-oriented technological measures, (iii) cryptographic measures used, and (iv) any other technological solutions (e.g., technologies, protocols, tools) which do not fall under the other attributes and support the security and privacy objectives.
- The dimension *Processes* aims to answer the question: how the dimensions of People, Organization, and Countermeasures are integrated together in the processes in the organization? The category of *Usage of the system* describes the use cases of the system as a part of the business processes. Meanwhile, the category of *System lifecycle* describes how the security and privacy countermeasures are incorporated into the system lifecycle (e.g., either the security and privacy countermeasures are once implemented and never updated or they are regularly reassessed through a risk management framework and updated if needed).

While FISP-ProCOP is presented in the form of a matrix, it does not depict relationships between dimensions, categories, and attributes, for instance, in contrast to RMIAS. On the other hand, due to the tabular structure, our hypothesis is that the model is a more useful tool for depicting the static view of information security and privacy management in the complex information system than other reviewed frameworks and models. Additionally, the assumption is that such a representation of dimensions that affect information security and privacy in the system can help depict the effect of attributes on one another by considering measures usage from multiple perspectives. As a result, FISP-ProCOP should help to cross-validate the assumption of the direct effect of some security and privacy countermeasures on meeting the stated organizational goals (e.g., stated by the standard).

4 Research Method

The goal of this article is to identify the challenges of information security and privacy management in intelligent transportation systems (ITSs). Thus, we (1) define the state-of-the-art measures of information security and privacy management within four dimensions — processes, organizational design, people, and technological solutions; (2) survey the companies to compare their measure of information security and privacy management with the state-of-the-art solutions.

4.1 Literature Review

First, the state-of-the-art measures were defined based on the literature review following the guidelines in [19].

Data sources. The search for literature was performed using the following databases: Scopus, ACM Digital Library, and Web of Science. These databases were selected because they contain peer-reviewed papers and allow to use complex search queries with logical expressions. Another popular database, namely IEEE Xplore, was not used for the literature search as Scopus already contains papers published in IEEE and, therefore, there is no need to use both these databases together.

Search Strategy. For the literature review, we used the following query: ((“security” OR “privacy protection” OR “data protection”) AND (“technologies” OR “measure”)) AND (`Industry_name`), where instead of `Industry_name`, we use “vehicle sharing”, “ride-hailing”, “smart parking”, “toll”, “connected vehicles” and their synonyms. Also, we limit the queries to computer science subject/research areas. The search strategy resulted in 283 papers found (vehicle sharing – 33, ride-sharing – 7, smart parking – 167, toll – 19, connected vehicles – 57).

Inclusion and Exclusion Criteria. To filter out the papers that were selected using the search string but that are not relevant to our research scope, we defined a few inclusion and exclusion criteria (see Table 2). Some of the exclusion criteria were applied to the papers directly in the databases using the corresponding features (e.g., EC1 and EC2)

Table 2. Inclusion and exclusion criteria

Inclusion Criteria	Exclusion Criteria
IC1. the paper discusses information security of an ITS	**EC1.** non-English papers
IC2. the paper discusses at least one method or technique of managing information security or privacy in the ITS	**EC2.** papers published earlier than 2015
IC3. the paper discusses information security issues to be addressed in the field	**EC3.** no full access available
IC4. the paper contains an instance of some attributes from FISP-ProCOP	**EC4.** the paper is a duplicate or an earlier version of another paper

Data extraction. After applying the defined exclusion and inclusion criteria to the queried paper, 24 papers have been selected for the data extraction. From the selected papers, we extract policies, approaches, methods, and techniques for information security and privacy management (referred to later as “measures”). The data from the review is organized in four dimensions (processes, organizational design, people, and technological solutions) based on FISP-ProCOP.

4.2 Survey Research

As the next step, the intelligent transportation sector companies were surveyed using a questionnaire to identify their level of information security and privacy management maturity. The questionnaire was developed using the technologies and measures identified from the literature review.

To define the state of intelligent transportation markets maturity (RQ1), operation areas for ITS (RQ2) which information is manipulated and should be protected in ITSs (RQ3), which information security and privacy standards (RQ4), methods and procedures (RQ5), tools and technologies (RQ6) are used for protecting ITSs, we conducted an exploratory empirical survey study. This method was selected to explore the phenomenon of assuring information security and privacy in intelligent transportation systems and gain insights into how it is done in the operating systems from the perspective of organizations that manage such ITS. We selected a survey with a defined set of

questions for a few reasons. First, it gives the respondents the possibility to answer the question without the restriction in time and allows them to use the help of colleagues or documentation, which contributes to the quality of the obtained data. Second, the questions in the written form can be translated to the respondent's native (or work) language if needed. Finally, the survey is intended to discover the facts about the used measures among the predefined range of options identified from the literature, so there is no need for elaborating questions as for other qualitative empirical research methods like interviews.

Population Selection. As the population of our study, we select the organizations contributing to intelligent transportation systems in two selected regions – Estonia and the South Moravian region in the Czech Republic. The two targeted regions are of similar size in terms of population, economy, and level of digital development, as depicted in Table 3. South Moravia (referred to as "SM") stands as a hub for the ICT industry and education in the Czech Republic, boasting a smart specialization strategy of cybersecurity. South Moravia has the largest concentration of software development companies, SMEs, and start-ups that are producing and developing advanced ICT solutions and technologies in the Czech Republic. Estonia ranks among the world's most advanced digital societies. While Estonia is a target of a range of cyber threats, it is ranked second by the National Cyber Security Index (as of the end of 2023) [4]. According to ICT Development Index (IDI) of 2021 [5] and the digital economy and society index report of 2022 [6], the selected regions have similar scores of digital development in general and in terms of the level of advancement in digital skills, the number of ITC specialists, and digital technology integration, which are the enablers of ITSs development and usage.

Table 3. Comparison of targeted regions' characteristics

Region	**GDP**[1], mln EUR	**Popula-tion**[1], mln	**IDI**[1], score	**DESI assessment**[2]			
				DESI, score	**At least basic digital skills**, % of population	**ICT specialists**, % of population	**Integration of dig.technologies**, score
South Moravia	28.1	1.2	86.1*	49.1*	60*	4.6*	33.8*
Estonia	36	1.3	96.9	56.5	56	6.2	36.5

* - the score was calculated for the Czech Republic overall, not for the SM region specifically,
[1] - based on the data of 2021, [2] - based on the data of 2022

To analyze the threat landscape of the selected regions, we used the national cybersecurity state reports from the national information security agencies that reviewed the cyber incidents that took place in each region in 2022. According to [20], in Czechia, the most common cyberattacks were phishing, external network scanning, and fraudulent e-mails. Within Czech digital services, the majority of incidents targeted the availability of services or data. The most used attacks were scanning, web application attacks, phishing, and denial of service. The report also highlights the trend of the growing interest of malicious attackers in the transportation sector. Meanwhile, in Estonia, the major incidents with an impact were caused by phishing, service interruption, accounts takeover, and fraud [21]. Additionally, the transport and public sectors have been targets of denial of service attacks.

Study Setup. The study setup started by defining the profile of the targeted organization and the profile of the organization's representative. The targeted organizations should contribute to

[4] https://ncsi.ega.ee/country/ee/
[5] https://www.itu.int/hub/publication/d-ind-ict_mdd-2023-2/
[6] https://digital-strategy.ec.europa.eu/en/policies/desi

ITS. Organizations may develop solutions, systems, and/or devices for ITS and/or use intelligent transportation systems for their operations. The set of operation areas which we surveyed can be found in Table 4. Additionally, we were looking for organizations from the following operation areas: (electronic) toll collection, V2X communication, roadside unit operations, and ITS sensors. However, no organizations operating in these four areas and willing to participate in the survey were found in the selected regions.

Table 4. Operation areas of intelligent transportation systems

ITS Area	N_{total}*	N_{EE}*	N_{SM}*	**ITS Area**	N_{total}*	N_{EE}*	N_{SM}*
Connected vehicles	6	2	4	EV charging	2	0	2
Traffic management	6	1	5	Autonomous vehicles	3	3	0
Parking service	5	2	3	Mobility analysis	1	1	0
Vehicle-sharing	3	2	1	Other (ITC services)	1	1	0
Ride-hailing	2	2	0				
Total	$N_{total} = 15;$		$N_{EE} = 8;$	$N_{SM} = 7,$			

where N_{total}, N_{EE}, N_{SM} - number of participants in both regions, in Estonia and in SM respectively;

* some organizations operate in more than one area

The initial pool of targeted organizations consisted of 29 in Estonia and 29 in South Moravia. We used several channels to approach the targeted companies. The invitation emails were sent to the Estonian ITS network [7] mailing list. Other organizations were approached through publicly available emails on the organization's website or using the direct contacts of the project partners in the targeted organizations. Additionally, if no response was received through email after two reminder follow-up emails, we looked for the public email of the targeted organization employees (e.g., using the organization's website or LinkedIn). While the assumption of the study was that the targeted companies are mostly IT companies, and, therefore, most of the employees know English at least on the intermediate level, the emails were sent in two languages - the local language of the region (Czech for South Moravia and Estonian for Estonia) and English. The reason for the bilingual email was the intention to make it more appealing and increase the response rate.

The expected organizations' representatives who would answer the questionnaire should have a good understanding of the IT system (the key functionality and objectives) and be aware of internal organizational realities (incl. policies for the system support). Therefore, we approached people who occupy one of the following positions (or similar roles). In case the organization manages the intelligent transportation system fully or maintains it, the targeted representatives were people in the position of chief technology officer (CTO), product owner/manager/analyst, system analyst, process owner/manager/analyst, software architect, information security officer (ISO), senior developer or system administrator (SysAdmin). In case the organization is a transportation sector representative who does not have their own systems and uses only external systems (e.g., bought solutions or provided under the service-level agreement), the targeted representatives were people in the position of project manager, process owner/manager/analyst, IT manager, information security officer (ISO), chief information officer (CIO). As the questionnaire covers different aspects of the ITS, we expect the representative may need to consult with the system documentation, organizational guidelines, and/or colleagues.

The recruitment processes started on March 10, 2023, in South Moravia, and on March 24, 2023, in Estonia, and we closed the questionnaire on June 1, 2023. To get a more balanced dataset, we conducted the second round of recruitment in South Moravia between September 1, 2023, and

[7] https://its-estonia.com/

October 23, 2023. With a response rate of 24 % and 27 %, we recruited representatives from 7 organizations in South Moravia and 8 in Estonia (15 organizations in total). The distribution of roles of the questionnaire respondents can be found in Table 5, and information about the profile of the surveyed organization is discussed later in Section 6.2.

Table 5. Study participants

Role	Number of respondents	Role	Number of respondents
Software Developer	2	Product Manager	3
DevOps	1	Project Manager	2
ISO	2	Process Manager	1
CTO	2	Operations Specialist	1
SysAdmin	1		

Data Collection and Analysis. Before conducting the survey, we developed a questionnaire [22] based on the main research questions and findings from the prior literature review. The whole questionnaire was in English. Google Forms were used for delivering the survey to respondents as it allowed us to make branching in the questionnaire depending on the answers, making it easier for respondents to navigate. The questionnaire included questions related to general information about the company and its intelligent transportation system (see questions 1.1 – 1.7 in Appendix II related to RQ1, RQ2). The rest of the questionnaire was organized into four parts and roughly aligned to the four dimensions based on the proposed FISP-ProCOP, and, thus, these sections aim to answer RQ3, RQ4, RQ5, and RQ6. Section "Organization" contains questions about organizational design, "Security and Privacy measures. Part 1" covers questions about people, "Security and Privacy measures. Part 2"and "Security and Privacy measures. Part 3" investigates the used technological solutions, while "Security and Privacy measures. Part 4" covers processes and practices. It is noteworthy that the division of questions does not strictly adhere to the framework; however, questions are grouped into logically organized sections aimed at enhancing the interviewee's comprehension. The mapping of the questions with the dimension of the framework can be found in Appendix III. The questionnaire ends with a section of follow-up questions about the survey which contributed to RQ5 and practices used for communicating security and privacy measures to stakeholders (e.g., *Which sources did you use to answer this survey?*, *How easy was it for you to find the information asked in this survey?*).

The respondents were not limited in time for answering the questionnaire. Before distributing the questionnaire to the full pool of targeted companies, we piloted it with three respondents by asking them to provide feedback about the questions (e.g., *Were the questions understandable?, Did any of the questions seem irrelevant?*). The pilot did not reveal the need to update the questions and confirmed its usability for the targeted audience. Thus, it was used for surveying other respondents without any changes.

To analyze the data obtained through the questionnaire, one of the authors reviewed the answers to ensure each entry contained relevant answers, and that the provided information about the organization corresponded to the initially targeted organizations. For the further analysis of answers to each question, from all the data entries are removed the identifiers of the respondents (name, contact information) and the names of the organizations were removed; so each organization was treated equally.

5 Literature Review Results

This section demonstrates how the proposed FISP-ProCOP is used for the data extraction from the literature. As a result of the analysis of extracted sources, we provide an overview of the state-of-the-art aspects of managing security and privacy in intelligent transportation systems. The results are grouped by the sub-types of ITS and the goal of the ITS, key components, stakeholders and processes, challenges of ITS development in information protection, relevant regulations and standards that guide the ITS development and support, as well as the security and privacy countermeasures recommended for ITS. Table 6 contains a set of selected papers used for the data extraction. A detailed report with an overview of smart parking, ride-sharing, connected vehicles, and toll collection is depicted in an external report [23].

Table 6. Literature review papers mapping

ITS area	Papers included in the literature review
Smart Parking	[3], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33], [34], [35]
Ride-Sharing	[36], [37]
Connected Vehicles	[4], [38], [39]
Toll Collection	[5], [25], [40], [41], [42], [43]

Our study shows that the research intensity varies from one operation area of intelligent transportation to another, and, for instance, smart parking is the most researched compared to others. Thus, the results for some operation areas are less complete with respect to the used reference model compared to others. When presenting the review results, the missed dimensions or attributes for the operation area mean that we did not find the respective data in the selected literature. Also, we do not include the architectural or technical measures which primarily deliver the main system functionality and do not significantly affect information security or privacy in the ITS.

The aggregated results of the literature review are depicted with respect to the proposed FISP-ProCOP model in Appendix I. The tables in the appendix depict the state-of-the-art measures of information security and privacy management in intelligent transportation systems. However, the state-of-the-art measures are missing for some of the categories and attributes for the dimensions of People and Organisations. The reason is that we were not able to systematically extract them based on the literature review, and the level of detail for the missed attributes differs across papers and operation areas of ITS.

The literature review shows that within ITSs, the information assets to be protected are related to the information about a vehicle, driver and passenger, and transportation service usage. For instance, in systems for smart parking, ride-sharing, and vehicle-to-vehicle communication, the confidentiality of passenger's/driver's data is of primary security concern, along with assuring the availability and integrity of parking slots usage data. Therefore, the state-of-the-art measure for ITSs security management includes mitigating threats that negate the integrity of the parking slots payments status [27] to enable public verifiability (e.g., by the parking officer), which can be abused by the driver's motive for payment avoidance (e.g., harvesting attack). A significant amount of studies also aim to mitigate the threats to negating the confidentiality of passengers' or drivers' personal data caused by the storage of such data in a centralized manner by the service providers. Additionally, the reviewed studies aim to mitigate the threat of violating passengers' or drivers' privacy by linking the data instances of service usage or payment history. More details on motives and level of trust in the actors (which are mentioned in Table A2), along with other security threats the reviewed papers aim to mitigate, can be found in the supplementary report in [23].

6 Survey Research Results

Here, we present the results of our survey study. The results present a comparison of two regions – South Moravia and Estonia – with state-of-the-art measures affecting information security and privacy management. Figure 3 gives a high-level view of the survey results depicting the usage attributes in FISP-ProCOP by the surveyed organizations. The attributes in the figure are the ones identified through the literature review (in black text) and other measures identified through the questionnaire (in dark grey text). For instance, in the attribute CT Architectural Measures, such attribute instances as "multi-party computation" and "blockchain-based system" are the measures identified through the literature review, and they are written in black in the table. Meanwhile, for the same attribute, the instance "storage of annotated data" is taken from the questionnaire option, which is not mentioned in the literature and, thus, it is written in Table in grey color. The distribution of attribute usage is color-coded so that the red marked cells represent the least used attributes, the white – used on average, and the green – the most used (the scale for the color-coding is in Figure 3). For instance, in the attribute "CT Architectural Measures", such attribute instance as "multi-party computation" is marked by the dark red cell color, which means 0 responses in the survey support this measure; while "anonymous authentication" is colored in white refers to 3 respondents in the survey who mentioned it as used in their organization. Finally, "securing data in transit" is the most mentioned among attribute instances, and thus, its cell is colored green. In this section, we describe the depicted distribution, while our report in [23] contains additional survey results. The titles of sub-sections in Figure 3 correspond to the categories in the used framework (Table 1).

6.1 Findings from Study Setup Phase

The selected regions have a similar number of companies operating with ITSs. Noteworthy is the existence of ITS networks in both regions. In Estonia, an ITS network unites the intelligent transportation and logistic systems (ITS) community [8] and in South Moravia, there is a Czech network of Intelligent transportation systems & services (ITS&S) [9]. However, while in both of the regions, ITS are in the development phase, the networks cover the number of organizations that do not develop or maintain ITS but are interested in collaboration with ITS-oriented organizations. For instance, the network includes members who provide general IT services, mapping solutions, or network solutions that could be used as a part of ITS or for its setup.

6.2 Operation Area of ITSs

The distribution of operation areas for the surveyed organizations is depicted in Figure 4. The results show that most of the surveyed organizations use ITSs for traffic management (6 out of 15), for operating connected vehicles (6 out of 15), and/or for smart parking (5 out of 15). Among 8 organizations from Estonia, 3 organizations use ITSs to operate autonomous vehicles, and 2 organizations operate in the following areas: smart parking, vehicle sharing, connected vehicles, and ride-hailing. None of the surveyed organizations in Estonia operates in EV charging. As for organizations in South Moravia, 6 out of 7 organizations use ITSs for traffic management (3 of which are also using ITSs for connected vehicles). None of the surveyed organizations in South Moravia are involved in autonomous vehicle operation, ride-hailing, mobility analysis, or providing ICT services. Finally, only 4 of the surveyed organizations' ITSs are used exclusively for one operation area, while others' ITSs are used in 2 areas (6 out of 15) or even 3 areas (4 out of 15).

[8] https://its-estonia.com/

[9] http://www.sdt.cz/

Dimension	Category	Attribute	Attribute instances										
P. People	PA (Actors)	PA	Time-stamping authority	Defence	Parking/Toll Officer	Trusted Authority	Passenger	Parking Service Provider	System provider	Employee	City Government	Driver	
O. Organi-zation	OS (Strategy)	OS System purpose	Safety of urban traffic	Reduced cost for goods delivery	More livable cities	Improved parking facilities	Public transport control	Decreased the traffic congestion	Improved city services	On-demand mobility			
		OS Challenges	Heterogeneous network	Resource constrained devices	High system quality expectations	Privacy vs efficiency	User data privacy and security	Data minimisation	Expected level of security	Lack of industry regulations	Interoperability		
	OC (Formal Constraints)	OC regulations	EU 2019/2144	EU 2018/858	ITS Directive	UN R155	GDPR						
		OC standards	NIST SP	Other standards from ISO/IEC 27000-series	E-ITS	ETSI standards series	Cyber Security Act in Czechia	ISO 27001					
	OI (Information types)	OI	Information about roadside units	Other information	Information about passenger	Information about transactions	Aggregated information	Information about driver	Information about vehicle				
C. Sec. & Privacy Counter-measures	CP (Practicies & Policies)	CP	Normal best practices	Penetration testing	Threat modelling	Security Development Lifecycle	Risk management	Security framework	Security strategy				
	CE (Training & Education)	CE Trainings Employees	Reading news about security isues	Cyber hygiene trainings	Trainings for raising awareness about security threats	Data protection trainings							
		CE Sources For Survey	Documentation	Colleagues	Knowledge of the organisation	Knowledge of the system							
	CT (Technology)	CT Crypto	Homomorphic encryption	Zero- Knowledge Proof	Oblivious pseudorandom function (OPRF)	Blind signature	Oblivious transfer protocol	Trusted execution environment (TEE)	Private set intersection (PSI)	Hash-based message authent. codes	Elliptic curve cryptography	Diffie-Hellman group key exchange	RSA digital signature
		CT Secure Communication	Custom asymmetric encryption	IPSec protocol	Other secured communication protocol	Customer end-to-end encryption	VPN solution	TLS protocol					
		CT Architectural Measures	Blockchain- based system	Multi-party computation (MPC)	Storage of anotated data	Secret-sharing	Anonymous authentication	Storage of personal data on the data subject device	Securing data in transit				
		CT Authent. & Access Control	Biometric- based authentication	Pseudo- random identity assignment	Anonymous credential system	Attribute-based credentials and access control	RFID authenti-cation	2-factor authentication	Role-based access control	Public Key Infrastructure			
		CT UC Navigation & Routing	Location obfuscation	Third-party navigation system	Privacy- preserving navigation systems								
		CT UC Payment	Anonymous payment	Automated payment using smart contract	Cash	Direct carrier billing (DCB)	Token-based payment	Card-based payment					
		CT UC Location Based Search	Private information retrieval	Hashmap storing of parking slot/toll/vehicle locations	Search based on the exact location								
		CT UC Reserv. Document Creation	Blind signature	Anonymous reservation	Presenting proof-of-knowledge								
Pr. Proc-esses	PrL (System Lifecycle)	PrL Principles for System Development	Privacy-related testing and verification	Usage of sensor devices which have built-in security measures	Data minimisation	Secure programming	Privacy by design						
		PrL System Support Networkt	Firewall	VLANs	Security incident and event management systems (SEIM)	Intrusion detection system	Behavioural analytics system	Vulnerability scanner	Network traffic analyser				
	PrU (Usage of the System)	PrU Use Cases	Pass/reservation document creation	Navigation or routing	Payment	Location-based search							

Cell colour mapping: 0 3 6 14
(by number of supporting responses)

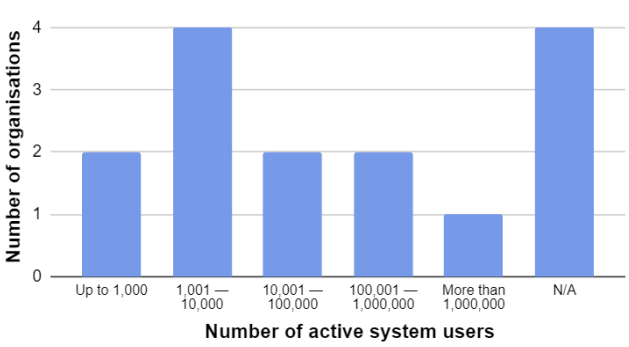
Text colour mapping: **measure1 (black)** - state-of-the-art measure
measure2 (grey) - other

Figure 3. Distribution of the usage of the measure by the surveyed organizations

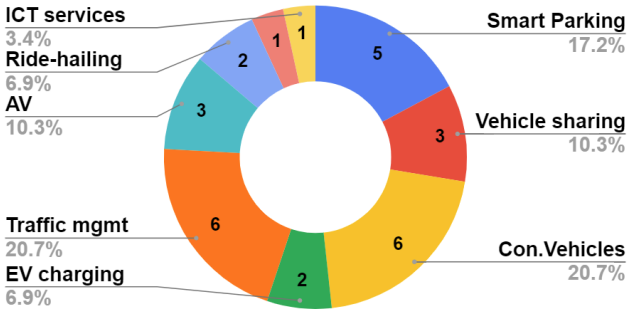
6.3 Actors

To identify the sources of human-related security and privacy aspects, we asked the respondents about the stakeholders of their products and services of the intelligent transportation system. We consider "individuals, groups or organizations whose actions can influence or be influenced by the development and use of the system whether directly or indirectly" [44] as stakeholders.

As a significant share of the surveyed organizations operates with connected vehicles, a driver is the most mentioned stakeholder (8 out of 15). All the organizations (except for one) that operate with connected vehicles consider drivers to be stakeholders. The second most mentioned stakeholder is presented by the city government (7 out of 15), followed by external system providers (under a service-level agreement) and internal organization employees (5 out of 15). The next ones are a parking service provider, trusted authority, and passenger (3 out of 15). Time-stamping authority, parking or toll officer, and a defense agency were indicated only by one organization each.



(a) Number of active ITS users



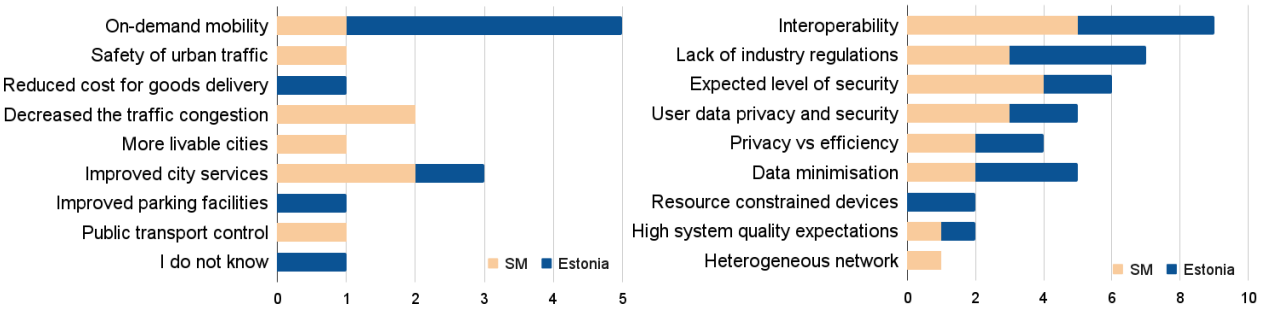
(b) Operation areas (some organizations operate in more than one area)

Figure 4. Overview of the surveyed organizations

6.4 Organizational Objectives, Strategy, and Challenges

To understand the strategies of surveyed organizations about their ITSs, we asked respondents about the purposes of their ITSs and the challenges they face during the usage, development, and support of the ITSs. The study shows that five of the surveyed organizations enable on-demand mobility, and three aim to improve city services. Only two aim to decrease traffic congestion. Other ITSs aim to improve safety or urban traffic, reduce the cost of goods delivery, improve parking facilities, or make cities more livable overall (incl. environmental state). On the way to achieving its purposes, most organizations face the challenges of being interoperable with other systems and/or providers (9 out of 15) and perceive the lack of industry regulations and/or standards (7 out of 15). Notably, interoperability is a challenge for organizations which has a varying number of external system integrations (1-2 external systems or more than 5), which means that it is a challenging task for more advanced and complex ITSs as much as for smaller ones. Fewer organizations are challenged by the expected level of security (highlighted by 6 out of 15 respondents), addressing user data privacy, security, and data minimization (5 out of 15). Even fewer respondents point out that ensuring the balance between privacy and efficiency of the system is challenging for the organization. Finally, 10 out of 15 organizations deal with at least 3 of the challenges mentioned in the survey.

Information Used in ITSs. In order to achieve its objectives while being constrained by the challenges, let us have a look at what kind of information is manipulated in intelligent transportation systems (see RQ3). Overall, the information can be grouped into seven groups: related to vehicle, driver, parking/ride/toll, passenger, roadside ITS components, aggregated,



(a) Purpose of ITS **(b)** Challenges for ITS

Figure 5. Overview of the surveyed organizations

and other (internally used data about the platform or environment). Vehicle-related information is mostly manipulated (by 11 out of 15 organizations) and includes the vehicle's location, state details, identity, and speed of surrounding vehicles. Driver-, parking/ride/toll-related, and aggregated information are the second most manipulated by the surveyed organizations (7 out of 15). Driver-related information includes data about the driver's identity, location, transactions, and payment details. Parking/ride/toll-related information includes data about available parking spaces or tolls, parking/ride/toll-transactions, and such information is naturally collected by organizations that operate with smart parking, ride-hailing, and EV charging. Aggregated data based on the transaction history is manipulated by almost the same organizations that operate with parking/ride/toll transactions. Passenger-related information includes data about passengers' identity, transactions, payments, or anonymous transaction validation and is manipulated only by three organizations that conduct either traffic management or ride-hailing. Information about roadside ITS units (incl. traffic lights) is used only by two organizations that operate with connected vehicles. Other kinds of information about the environment are manipulated only by two organizations that operate with autonomous vehicles or mobility analysis.

OC. Standards and Regulations. The questions about regulations and standards are among the least answered (5 and 4 out of 15 respondents answered "I don't know" to the respective questions). The respondents who could not answer the questions occupy exclusively technical positions (software developers, CTO, SysAdmin, and operations specialist). Ten responses mentioned among them six security- or privacy-related regulations which affect the surveyed organizations: European *General Data Protection Regulation (GDPR)* [45], European *ITS Directive* [6], United Nations Regulation *UN R155* [46], European Regulations *EU 2019/2144* [47] and *EU 2018/858* [48], and *NIS2 directive* [49] (which is also a European regulation). GDPR affects all the respondents (both in South Moravia and Estonia). UN R155 is mentioned by three organizations (in total, from South Moravia and Estonia). The regulations EU 2019/2144 and EU 2018/858 are highlighted by only one Estonian company. The NIS2 directive is also mentioned by only one organization from South Moravia. It is interesting to note that only respondents occupying positions that require an overall view of the system and its infrastructure (as an information security officer and DevOps) highlight regulations other than GDPR (which is known to a broader audience).

There are six security standards followed by the surveyed organisations: *Předpis 181/2014 Sb. (Zákon o kybernetické bezpečnosti)* (Cyber Security Act in Czechia), *ISO/IEC 27001*, *other standards from ISO/IEC 27000-series*, *ETSI standards series* [10], *Eesti infoturbestandard* (Estonian Information Security Standard, E-ITS), and *NIST Special Publications* (NIST SP) [11]. Cyber

[10] The respondents were asked about usage of any of the following ETSI technical specifications (of category – Intelligent Transport Systems (ITS); Security): ETSI TS 102 941 (on trust and privacy management), 102 731 (on security services and architecture), 103 097 (on security header and certificate formats).

[11] The respondents were asked about NIST SP 800-39 and NIST SP 800-37.

Security Act in Czechia is mentioned by 4 out of 7 of the surveyed organizations in South Moravia (while one company from South Moravia claims that no standards apply to them). In South Moravia, 6 out of 7 organizations follow ISO/IEC 27001, and 5 out of 7 follow ETSI standards. One South Moravian organization also follows NIST SP (probably due to operating globally, including in the United States). Among Estonian organizations (representatives of which were able to provide the answer), ISO/IEC 27001 is the main security standard followed by 3 out of 4 organizations. One organization in Estonia follows only E-ITS, which is compatible with ISO/IEC 27001.

6.5 Countermeasures to Assure Information Security and Privacy Assurance

Here, we discuss the results of using direct countermeasures for assuring information security and privacy. The countermeasures are divided into three groups – organizational policies and practices, people-oriented training and education, and technological measures.

CP. Policies & Practices. There are six practices used by the surveyed organizations: penetration testing, following a selected risk management framework, following a selected security framework, following a national (cyber) security strategy, threat modeling, and security development lifecycle. Overall, in the selected regions, following a selected risk management framework and security framework along with a national (cyber) security strategy are the most used (6 out of 15). Comparing the two regions, South Moravian companies are leading in terms of the number of used organizational countermeasures.

In addition to the mentioned security and privacy practices, we studied principles used during the ITS development and support activities. Secure programming and privacy by design are the most commonly used across the surveyed organizations (5 out of 15). However, the prevalence of principles differs from region to region. For instance, data minimization is as much used in Estonia as secure programming (3 out of 8 Estonian companies), while data minimization is used by only one South Moravian organization. In contrast, privacy by design is the most used principle in South Moravia (4 out of 7). In Estonia, privacy by design, privacy-related testing and verification, and usage of sensor devices that have built-in security measures are scarce (1 out of 8). Moreover, 2 out of 8 Estonian organizations indicated not using any of the proposed (or similar) principles.

Self-assessment of the ITS security level resulted in the consensus among South Moravian respondents in assessing their ITSs as “secure, but could be improved”. While 3 of 8 Estonian organizations consider their ITS “somewhat secure, should be improved”, another 4 (out of 8) assess their ITSs as “secure, but could be improved”. Finally, one Estonian organization seems to have either better practices of security or better communication with employees, so the representative indicates that their ITS is “secured according to up-to-date measures and considering relevant threats”.

Finally, 5 out of 15 respondents indicated that to answer the questionnaire, they used documentation (e.g., manuals, guidelines, technical documentation) or consulted with colleagues, while others used only their personal knowledge of the system and/or organization. Thus, the study shows that overall, the level of awareness about security and privacy in South Moravia and Estonia and the level of communication of the relevant knowledge is quite high with respect to the provided answers.

CE. Educational Measures and Trainings. As the organization’s employees and intelligent transportation system users are the most numerous groups of stakeholders, in our study, we asked respondents about security and privacy training established for these two stakeholder groups.

Similarly to the situation with policies, the practice of security and privacy-related training for end users is more established among South Moravian organizations. Almost all South Moravian representatives (except for one) indicated introducing the privacy policy during the first onboarding to the system; four representatives also mentioned regular reminders and/or introducing the

information security measure. Additionally, two organizations teach system users to recognize phishing. Meanwhile, 2 out of 6 Estonian organizations indicate that they do not conduct any training for system users. All other Estonian organizations educate users about their privacy policy. Only one introduces the security features of the system that concern their personal data to explain to users how their privacy is protected.

In our study, we mentioned three kinds of training for employees – data protection training (related to data privacy), training for raising awareness about security threats, and cyber hygiene training. Overall, data protection training and training for raising awareness about security threats are the most used types for educating organizations' employees. The representatives of South Moravian organizations mentioned at least one training type per organization. Two of the Estonian organizations mentioned that they do not have any training in place. Cyber hygiene training is less popular in South Moravia (3 out of 7) than in Estonia (3 out of 8). Also, one Estonian organization mentioned reading news about security issues as a type of education for employees.

CT. Technological Countermeasures. The questions in the study about technological countermeasures were based on the state-of-the-art measures found during the literature review. Additionally, the answer options are populated with more commonly used, not state-of-the-art, ITS measures to capture at least any data for maturing ITSs.

CT.1. Architectural Measures. The most commonly used architectural countermeasures across regions are securing data in transit, followed by storing sensitive personal data on the data subject device, anonymous authentication, and, finally, secret-sharing. None of the respondents indicated using blockchain-based systems or multi-party computation (MPC) in their ITSs. All the respondents indicated using at least one of the mentioned architectural measures, while some highlighted using two or three measures per organization (two organizations in South Moravia and one – in Estonia).

CT.2. Use Case-Oriented Measures. For the use case-oriented measures, except for the state-of-the-art ones mentioned in Appendix I, the questionnaire includes the options of more commonly used measures. The results show that only around half of the organizations have the functionality of navigation and routing, payment, and/or location-based search, while none of the surveyed organizations' ITSs created a reservation or passes documents. As shown in Figure 3, the state-of-the-art measures are not used (or are used by one organization only).

CT.3. Cryptographic Measures. The question about cryptographic measures was as challenging as the one about security practices and policies (7 out of 15 respondents could not answer the question). Among 3 South Moravian organizations, there is no clear preferences for cryptographic measures. RSA digital signature is used by 2 organizations (2 out of 3 respondents who were able to answer). Trusted execution environment (TEE), private set intersection (PSI), elliptic curve cryptography, Diffie-Hellman group key exchange, and hash-based message authentication codes are equally used. In Estonia, RSA signature is a clearly leading measure (used by 3 out of 4 respondents), followed by Diffie-Hellman group key exchange (2 out of 4) and elliptic curve cryptography (1 out of 4). The results show that none of the other state-of-the-art measures are used.

6.6 Processes

Here, we present the results of the study about the processes in organizations related to the intelligent transportation system lifecycle and support.

Most of the surveyed organizations have a development team that is fully responsible for the system, its support and development (11 out of 15) and, thus, holds the sole responsibility and control over the ITS. Only 2 out of 15 organizations have a small development/support team who in-house manage the system developed by an external service provider. And only one company out

of 15 uses a ready-to-use solution, which the system provider continuously updates. Thus, in both South Moravia and Estonia, ITSs are rather centralized and managed mainly by one organization (i.e., owner) rather than used as a service or managed collaboratively.

As the involvement in the system lifecycle does not differ much across the organizations, we cannot conclude that it affects the dynamics of the systems (i.e., how much the system changes over time). Across the regions during the last 5 years, 27% of organizations (4 out of 15) have a new system that has been developed separately from the old system, and as many organizations (4 out of 15) made significant changes in the system and its components. Even though a major part of the organizations highlighted interoperability as a challenging task, no organizations had to make major changes in the system and its components due to the integration with external system(s). Another 20% of organizations (3 out of 15) make minor changes to the main functionality and actively support the existing system. Only 20% of organizations (3 out of 15) make major changes to the main functionality and actively support and develop the existing system. Finally, none of the respondents indicated that their ITS had not changed at all during the last 5 years, which confirms the fact that ITSs are in the active development phase and are still establishing in the selected regions (which is also highlighted by the respectively low number of active organizations on the market). Comparing the dynamics of ITSs in regions, the results show that, in South Moravia, organizations tend to develop a new system separately from the old system (3 out of 7 in South Moravia over 2 out of 8 in Estonia).

The research on how security and privacy assurance are integrated into the existing process is the major interest of our study. The results show that a significant part of organizations in the surveyed regions update their ITS regularly with ad-hoc security patches (6 out of 15) or security patches (4 out of 15). Based on this, we conclude that such organizations have an average level of security integration in the system lifecycle.

With regard to system support, we focused on network security measures in the study. The presented options were the following: intrusion detection system, security incident and event management systems (SIEM), behavioral analytics system, network traffic analyzer, and vulnerability scanner. More than half of the representatives (9 out of 15) indicated this type of measure either as not applicable or could not provide an answer. Among the given answers, the network traffic analyzer is the most used measure (5 out of 15). Intrusion detection systems, behavioral analytics systems, and vulnerability scanners are equally used by 3 out of 15 respondents. Two organizations use security incident and event management systems. Also, one organization uses firewalls and VLANs. All of the answers indicate that if organizations opt for using network protection, they use at least two different measures for that. Also, as firewalls were not mentioned as an option in the survey, we assume that there may be more than one organization among the sample that uses firewalls for network protection. However, we acknowledge that the respondents might not have mentioned some of the used measures (including firewalls) due to not being willing to provide such sensitive details or not being aware of their usage.

6.7 Other Findings Based on the Study Results

While employees of exclusively technical positions did not answer the questions about security and privacy-related regulations and standards, we conclude that there is a lack of information security countermeasures for security policies and training which would communicate to all the stakeholders existing organizational limitations in terms of regulations and/or training on this matter.

The results show that ITSs commonly rely on some trusted party, whether for coordination or identity handling. Meanwhile, public key infrastructure (PKI), together with role-based access control (RBAC), are the most common tools for ITSs to control access to exchanged data by securing data in transit.

Finally, while some of the organizations are certified with respect to the ISO/IEC 27001 standard (or aim to be certified), which guides information security management, none of the respondents

mentioned using the standard ISO/IEC 27701 for privacy information management. The review of the surveyed organizations' official websites confirmed that none of them are certified with respect to ISO/IEC 27701. Thus, we conclude that organizations operating in ITSs within Estonia and South Moravia are not as rigorous about privacy management as about security management.

Statistical Analysis. We analyze the data to determine whether there are any dependencies between the usage of different information security and privacy measures based on the survey results. Each survey answer provided by an organization representative is considered a separate data entry. Each question in the survey contains a limited set of answers. Therefore, each measure about which it was asked in the survey corresponds to a categorical (nominal or ordinal) data variable. An example of an ordinal variable is the level of security integration into the system lifecycle. An example of a nominal variable is the region of operation or respondent's position. As a result, each data entry consists of a set of categorical variables. During the data preparation, some nominal categorical variables were split into a set of variables so that each variable describes a single answer, not a set nominal value. For instance, while in the original dataset, there is one variable corresponding to challenges faced by a company and the value is a set of challenges, in the analyzed dataset, we split each challenge into a separate variable (e.g., `chall_HighQualExpect` and `chall_Heterogeneous`) which describes the fact of presence (value=1) or absence (value=0) of the challenge for the organization.[12]

As the dataset consists of categorical and ordinal data, we use Spearman's rank correlation coefficient (r_s), which measures a monotonic association between two variables [50]. Table 7 describes variables with statistically significant high correlation coefficients with significance level p-value$\leq$0.05.

Table 7. Correlation between variables collected through the survey (p-value ≤ 0.05)

Variable 1	Variable 1 description	Variable 2	Variable 2 description	r_s
practices Policies_5	Used practice and policy: Threat modelling	practices Policies_6	Followed practice and policy: Security Development Lifecycle	1
chall_HighQual Expect	Challenge: High expectations from ITS quality	Pr_systemSupport _network_2	Followed system support practice: SIEM system	1
stakeholders_1	Stakeholder: Trusted Authority	practices Policies_1	Followed practice and policy: Penetration testing	1
architMeasures_2	Arhitectural measure: Anonymous authentication	C_authent AccessControl_8	Authentication measure: Anonymous credential system	1
hasPayment	Has payment	C_UC_payment_1	Card-based payment	0.866
practices Policies_3	Used practice and policy: Selected security framework	trainings Employees_2	Trainings for raising awareness about security threats	0.873
C_secure Communication_5	Customer end-to-end encryption	P_principles_system Development_2	Privacy by design	0.853

The strongest correlation (r_s=1) is found between the three variable pairs. The first correlation corresponds to the causation: `policy_6` (Security Development Lifecycle) causes `policy_5` (Threat model), as threat modeling is the mandatory building block of the Security Development Lifecycle. The strong correlation between having a challenge of high expectations from ITS quality

[12] The list of analyzed variables and their mapping to the survey questions, together with the full list of significant correlation values, can be found in the report [23].

(chall_HighQualExpect) and the practice of using security incident and event management systems (SIEM, Pr_systemSupport_network_2) can be explained by the fact that SIEM helps to improve ITS quality and supports maintaining system security during incidents. Finally, the correlation between having Trusted Authority (stakeholders_1) as a stakeholder and using penetration testing (practicesPolicies_1) may refer to the organization's awareness of security vulnerabilities, which may originate from internal management of the system (incl. identity management and system development). Thus, such organizations acknowledge both the need to review their system with penetration testing and outsourcing identity management to a Trusted Authority.

A weaker correlation ($0.85<r_s\leq 0.95$) is found between three variable pairs. First, as we pointed out before, almost all the organizations having payment functionality use a card-based payment method (r_s=0.86), which may refer to the need to have its payment option when having an intelligent transportation system in the selected regions. Second, the strong correlation between end-to-end encryption and privacy by design is expected, as using end-to-end encryption is one of the foundational principles of privacy by design. Therefore, r_s=1 is expected to be present to characterize the causation. Not having causation in the dataset questions the correctness of the answers of some respondents. So, either the organizations claim to assure privacy by design but do not follow all its principles, or there is a lack of respondents' awareness about the privacy practices they follow. Third, the correlation between the usage of a selected security framework (practicesPolicies_3) and training for raising awareness about security threats (trainingsEmployees_2) confirms the actual usage of some security frameworks by the respondents as usually such frameworks (e.g., NIST cybersecurity framework [12]) prescribe training employees about security risks and threats.

To sum up, the statistical data analysis of the survey dataset shows that the used reference model of information security and privacy assurance in the intelligent systems (Table 1) can depict cross-dimensional dependencies between the categories of information security and privacy measures. As a result, the frameworks can be used to cross-check the implementation of the measures across different aspects of organizations.

7 Recommendations

Based on the literature review results and the survey in Estonia and South Moravia, we formulate a set of recommendations for the organizations involved in developing and supporting intelligent transportation systems in these regions:

1. **Conduct regular internal training about the security goals and practices aligning those with the organizations' goals, strategies, stakeholders, and their interests in an ITS**. The study shows that process, project, and product managers, to a large extent, are unaware of the ITS security and privacy level. Such training should highlight the stakeholders' roles and manage their interests as a part of information security and privacy management. The reason is that our study shows that almost half of the representatives of organizations that manipulate driver-related data do not consider the driver as a stakeholder, and none of the representatives who indicated manipulation of passenger-related data consider the passenger a stakeholder. We believe that such results may be either a sign of a lack of representatives' awareness about the situation or a sign of neglecting actors and their interests regardless of using their data.
2. **Design an ITS considering the need for interoperability with external systems and partners from day zero**. The study shows that on the way to achieving their purposes, most organizations face the challenges of making their system interoperable with external systems. Thus, organizations should develop ITS considering the requirements for data, services, and infrastructure interoperability [51].

3. **Provide employees in technical positions with the requirements for ITSs which are aligned with relevant regulations and standards by a product manager, national organization of ITSs, and national government (e.g., in the form of strategies or regulations for the transportation sector)**. The study shows that people involved in ITSs engineering may not be aware of the regulations and standards followed by their organisation (based on their answers to the questions about regulations and standards).
4. **When developing an ITS, consider the usage of state-of-the-art measures from academic publications**. Based on the study results, organizations developing ITS mostly do not use state-of-the-art security and privacy measures proposed in academic papers.
5. **Collaborate with the research institutions which would help to navigate with the state-of-the-art security and privacy countermeasures**.
6. **Strengthen collaboration between organizations developing ITSs and research and education institutions to increase awareness of the state-of-the-art measures of information security and privacy management**. The mentioned collaboration could be facilitated, for instance, by the effort of existing ITS community or networks.

8 Related Work

As we see from the literature review (Section 5), the existing works (e.g., [29], [4]) on information security and privacy management focus on one selected operation area of ITSs and either propose new or review the existing technical countermeasures for ITSs. The closest work to this paper is by Hahn et al. [52], as it provides an overview of security and privacy challenges for ITSs in general. However, the findings are based only on the literature review. At the same time, in our work, we validate the relevance of the challenges from the literature and check the usage of state-of-the-art measures in running ITSs. In contrast, in this article, we conducted a secondary study on the InfoSec & PM measures and compared the results with the measures used in real-life ITSs. Thus, our study is not a survey per se but also presents results of the intelligent transportation industry assessment in Estonia and South Moravia.

In [53], Boccardo et al. propose an information security maturity assessment method. The method is based on CIS Controls to assess the usage of security controls for the steps of security risk management following NIST CSF and to which category of BMIS the controls belong. However, in this work, authors omit the category of organisation-related measures. In [54], Seeba et al. propose a framework for security level evaluation (F4SLE) that assesses organizations with respect to the Estonian Information Security Standard (E-ITS) as a baseline. Similarly, in this article, we propose a framework for qualitative assessment of the measures' usage. However, we do not restrict the assessment to CIS Controls and conduct the specialized gathering of the baseline state-of-the-art measures using a literature review for the selected system operation area (i.e. transportation). Also, our work aims to define the challenges and gaps of securing information within ITSs, in general, to provide recommendations for practitioners and policymakers, while both [53] and [54] should become a tool for assessing each organization separately.

9 Limitations

9.1 Limitations of FISP-ProCOP

The proposed FISP-ProCOP is aimed to depict the static picture of the aspects contributing to information security and privacy management, not capturing the dependencies between them. As a result, its primary application is as an instrument for depicting the state of the organization, which later on can be used as an input for the dependencies analysis as presented in Section 6.7. The main limitation of the proposed framework is that it only depicts a static and high-level picture of security- and privacy-related factors. Thus, FISP-ProCOP cannot explain why each element

instantiation is present or how each attribute instance is connected with another; e.g., while the framework captures the countermeasures used to protect information assets and actors, the threats or vulnerabilities related to these elements are not included in the framework. Thus, in the case of FISP-ProCOP usage for the survey study in the regions, we classified "VPN solution" as a measure of securing communication-based on the survey question-answer. At the same time, the organization using the framework may need to put this measure under another attribute within the CT category of FISP-ProCOP. To mitigate the limitation of the static picture and lack of dependency and reasoning between the attribute instances, an organization may add an attribute of "Threats and vulnerabilities" under the category of "OI. Information Involved" to reflect threats to the identified information used in the ITS. Each defined threat and vulnerability can be used as a defining use case attribute under the category of "CT. Technology".

As FISP-ProCOP is developed based on the current state of system development and, considering the security frameworks used at the time of its development, the framework lacks the accompanying procedure and conditions of its update. To reflect the evolution of ITS technologies and emerging security threats, organizations using the framework may extend the attributes of the specified categories based on their needs until the procedure of updating FISP-ProCOP is developed.

9.2 Threats to Validity

The usability of the proposed framework is validated through two empirical studies – the literature review and survey – by the same person (the article's first author). Thus, we do not have an evaluation of how easy the framework is for an external audience to use. While the response rate to the survey is 24% in South Moravia and 27% in Estonia, the limited sample size makes the results such that they cannot be generalized to the whole population (i.e., ITS-related organizations in Estonia and South Moravia). Due to this, our recommendations in Section 7 are primarily for the surveyed region and depict conclusions made based on the observations and comparison of the survey and literature review results. Finally, the presented results of the empirical studies are limited to the selected inclusion and exclusion criteria of the studied subjects. Thus, the recommendations are targeted to the selected regions (Estonia and South Moravia) and should not be generalized to other regions.

Due to the limited scope of FISP-ProCOP, the survey study does not provide data on the threats that organizations are mitigating through countermeasures. Thus, the numeric results of using one or another technology or practice cannot be used to conclude the efficiency of the countermeasures or the need for others to use them unconditionally. On the other hand, such statistics provide insight into the technological stack used per region. As a result, the country policymakers and the organization's management can understand the technological stack their employees might need.

10 Concluding Remarks

This paper has investigated how information security and privacy are managed in the context of intelligent transportation systems. The study's contribution is three-fold. First, we developed a framework for information security and privacy management (FISP-ProCOP). Second, we showed through two studies how the proposed FISP-ProCOP used as a theoretical model for the empirical study helps to depict the aspects contributing to information security and privacy management (InfoSec & PM) in an organization that uses an intelligent system (e.g., the intelligent transportation system (ITS)). Third, the two empirical studies resulted in defined state-of-the-art measures for InfoSec & PM for ITSs and the distribution of their usage by the organizations in South Moravia (Czech Republic) and Estonia. The study also showed that the proposed FISP-ProCOP depicts some dependencies between measures, and, thus, using its matrix structure for the state of InfoSec & PM in the organization helps to cross-check the usage of policies or methodologies by the organization departments. Finally, the study results show that the state-of-the-art measures

recommended for assuring information security and privacy in the literature are not used by the operating organizations in the selected regions. One of the reasons for this might be the major orientation of the academic research on the technological countermeasure and not much focus on how these measures fit into the organizational structure and the existing processes. Based on the results of the empirical studies, we defined recommendations for organizations developing or supporting ITSs in Estonia and South Moravia on how to support their information security and privacy management.

In future work, we will validate the usability of the proposed framework by asking the information security or privacy experts to use FISP-ProCOP to depict the state of the organizations they work for. Additionally, to improve the usability of the framework, we plan to create a supplementary tool for analyzing data extracted through the framework. As the next step, we will validate the recommendations created based on the empirical studies through interviews with the local information security authorities and by comparing our recommendations with the regional security and privacy strategies for the transportation sector. Finally, future work should specify the conditions and a procedure for updating the framework in order to capture the continuous evolution of intelligent transportation systems and emerging security threats.

Acknowledgements

The authors are grateful to Hendrik Pillmann from the Information System Authority (RIA) and Liina Kamm from Cybernetica AS for their support during the study execution and whose critical comments helped improve the article. Also, the authors would like to thank reviewers for helpful comments contributing to significant article improvements.
This article is supported by the European Union under Grant Agreement No. 101087529.

References

[1] Council of the European Union, "Council adopts new framework to boost the roll-out of intelligent transport systems," Available: https://www.consilium.europa.eu/en/press/press-releases/2023/10/23/council-adopts-new-framework-to-boost-the-roll-out-of-intelligent-transport-systems/, 2023.

[2] European Commission, "Directive (EU) 2023/2661 of the European Parliament and of the Council of 22 November 2023 amending Directive 2010/40/EU on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport," Available: https://eur-lex.europa.eu/eli/dir/2023/2661/oj, 2023.

[3] R. Borges and F. Sebé, "An Efficient Privacy-Preserving Pay-by-Phone System for Regulated Parking Areas," *International Journal of Information Security*, vol. 20, no. 5, pp. 715–727, Oct. 2021, Available: https://doi.org/10.1007/s10207-020-00527-2

[4] W. Chen, H. Wu, X. Chen, and J. Chen, A Review of Research on Privacy Protection of Internet of Vehicles Based on Blockchain," *Journal of Sensor and Actuator Networks*, vol. 11, no. 4, 2022, Available: https://doi.org/10.3390/jsan11040086

[5] N. Sathyanarayana, "A Survey on Vehicle Detection and Classification for Electronic Toll Collection Applications," in *Distributed Computing and Optimization Techniques: Select Proceedings of ICDCOT 2021*. Springer Nature Singapore, 2022, pp. 101–110, Available: https://doi.org/10.1007/978-981-19-2281-7_10

[6] European Parliament, Council of the European Union, "Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport," 2010, Available: http://data.europa.eu/eli/dir/2010/40/oj

[7] A. Perallos, U. Hernandez-Jayo, E. Onieva, and I. J. G. Zuazola, *Intelligent Transport Systems: Technologies and Applications*. John Wiley & Sons, 2015.

[8] P. Papadimitratos, A. D. La Fortelle, K. Evenssen, R. Brignolo, and S. Cosenza, "Vehicular Communication Systems: Enabling Technologies, Applications, and Future Outlook on Intelligent Transportation," *IEEE Communications Magazine*, vol. 47, no. 11, pp. 84–95, 2009, Available: https://doi.org/10.1109/MCOM.2009.5307471

[9] A. Malatras, Z. Stanic, I. Lella, R. De Sousa Figueiredo, E. Tsekmezoglou, M. Theocharidou, R. Naydenov, and A. Drougkas, "ENISA Threat Landscape: Transport Sector (January 2021 to October 2022)," 2023, Available: https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape

[10] R. von Roessing, "The ISACA business model for information security: An integrative and innovative approach," in *ISSE 2009 securing electronic business processes*. Springer, 2010, pp. 37–47. Available: https://doi.org/10.1007/978-3-8348-9363-5_4

[11] J. McCumber, *Assessing and managing security risk in IT systems: A structured methodology*. Auerbach Publications, 2004.

[12] NIST, "Cybersecurity Framework," 2018, Available: https://www.nist.gov/cyberframework

[13] Y. Cherdantseva and J. Hilton, "A Reference Model of Information Assurance & Security," in *2013 International Conference on Availability, Reliability and Security, ARES 2013*. IEEE Computer Society, 2013, pp. 546–555, Available: https://doi.org/10.1109/ARES.2013.72

[14] A. A. Alrehili and O. H. Alhazmi, "ISO/IEC 27001 Standard: Analytical and Comparative Overview," *Lecture Notes in Networks and Systems*, vol. 891, p. 143 – 156, 2024, Available: https://doi.org/10.1007/978-981-99-9524-0_12

[15] NIST, "NIST Special Publication 800-39. Managing Information Security Risk: Organization, Mission, and Information System View," 2011, Available: https://doi.org/10.6028/NIST.SP.800-39

[16] NIST, "NIST Special Publication 800-37: Risk Management Framework for Information Systems and Organizations," 2018, Available: https://doi.org/10.6028/NIST.SP.800-37r2

[17] NIST, "NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations," 2020, Available: https://doi.org/10.6028/NIST.SP.800-53r5

[18] M. Adach, K. Hänninen, and K. Lundqvist, "Security Ontologies: A Systematic Literature Review," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 13585 LNCS, p. 36 – 53, 2022, Available: https://doi.org/10.1007/978-3-031-17604-3_3

[19] B. Kitchenham and S. Charters, "Guidelines for performing Systematic Literature Reviews in Software Engineering," Tech. Rep. EBSE-2007-01, Jul 2007.

[20] National Cyber and Information Security Agency (NÚKIB), "2022 Report on the State of Cybersecurity in the Czech Republic," 2023, Available: https://nukib.gov.cz/download/publications_en/2022_Report_on_the_State_of_Cybersecurity_in_the_Czech_Republic.pdf

[21] Information System Authority (RIA), "Cyber Security in Estonia 2023," 2023, Available: https://www.ria.ee/sites/default/files/documents/2023-02/Cyber-Security-in-Estonia-2023.pdf

[22] M. Bakhtina, R. Matulevicius, and L. Malina, "Supplementary Material for Empirical Study of Information Security and Privacy Management in Intelligent Transportation Systems in Estonia and South Moravia," Apr. 2024, Available: https://doi.org/10.5281/zenodo.10960351

[23] M. Bakhtina, R. Matulevicius, and L. Malina, "Report on Empirical Study of Information Security and Privacy Management in Intelligent Transportation Systems," Apr. 2024, Available: https://doi.org/10.5281/zenodo.10960046

[24] M. Khalid, K. Wang, N. Aslam, Y. Cao, N. Ahmad, and M. K. Khan, "From Smart Parking Towards Autonomous Valet Parking: A Survey, Challenges and Future Works," *Journal of Network and Computer Applications*, vol. 175, p. 102935, 2021, Available: https://doi.org/10.1016/j.jnca.2020.102935

[25] R. Garra, S. Martínez, and F. Sebé, "A Privacy-Preserving Pay-by-Phone Parking System," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 7, pp. 5697–5706, 2017, Available: https://doi.org/10.1109/TVT.2016.2634785

[26] L. Zhu, M. Li, Z. Zhang, and Z. Qin, "ASAP: An Anonymous Smart-Parking and Payment Scheme in Vehicular Networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 4, p. 703–715, 2020, Available: https://doi.org/10.1109/TDSC.2018.2850780

[27] Z. Li, M. Alazab, S. Garg, and M. S. Hossain, "PriParkRec: Privacy-Preserving Decentralized Parking Recommendation Service," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 5, pp. 4037–4050, 2021, Available: https://doi.org/10.1109/TVT.2021.3074820

[28] M. Weber and I. Podnar Žarko, "A Regulatory View on Smart City Services," *Sensors*, vol. 19, no. 2, 2019, Available: https://doi.org/10.3390/s19020415

[29] R. Borges and F. Sebé, "Parking Tickets for Privacy-Preserving Pay-by-Phone Parking," in *Proceedings of the 18th ACM Workshop on Privacy in the Electronic Society*, ser. WPES'19. ACM, 2019, p. 130–134, Available: https://doi.org/10.1145/3338498.3358638

[30] P. Dzurenda, C. A. Tafalla, S. Ricci, and L. Malina, "Privacy-Preserving Online Parking Based on Smart Contracts," in *Proceedings of the 16th International Conference on Availability, Reliability and Security*, ser. ARES '21. ACM, 2021, Available: https://doi.org/10.1145/3465481.3470058

[31] I. Chatzigiannakis, A. Vitaletti, and A. Pyrgelis, "A Privacy-Preserving Smart Parking System Using an IoT Elliptic Curve Based Security Platform," *Computer Communications*, vol. 89-90, pp. 165–177, 2016, Available: https://doi.org/10.1016/j.comcom.2016.03.014

[32] W. A. Amiri, M. Baza, K. Banawan, M. Mahmoud, W. Alasmary, and K. Akkaya, "Privacy-Preserving Smart Parking System Using Blockchain and Private Information Retrieval," in *2019 International Conference on Smart Applications, Communications and Networking (SmartNets)*, 2019, pp. 1–6, Available: https://doi.org/10.1109/SmartNets48225.2019.9069783

[33] F. Al-Turjman, H. Zahmatkesh, and R. Shahroze, "An Overview of Security and Privacy in Smart Cities' IoT Communications," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 3, p. e3677, 2022, Available: https://doi.org/10.1002/ett.3677

[34] P. Dzurenda, F. Jacques, M. Knockaert, M. Laurent, L. Malina, R. Matulevicius, Q. Tang, and A. Tasidou, "Privacy-Preserving Solution for Vehicle Parking Services Complying with EU Legislation," *PeerJ Computer Science*, vol. 8, p. e1165, 2022, Available: https://doi.org/10.7717/peerj-cs.1165

[35] Y. Fang, Y. Zhao, Y. Yu, H. Zhu, X. Du, and M. Guizani, "Blockchain-Based Privacy-Preserving Valet Parking for Self-Driving Vehicles," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 4, p. e4239, 2021, Available: https://doi.org/10.1002/ett.4239

[36] R. Shivers, M. A. Rahman, M. J. H. Faruk, H. Shahriar, A. Cuzzocrea, and V. Clincy, "Ride-Hailing for Autonomous Vehicles: Hyperledger Fabric-Based Secure and Decentralize Blockchain Platform," in *2021 IEEE International Conference on Big Data (Big Data)*. IEEE, 2021, pp. 5450–5459, Available: https://doi.org/10.1109/BigData52589.2021.9671379

[37] S. Ramezanian, G. Akman, M. T. Damir, and V. Niemi, "Lightweight Privacy-Preserving Ride-Sharing Protocols for Autonomous Cars," in *Proceedings of the 6th ACM Computer Science in Cars Symposium*, ser. CSCS '22. ACM, 2022, pp. 11:1–11:11, Available: https://doi.org/10.1145/3568160.3570234

[38] Z. Wang, H. Wei, J. Wang, X. Zeng, and Y. Chang, "Security Issues and Solutions for Connected and Autonomous Vehicles in a Sustainable City: A Survey," *Sustainability*, vol. 14, no. 19, 2022, Available: https://doi.org/10.3390/su141912409

[39] W. Chen, H. Wu, X. Chen, and J. Chen, "A Review of Research on Privacy Protection of Internet of Vehicles Based on Blockchain," *Journal of Sensor and Actuator Networks*, vol. 11, no. 4, 2022, Available: https://doi.org/10.3390/jsan11040086

[40] R. Borges, F. Sebé, and M. Valls, "An Anonymous and Unlinkable Electronic Toll Collection System," *International Journal of Information Security*, vol. 21, no. 5, pp. 1151–1162, 2022, Available: https://doi.org/10.1007/s10207-022-00604-8

[41] X. Deng and T. Gao, "Electronic Payment Schemes Based on Blockchain in VANETs," *IEEE Access*, vol. 8, pp. 38 296–38 303, 2020, Available: https://doi.org/10.1109/ACCESS.2020.2974964

[42] D. Das, S. Banerjee, and U. Biswas, "Design of a Secure Blockchain-Based Toll-Tax Collection System," in *Micro-Electronics and Telecommunication Engineering. ICMETE 2021*. Springer, 2022, vol. 373, pp. 183–191, Available: https://doi.org/10.1007/978-981-16-8721-1_18

[43] S. Sutar, S. Chopade, A. Ekadari, and L. Ahire, "Security Based Electronic Toll Collection Using NFC and Android Application," *International Journal of Scientific and Research Publications*, vol. 5, 2015.

[44] H. Sharp, A. Finkelstein, and G. Galal, "Stakeholder Identification in the Requirements Engineering Process," in *10th International Workshop on Database & Expert Systems Applications. DEXA 99*, 1999, pp. 387–391, Available: https://doi.org/10.1109/DEXA.1999.795198

[45] European Parliament, Council of the European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," 2016, Available: http://data.europa.eu/eli/reg/2016/679/2016-05-04

[46] United Nations Economic Commission, "UN Regulation No 155 – Uniform provisions concerning the approval of vehicles with regards to cybersecurity and cybersecurity management system," 2021, Available: https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security

[47] European Parliament, Council of the European Union, "Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users," 2019, Available: http://data.europa.eu/eli/reg/2019/2144/oj

[48] European Parliament, Council of the European Union, "Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles," 2018, Available: http://data.europa.eu/eli/reg/2018/858/oj

[49] European Parliament, Council of the European Union, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)," 2022, Available: http://data.europa.eu/eli/dir/2022/2555/oj

[50] S. Boslaugh, *Statistics in a Nutshell, 2nd Edition*. O'Reilly Media, Incorporated, 2012.

[51] M. Sadeghi, A. Carenini, O. Corcho, M. Rossi, R. Santoro, and A. Vogelsang, "Interoperability of Heterogeneous Systems of Systems: Review of Challenges, Emerging Requirements and Options," in

Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing, ser. SAC '23. ACM, 2023, p. 741–750, Available: https://doi.org/10.1145/3555776.3577692

[52] D. Hahn, A. Munir, and V. Behzadan, "Security and Privacy Issues in Intelligent Transportation Systems: Classification and Challenges," *IEEE Intelligent Transportation Systems Magazine*, vol. 13, no. 1, pp. 181–196, 2021, Available: https://doi.org/10.1109/MITS.2019.2898973

[53] D. R. Boccardo, L. M. Bento, and F. H. Costa, "Towards a Practical Information Security Maturity Evaluation Method focused on People, Process and Technology," in *2021 IEEE International Workshop on Metrology for Industry 4.0 & IoT (MetroInd4. 0&IoT 2021)*. IEEE, 2021, pp. 721–726, Available: https://doi.org/10.1109/MetroInd4.0IoT51437.2021.9488471

[54] M. Seeba, S. Mäses, and R. Matulevičius, "Method for Evaluating Information Security Level in Organisations," in *Research Challenges in Information Science - 16th International Conference, RCIS 2022, Proceedings*, ser. Lecture Notes in Business Information Processing, vol. 446. Springer, 2022, pp. 644–652, Available: https://doi.org/10.1007/978-3-031-05760-1_39

Appendix I. State-of-the-Art Measures of Information Security and Privacy Assurance in ITS

The report with more detailed results of the literature review (including the data extraction procedure and references to the sources) and survey results can be found in [23].

Table A1. State-of-the-Art Technological Countermeasures

Attribute		**Attribute instances**					
Architectural		Blockchain-based system	Anonymous authenti-cation	Storage of sensitive personal data on the data subject device	Secret- sharing	Multi-party computation (MPC)	Securing data in transit
Use case-oriented	Authenti-cation & Access control	Anonymous credential system	Attribute- based credentials and access control		RFID authenti-cation	Pseudo-random identity assignment	Biometric-based authentica-tion
	Secure communi-cation	TLS protocol	IPSec protocol	VPN solution	Other secured communica-tion protocol	Customer end-to-end encryption	Custom asymmetric encryption
	Navigation and routing	Privacy- preserving navigation systems		Location obfuscation			
	Payment	Automated payment using smart contract		Anonymous payment			
	Location-based search	Hashmap storing of parking slot/ toll/ vehicle locations		Location-based search	Search based on the exact location		
	Pass document creation	Blind signature	Anonymous reservation	Presenting proof-of-knowledge			
Cryptographic		RSA digital signature	Homomor-phic encryption	Zero-Knowledge Proof	Oblivious pseudo-random function (OPRF)	Trusted execution environment (TEE)	Private set intersection (PSI)
		Blind signature	Elliptic curve cryptography	Diffie-Hell-man group key exchange	Hash-based message authentica-tion codes	Oblivious transfer protocol	

Table A2. State-of-the-Art attributes: People, Processes and Organization dimensions

Dimension & Attribute		Attribute instances				
People	Actor	Driver	Passenger	City Government	Trusted Authority (who issues credentials)	
		Time-stamping authority	Organization employee	Parking Service Provider	System provider (based on SLA)	
Organization	Purpose of ITS usage	Decrease the traffic congestion	Resolve the problem of air pollution	Improve of the city services	Improve parking facilities management	Enable on-demand mobility
		Optimise driver's time spent on parking	Optimise parking spaces usage	Prevent unauthorized spots occupation		
	Challenges	Absence or lack of industry regulations and/or standards		The balance between privacy and system efficiency		Heterogeneous network
		Prevention of data leakage through data privacy and security of users' data		Providing the expected level of system security before the system is launched		Data minimization principle
		High expectations from such system quality characteristics (e.g., platform independence, OS independence		Absence of national strategy for smart environments	Resource-constrained devices usage	Interoperability with other systems and/or providers
	Legislation & regulations	General Data Protection Regulation (EU GDPR)	European Union directive 2010/40/EU (7 July 2010)	Consumer protection directives 2019/770 and 2019/771	UNECE regulation No 155 Cyber security and cyber security management system (from 2020)	
	Standards	ISO/IEC 27001	ISO/IEC 27002	Other standards from ISO/IEC 27000-series	NIST Special Publications	ETSI standards series
	Information	Driver's identity	Driver's location	Driver's transactions history	Driver's payment details	Available parking spaces
		Available tolls	Passenger's identity	Passenger' transactions history	Passenger's payment details	Vehicle's location
		Vehicle's state details	Vehicle's identity	Parking/ Ride/ Toll transaction		
Process	System support	Intrusion detection system	Security incident and event management systems (SIEM)	Behavioural analytics system	Network traffic analyser	Vulnerability scanner
	ITS in the business process	Navigation/ routing	Payment	Location-based search	Pass/Reservation document creation	

Appendix II. Questionnaire (shortened)

General questions about the company

1.1. What is your organization's name?
1.2. What is your position/role in the organization?
1.3. Where does your company primarily operate?
1.4. For which purposes does your company use IT system(s)?
1.5. Would you call the system used in your company "an intelligent transportation system"?
1.6. In which area does your company primarily operate?
1.7. How many active end-users does your digital solution have in the selected region?

Section "Organization"

2.1. What is the main objective of your ITS?
2.2. How much is your company involved in the lifecycle of your ITS?
2.3. How much has your system changed during the last 5 years?
2.4. With how many external systems is your system integrated?
2.5. What are the challenges you face during the usage/development/support of your ITS?
2.6. What kind of information is used within your ITS?
2.7. Which security or privacy-related legislation and/or regulations affect your ITS?
2.8. Which cyber/information security standard(s) does your organization follow?

Section "Security and Privacy measures. Part 1"

3.1. Who are the stakeholders of your products/services the ITS?
3.2. What are the practices and policies used for assuring information security and/or privacy management in your company?
3.3. How much security development is integrated into your system lifecycle?
3.4. Which information security and privacy training are established for your system users?
3.5. Which information security and privacy training are established for the employees?

Section "Security and Privacy measures. Part 2"

4.1. Which of the following architectural measures are used in your ITS?
4.2. Which technologies are used in your ITS for authentication and access control?
4.3. Which measures are used in your ITS for secure communication between parties?
4.4. Which cryptographic measures are used in your intelligent transportation system?

Section "Security and Privacy measures. Part 3: System functionality"

4.5.1. Do you have navigation/routing functionality in your ITS?
4.5.2. Which technologies are used in your ITS for navigation/routing?
4.6.1. Do you have payment functionality in your ITS?
4.6.2. Which technologies are used in your ITS for payment?
4.7.1. Do you have location-based search in your ITS?
4.7.2. Which technologies are used in your ITS for parking slot/toll/vehicle search?
4.8.1. Do you have functionality of pass/reservation document creation in your ITS?
4.8.2. Which technologies are used in your ITS for pass/reservation document creation?

Section "Security and Privacy measures. Other"

4.9. What are the other security- or privacy-preserving technologies used in your ITS which were not mentioned?
4.10. Do you consider employing post-quantum cryptography in the future in your ITS?

Section "Security and Privacy measures. Part 4: Processes"

5.1. Which of the following principles are used during your system development/support?
5.2. Which network security measures are used for your ITS support?

Follow-up questions about this survey

How would you assess the level of your information system security? Which sources did you use to answer this survey? How easy was it for you to find the information asked in this survey?

Appendix III. Mapping FISP-ProCOP with the questionnaire

Table A3 maps attributes of FISP-ProCOP with the questions from the questionnaire in Appendix II.

Table A3. Mapping attributes of FISP-ProCOP with the questions from the questionnaire.

Dimension	Category	Attribute	Questions from the questionnaire
P. People	PA. Actors	Actors, stakeholders, entities	3.1; Follow-up questions
		Goals, tasks, motives	
	PR. Relationships	Relationships and dependencies between actors	-
O. Organization	OS. Strategy	Purpose for the system usage, org. design & strategy	2.1,
		Challenges to address	2.5
	OC. Formal Constraints	Legislation, regulation, standard	2.7-2.8
	OI. Information Involved	Type of information used	-
		How the information is manipulated	2.6
		Security criteria	-
		Privacy objectives	-
C. Sec. & Privacy Countermeasures	CP. Policies & Practices	Policies & practices	3.2-3.3, 4.1, 5.1; Follow-up questions
	CE. Training & Education	Training & education	3.4-3.5
	CT. Technology	Architectural measures	4.1
		Use case-oriented technological measures	4.2-4.3, 4.5-4.8
		Cryptographic building blocks	4.4, 4.10
		Others technological measures	4.9
Pr. Processes	PrL. System Lifecycle	Security as a part of the system lifecycle	2.2-2.3, 5.2
	PrU. Usage of the System	Use cases of the system as a part of the business processes	4.5-4.8