Smart Cities: Emerging Risks and Mitigation Strategies

Konstantinos Kirytopoulos, Theofanis Christopoulos, and Emmanuel Dermitzakis

1 Introduction

The urbanization phenomenon is encountered in every corner of the earth and directly affects almost 50% of its population, with the forecasts of experts showing even higher percentages in the years to come (Shen et al., 2016). The population concentration and growth in urban areas lead to the need for continuous improvement in the management of resources, goods, services and infrastructure. In order to meet these needs of the growing urban life and achieve better decision-making, it is necessary for cities to transform into smart cities. This transformation will positively impact the quality of life of their citizens, support economic development and promote environmental sustainability (Silva et al., 2018). This transition has already been attempted by a number of cities, and experience has shown that it directly or indirectly affects all urban activities while engaging all stakeholders, city members and institutions (state, companies, universities and citizens) (Shamsuzzoha et al., 2021).

For the long-term sustainability of these multidimensional cities, special attention to risks is required by those responsible for the development and operation of smart cities. Particular attention has already been devoted both in research and in the implementation of new technologies, in order to address relevant risks. Typical examples are the models that have been developed for assessing the personal information risks managed within a smart city (Yan et al., 2020), or cyber-security risks related to digital assets (Sheehan et al., 2021). Still though, we are far from saying that risks have been addressed entirely. Risk management aims to prepare those responsible for possible incidents in order to avoid improvising responses

K. Kirytopoulos (✉) · T. Christopoulos · E. Dermitzakis
School of Mechanical Engineering, National Technical University of Athens, Athens, Greece
e-mail: kkir@mail.ntua.gr

P. Fitsilis (ed.), *Building on Smart Cities Skills and Competences*, Internet of Things,
https://doi.org/10.1007/978-3-030-97818-1_7

when they occur (Pym, 1987). Identified risks and their potential treatment strategies are key elements in the design and management of smart cities. Nevertheless, a detailed risk taxonomy for the risks of smart cities is still missing from the literature (Ullah et al., 2021). The aim of this chapter is to alert smart cities' designers and other stakeholders on the potential risks that can occur, as well as present some high-level strategies to overcome such risks.

2 The Smart System as a Multisystem Construct

In order to achieve the transformation of a city into a smart city, the integration of new technologies is required, so that the digital and the physical world can merge. Therefore, sophisticated technologies compose the basis on which the philosophy of a smart city is built. Fundamental technologies that build a smart city are Information and Communications Technologies, with their main applications being:

- Internet of Things (IoT): a network which includes a plethora of technologies (e.g. sensor nodes, software solutions, information technologies), aiming at the generation, transfer and exploitation of data (Nižetić et al., 2020).
- Big data: massive volumes of data produced from multiple sensors (Rathore et al., 2015).
- Cloud computing: The National Institute of Standards and Technology's defines cloud computing as "*a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*" (Mell & Grance, 2011).

All the above-mentioned technologies resonate in every urban activity. The main identified dimensions in the literature are smart economy, smart mobility, smart environment, smart people, smart living and smart governance (Giffinger et al., 2007). The "smartness" of these categories is more than just a fancy term. It describes the tendency to improve the economic, social and environmental conditions within cities in a people-oriented way (Silva et al., 2018).

As these urban activities overlap, so do the actuated technologies. A typical example is big data generated in the context of the smart city. More specifically, the debate in the scientific community raises the question whether it is more efficient to collect and manage data under a single roof (centralization of data) (Economic and Social Council of United Nations, 2016) or whether separating data by city dimension is an effective solution to avoid failures and vulnerabilities (decentralization) (Tariq et al., 2020). Another example are the sensors within smart cities, which are the core of smart cities and produce a large amount of data (Ahad et al., 2020). The data from the same sensor can be useful to stakeholders from different fields of activity and can contribute significantly to their decision-making.

Finally, the overlapping functional areas are favoured by the existence of the Internet of Things, which not only allows the extraction of data from existing infrastructure but also supports their fully autonomous operation through the use of artificial intelligence (Mainzer, 2020).

These interrelations and overlaps of activities and technologies have an impact on the smart city's stakeholders. The main stakeholders are the government and local authorities, industries, universities and citizens (Fernandez-Anez, 2016). Each one has their own role, their own contribution and their own requirements in relation to the smart city. Therefore, it is almost impossible to carry out changes and developments in the city's sectors, either in terms of structure or technologies, without affecting their sustainability, since the interests of the stakeholders are also often conflicting (Shamsuzzoha et al., 2021). However, the need to synthesize and manage these technologies in smart cities with a citizen-centred approach cannot be overlooked (Anthopoulos et al., 2007).

The multilayered application, integration and interconnection of new and complex technologies in an intertemporal establishment like a city comes along with risks, both threats and opportunities, while their management is more complicated than the elements that they compose it (Ullah et al., 2021).

Risk management is a systematic process and consists of the following subprocesses: identification, analysis, evaluation, treatment and monitoring and review of risks (International Organization for Standardization, 2018a). Identifying those risks has a complexity proportional to that of the technological systems being installed as well as the number of interconnections, but it is the first step towards their management.

3 Methodology

3.1 Systematic Literature Review

In order to identify the risks of smart cities and their possible mitigation strategies, a systematic literature review (SLR) was undertaken. SLR contributes to the research by setting objective criteria for the selection of the literature to be included, in order to minimize as much as possible the bias and subjective judgement of the researchers (Nightingale, 2009). The literature review process that was followed is summarized in Fig. 1.

The Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guideline is used to present the results of the literature review. This guideline is a statistical approach to the results to promote transparency and full inclusion of the results of the literature review (Page et al., 2021).

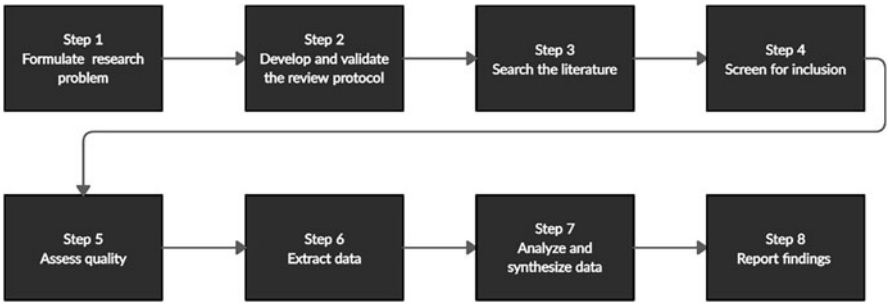

Fig. 1 Steps for SLR (Xiao & Watson, 2019)

3.2 Selecting Articles

For the search of the journals, the Scopus electronic database was used. Scopus database has a plethora of publishers, whose number exceeds 5000, while the number of peer-reviewed journals amounts to 34,500 (Gupta et al., 2019). Moreover, Scopus covers a wide range of scientific fields, for example, Computer Sciences, Social Sciences and Information Science (Mat Ludin et al., 2017).

In order to select the articles for analysis, certain selection criteria were applied, as presented in Table 1. Following the search method of article "title/abstract/keywords" (Derakhshanfar et al., 2019), 2378 results were identified. Next, only journals were selected (excluding conference proceedings, book series, books and other types of literature), to ensure the quality of the included publications, which is guaranteed through the peer review that journals go through (Prater et al., 2017). To include the most up-to-date literature, the search was limited to the last decade. Afterwards, only relevant subject areas were kept, excluding Mathematics, Environmental Science, Physics and Astronomy, Materials Science, Earth and Planetary Sciences, Chemistry, Medicine, Biochemistry, Genetics and Molecular Biology, Chemical Engineering, Agricultural and Biological Sciences, Pharmacology, Toxicology and Pharmaceutics, Neuroscience, Nursing and Immunology and Microbiology. The limitation of the subject areas resulted in 263 journal papers, followed by the restriction of the language to English, coming to 251. The document type was limited to articles, excluding conference papers, reviews, editorials, notes and undefined types, concluding to 231 papers. Finally, based on the research goals, 43 papers were finally selected, reviewing their titles, abstracts and then their content.

Table 1 Stages of setting criteria for the SLR

Search stage	Keyword string	Number of results
1	TITLE-ABS-KEY ((smart OR sustainable OR digital) AND (city OR cities OR town) AND (risk OR risks OR uncertaint*) AND (management OR identification OR mitigation OR response) AND ("sustainable development" OR "risk management" OR "Smart City" OR "sustainability" OR "risk mitigation" OR "risk assessment"))	2378
2	Limiting the search to journals	1308
3	Limiting the search to up to date journals	1079
4	Excluding irrelevant subject areas	263
5	Limiting the search to English journals	251
6	Limiting the search to articles	231
7	Reviewing titles, abstracts and content of the articles	43

3.3 Risk Clustering

To ensure homogeneity of language and lack of repetition and to avoid misinterpretation within the presentation of identified risks, intervention on the description of certain risks is necessary (Le et al., 2019). For this cause, the description of many risks was fine-tuned, while risks with slightly different names but with the same meaning were unified. More specifically, in many cases risks did not follow the typical risk metalanguage, and there was a mix up of causes, risks and impacts. For example, "overestimating the positive impacts of technology" (Ambrosino et al., 2015) was described in one study as a cause for other risks, while "delay in actual deployment of new technologies" (Lee et al., 2013) was described as a cause from strategic and legal risks. Also, as shown in Table 2, the same risk could be described by different authors in different terms.

4 Existing and Emerging Risks in the Development and Operation of Smart Cities

Risk as defined in ISO 31000:2018 is the "*effect of uncertainty on objectives*" (International Organization for Standardization, 2018b), while emerging risks are "*either new risks or familiar risks that become apparent in new or unfamiliar conditions*" (International Risk Governance Council, 2015). In the case of smart cities, this uncertainty is compounded by the city's exposure to new technologies on which cities are founded. This exposure to new technologies is the factor that increases the uncertainty within a smart city compared to a "non-smart city". More specific, these risks have their source in precisely this interwovenness and interconnection of the technologies used, their breakthrough nature and rapid pace

Table 2 Examples of different terminology used for the same risk

No.	Alternative terms used in the literature	Proposed risk's terminology	References
1	Natural disasters	Natural disasters	Yan et al. (2020), Ganin et al. (2019), Hayat (2016)
	Natural hazards		Yang et al. (2018)
2	Unstable power grid	Unstable power supply	Vincent et al. (2020)
	Unstable electric network		Jiménez-Bravo et al. (2018)
	Unstable power generation		Vincent et al. (2020)
	Premature energy depletion of sensors		Soyata et al. (2019)
	Power outage		Vitunskaite et al. (2019)
	Lack of energy supply of sensors		Ayala-Ruiz et al. (2019)
3	Absence of participation by civil society	Lack of participation from citizens	Mainzer (2020)
	Lack of participation from citizens		Gupta and Hall (2020)
	Disinterested citizens		Gupta and Hall (2020)
4	Institutional conditions can be deeply embedded in governance systems (structural inertia)	Organizational incapacity to manage change	Vu and Hartley (2018)
	Lack of capabilities to manage change		Vu and Hartley (2018)
	Organizational incapacity to adopt smart applications		Soyata et al. (2019)

of development. In addition, the smart systems that consist of these technologies are creating greater risks than the risk of each separate component (Axelrod, 2013).

All of the above leads us to the conclusion that, the importance of risk identification is particularly high, as the failure to identify certain risks implies failure to analyse them and subsequent exposure to that risk in the development and operation phases. The number of risks identified from literature review after properly naming and grouping them is 65, and they are presented in Table 3, in a Risk Breakdown Structure (RBS), accompanied by the percentage of the number of appearances of the risks in relation to the total number of risks. The RBS is used to present the identified risks. The risks in the RBS are categorized in groups with a hierarchical structure, allowing the reader to concentrate on the subjects that concern him.

5 Risk Management Skills and Mitigation Strategies for Safe Smart Cities

5.1 Risk Management Skills

To ensure the sustainability of smart cities, it is essential for both developers and managers of the cities to be equipped with risk management skills and knowledge to identify, analyse and treat risks. Only in that way they will be able to enhance opportunities and mitigate threats. Achieving effective risk management requires the risk manager to be equipped with certain competencies and skills. Risk management in smart cities is a complex and multidimensional process, and this requires at least the following:

- Technical skills: Technical skills refer to the ability to implement the processes of risk management (Marx & de Swardt, 2019). Standards for risk management, such as ISO 31000, set guidelines for integrated risk management, but the effectiveness of implementing standards varies from manager to manager.
- Smart city concept understanding: The risk manager should be able to see the big picture in the smart cities' concept. Knowledge of the key objectives of smart cities, the stakeholders and the factors that create uncertainty are necessary to be known, in order to manage the emerging risks.
- Project management skills: Tasks such as creating timelines, long-term planning and setting budget are included in project management procedures. These tasks will be used either directly or indirectly in the risk management procedure too.
- Soft skills: Building the right team, effective cooperation with all its members, effective transmission of information, wise judgement and communicating the risk management procedures to external stakeholders are just some of the soft skills that a risk manager may need (Carvalho & Rabechini Junior, 2015). This means that technical skills alone are not sufficient for successful risk management.

Table 3 The RBS of smart cities

Description of categories/risks		Frequency count	Percentage in relation to total risks
1.	**Economic**		
1.1.	Inappropriate cost planning	3	1.49%
1.2.	Economic distress	2	1.00%
1.3.	Low investment returns	2	1.00%
1.4.	Lack of funding	2	1.00%
1.5.	Financial losses during operation	1	0.50%
2.	**Social**		
2.1.	Lack of technology and information awareness among citizens and external stakeholders	7	3.48%
2.2.	Lack of participation from citizens	3	1.49%
2.3.	Lack of acceptance from society	2	1.00%
2.4.	Social inequality	1	0.50%
3.	**Organizational**		
3.1.	**Partnership risks**		
3.1.1.	Lack of technical know-how and expertise from contractors	3	1.49%
3.1.2.	Conflict of interest of multiple stakeholders	3	1.49%
3.1.3.	Unreliable partners due to vulnerability to cyberattacks	2	1.00%
3.1.4.	Underestimation of critical issues dealing with the interaction activities between providers or suppliers	1	0.50%
3.1.5.	Possible obstacles for technology's application to related industries	1	0.50%
3.1.6.	Trust issues with government officials	1	0.50%
3.1.7.	Lack of fixed tenure of companies that plan, release funds, implement, manage and evaluate the smart cities projects' CEOs	1	0.50%
3.2.	**Human resources**		
3.2.1.	Lack of personnel	2	1.00%
3.2.2.	Lack of staff training	6	2.99%

(continued)

Table 3 (continued)

Description of categories/risks		Frequency count	Percentage in relation to total risks
3.3.	**Operational risks**		
3.3.1.	Lack of standard management	3	1.49%
3.3.2.	Organizational incapacity to manage change	3	1.49%
3.3.3.	Lack of coordination across city's agencies	6	2.99%
3.3.4.	Lack of unified taxonomy from city governments to smart infrastructure systems	2	1.00%
3.3.5.	Great recovery time from disasters and malefactions	1	0.50%
3.3.6.	Limited consideration of interdependency issues between infrastructure systems	1	0.50%
3.4.	**Implementation risks**		
3.4.1.	Lack of project planning	3	1.49%
3.4.2.	Delays in implementation of projects	3	1.49%
3.4.3.	Lack of interest of constructors	2	1.00%
3.4.4.	Lack of project implementation knowledge	1	0.50%
3.4.5.	Challenges in land acquisition	1	0.50%
3.4.6.	Questionable quality of work	1	0.50%
3.4.7.	Unrealistic sociotechnical projects	1	0.50%
4.	**Environmental**		
4.1.	Natural disasters	4	1.99%
4.2.	Climate change	2	1.00%
5.	**Technological and technical**		
5.1.	**Infrastructure**		
5.1.1.	Insufficient maintenance of infrastructure systems	6	2.99%
5.1.2.	Information systems' errors	4	1.99%
5.1.3.	Failure to integrate technology projects into the social structure	3	1.49%
5.1.4.	Unstable power supply	6	2.99%
5.1.5.	Failure of digitization of existing infrastructure	1	0.50%

(continued)

Table 3 (continued)

Description of categories/risks		Frequency count	Percentage in relation to total risks
5.2.	**Requirements**		
5.2.1.	Failure of infrastructure assets to meet quality requirements	4	1.99%
5.2.2.	Poor service and device research	2	1.00%
5.2.3.	Lack of energy estimation techniques of IoT applications	1	0.50%
6.	**Strategic**		
6.1.	Lack of insight of smart city concept	6	2.99%
6.2.	Lack of clear strategy across municipality	4	1.99%
6.3.	Institutional resistance to change their approaches	2	1.00%
6.4.	Overestimating the positive impacts of technology	1	0.50%
6.5.	Insufficient focus on the consequences of infrastructure asset failure, especially on the community side	1	0.50%
7.	**Political**		
7.1.	Reputational damage	2	1.00%
7.2.	Political pressure	2	1.00%
7.3.	Lack of political will	1	0.50%
7.4.	Political uncertainty	1	0.50%
8.	**Legal**		
8.1.	Limitations of existing laws and regulations	6	2.99%
8.2.	Uncertainty in data's security responsibility	3	1.49%
8.3.	Strict regulations	1	0.50%
8.4.	Lack of strict policy enforcement	1	0.50%
9.	**Security**		
9.1.	**Cyber-risks**		
9.1.1	Cyberattacks	27	13.43%
9.1.2.	Private information and data disclosure risk	27	13.43%
9.1.3.	Installation of supervisory control devices	1	0.50%

(continued)

Table 3 (continued)

Description of categories/risks		Frequency count	Percentage in relation to total risks
9.1.4.	Lacking of personal information protection technologies	1	0.50%
9.1.5.	Unpredictable user behaviour	1	0.50%
9.2.	**Health and safety**		
9.2.1.	Harm of human beings from smart technologies	2	1.00%
9.2.2.	Terrorism	2	1.00%
9.2.3.	Human-induced incidents	1	0.50%
9.3.	**Physical resources risks**		
9.3.1.	Stealing devices	2	1.00%
9.3.2.	Sabotage infrastructures for war efforts	1	0.50%
9.3.3.	Deliberate damage of hardware equipment	1	0.50%
Total		201	100.00%

Competence in statistics: The risk manager will be required to use a significant number of mathematical models, simulations and statistics to analyse risks. For example, quantitative analysis follows risk identification and is used to express the probability of occurrence and consequences of identified risks in mathematical form (Baker et al., 1998). This analysis allows the comparison of risks in order to derive a priority for dealing with them, as the budget for this purpose is not limitless.

5.2 Risk Mitigation Strategies

It is necessary to develop appropriate risk response strategies to address the risks that threaten the existence of smart cities. This purpose is served by risk response strategies which address the causes, likelihood and consequences of risks, before or after their occurrence. PMI suggests as risk response strategies: avoidance, transfer, mitigation and acceptance. Definitions of each one are (Project Management Institute, 2017):

- Avoidance: “eliminate the threat or protect the project from its impact”.
- Transfer: “shifting ownership of a threat to a third party to manage the risk and to bear the impact if the threat occurs”.
- Mitigation: “reduce the probability of occurrence and/or impact of a threat”.
- Acceptance: “acknowledges the existence of a threat, but no proactive action is taken”.

First of all, cyberthreats could be assessed by training the personnel responsible for data management, for cyberattacks (Sheehan et al., 2021). Such a measure would help in avoiding potential errors that would create breaches in the smart systems for hacker attacks. Moreover, equipping city's personnel with cyber-attack assessment skills and knowledge would create one more layer of safety from such risks. Finally, since every sector of city is operating in smart technologies, it is not enough to train IT staff, but equipping all staff with good practices in operating technology systems is essential (Kitchin & Dodge, 2019).

Transfer strategy is served by cyber insurance companies, for example, in cyber-security issues, the number of which is increasing not only because of the growing need for their services but also because of legal considerations (Sheehan et al., 2021). By exploiting such excesses, the city is relieved of the cost of a cyberattack.

In case of data storage, encrypting data stored in clouds could prevent their retrievement, even if the attacker succeeded accessing in the cloud (Krämer et al., 2019). Also keeping backups for the important data would eliminate the losses of their potential delete by hackers. Finally, as mentioned before, decentralization of data management by city's sector would avoid exposing all city's data to the attackers. Each one strategy would reduce the impact of a breach of the databases.

There is however another evolving tool for avoiding the vulnerabilities of databases called blockchain. Blockchain is a decentralized storage technology which was initially developed for cryptocurrency transactions and then adopted for other applications, as in smart cities too. The key features of blockchain that make it suitable for replacing databases, as they are known today, are decentralization, resistance to cyberattacks, transparency and scalability (Bhushan et al., 2020; Cui et al., 2018).

Another example, which this time would address the possibility of the risk occurring, is the introduction of standards when creating smart systems in terms of security, encryption, verification and other factors (Sengan et al., 2020). By setting standards, no technology will fall short of safety measures, and the probability of data breach would be reduced. This fact is of crucial importance as in interdependent technological systems, their overall security is equal to the security provided by the weakest component (Kitchin & Dodge, 2019).

Standards can be applied not only to the technologies to be included in smart cities but also to the companies involved. Companies in smart cities are an extension of cities, as they generate, manage and move data to and from city services. Therefore, no matter how many measures the smart city takes for potential risks, it will remain vulnerable to the security flaws of the partner companies. For this reason, it is proposed in the literature that companies that want to participate in the smart city environment should commit themselves to following the standards that have already been developed and which deal with data ownership issues and security procedures for data protection (Vitunskaite et al., 2019).

Artificial intelligence (AI) is a crucial tool for managing data and countering cyberattacks at the same time. By utilizing the machine learning capability of AI applications, these applications are able to identify patterns for optimal data management (Bellam, 2018). The same pattern recognition capability can be also

used to identify cyber-attack patterns, while its self-learning capacity offers the ability to anticipate new cyber-risks (Srivastava et al., 2017). For the autonomous assessing of cyberthreats by AI, algorithms have already been developed and analysed in the literature, such as the neural network model (Krundyshev, 2020).

To extract data from the physical environment of the city and convert it into digital data, the deployment of a plethora of sensor nodes within the smart city is essential. The number of those makes it impossible to check their functionality and reliability in hardware and software level by physical testing. For this cause, dynamic trust measurement models have been developed and tested (Gong et al., 2018). Such measurement models consist of algorithms for the production and evaluation of the signatures of the nodes and for their comparison with trusted nodes (Gong et al., 2018).

Another measure to counter cyberattacks is to keep IoT devices and systems up to date (Andrade et al., 2020). The methods and means for cyberattacks are also evolving rapidly. Therefore, neglecting to upgrade the software used in the smart city environment will create vulnerabilities, as the systems will be outdated against the advances in attack methods.

Risks such as cyberattacks, private information and data disclosure or information systems' errors are often dealt by using other technological systems and automations. This fact raises new issues, as in studies the technologies are often the problem that generates a risk and not the means to solve it (Soyata et al., 2019). Consequently, the situation as it stands at present gives the impression of a vicious cycle. For this reason, but also because new technologies are being integrated and their complexity increases in each smart city, it is necessary to constantly reassess and identify new risks. Risk management is a process that follows the whole lifecycle of a smart city.

6 Conclusions

The number of smart cities is growing rapidly, a trend driven by changing conditions and needs within cities. Along with smart cities, the number of stakeholders who are required to participate in, adapt to and take decisions is growing. In decision-making both in the process of designing smart cities and in their operation, a risk management plan is necessary to ensure the sustainability of the endeavour. Risk management is becoming a complex process, similar in complexity to the interaction of the technologies that build smart cities.

This chapter aims to familiarize developers, managers and other stakeholders of smart cities with the risks to which smart cities may be exposed. Lack of risk awareness will threaten the existence of the smart city in the future, as these risks emerge. Identifying them is therefore the first step in addressing them.

In order to identify the risks that affect the design and operation of a smart city, an SLR was conducted, while the results were presented as PRISMA guidelines suggest. From the SLR the following categories of risks have been identified,

(1) economic, (2) social, (3) organizational, (4) environmental, (5) technological and technical, (6) strategic, (7) political, (8) legal and (9) security, with their subcategories presented in detail in Table 3.

For the effective implementation of risk management, risk managers need to be qualified with certain skills and competences. Such skills are technical skills, smart cities' concept understanding, project management skills, soft skills and mathematical skills. In addition to their personal skills, risk managers can use strategies that have already been developed to mitigate risks. Particular emphasis is given in the literature to address security risks, as the direct and indirect protection of citizens is a priority for any smart city. Following the avoidance, transfer and mitigation strategies and by utilizing new technologies, a number of methods are presented.

One potential limitation of this study is the bias of the researchers on the naming of risks, the grouping of common risks and finally their categorization in the RBS. To address this, detailed reviews were carried out by all researchers, and lengthy discussions were held. As in every RBS, the researchers may differentiate the final result; however, it is the authors' belief that the information (i.e. risks appearing in the RBS) is complete and accurate.

The generated RBS for smart cities' risks could be an advisor in identifying the risks that smart city managers will be asked to undertake. Moreover, high-level strategies are presented, as addressing methods of the identified risks. The equipment of those actively involved in smart cities with risk management skills and knowledge for risk mitigation strategies is an essential step to ensure the sustainability of smart cities from the top level of their management.

References

Ahad, M., Paiva, S., Tripathi, G., & Feroz, N. (2020). Enabling technologies and sustainable smart cities. *Sustainable Cities and Society, 61*. https://doi.org/10.1016/j.scs.2020.102301

Ambrosino, G., Finn, B., Gini, S., & Mussone, L. (2015). A method to assess and plan applications of ITS technology in public transport services with reference to some possible case studies. *Case Studies on Transport Policy, 3*(4), 421–430. https://doi.org/10.1016/j.cstp.2015.08.005

Andrade, R., Yoo, S., Tello-Oquendo, L., & Ortiz-Garces, I. (2020). A comprehensive study of the IoT cybersecurity in smart cities. *IEEE Access, 8*, 228,922–228,941. https://doi.org/10.1109/ACCESS.2020.3046442

Anthopoulos, L., Siozos, P., & Tsoukalas, I. (2007). Applying participatory design and collaboration in digital public services for discovering and re-designing e-government services. *Government Information Quarterly, 24*(2), 353–376.

Axelrod, C. W. (2013). Managing the risks of cyber-physical systems. *2013 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*. doi:https://doi.org/10.1109/lisat.2013.6578215.

Ayala-Ruiz, D., Castillo Atoche, A., Ruiz-Ibarra, E., Osorio de la Rosa, E., & Vázquez Castillo, J. (2019). A self-powered PMFC-based wireless sensor node for Smart City applications. *Wireless Communications and Mobile Computing, 2019*. https://doi.org/10.1155/2019/8986302

Baker, S., Ponniah, D., & Smith, S. (1998). Techniques for the analysis of risks in major projects. *Journal of the Operational Research Society, 49*(6), 567–572.

Bellam, S. (2018). Robotics vs. machine learning vs. artificial intelligence: Identifying the right tools for the right problems. *The Credit and Financial Management Review, 27*(2), 1–10.

Bhushan, B., Khamparia, A., Sagayam, K., Sharma, S., Ahad, M., & Debnath, N. (2020). Blockchain for smart cities: A review of architectures, integration trends and future research directions. *Sustainable Cities and Society, 61*. https://doi.org/10.1016/j.scs.2020.102360

Carvalho, M., & Rabechini Junior, R. (2015). Impact of risk management on project performance: The importance of soft skills. *International Journal of Production Research, 53*(2), 321–340.

Cui, L., Xie, G., Qu, Y., Gao, L., & Yang, Y. (2018). Security and privacy in smart cities: Challenges and opportunities. *IEEE Access, 6*, 46,134–46,145.

Derakhshanfar, H., Ochoa, J., Kirytopoulos, K., Mayer, W., & Tam, V. W. Y. (2019). Construction delay risk taxonomy, associations and regional contexts: A systematic review and meta-analysis. *Engineering, Construction and Architectural Management, 26*(10), 2364–2388.

Economic and Social Council of United Nations. (2016). *Smart cities and infrastructure. Nineteenth session of The Commission on Science and Technology for Development*, Geneva, 9–13 May. Retrieved May 24, 2021, from https://unctad.org/system/files/official-document/ecn162016d2_en.pdf

Fernandez-Anez, V. (2016). Stakeholders approach to smart cities: A survey on Smart City definitions. *Smart Cities*, 157–167.

Ganin, A., Mersky, A., Jin, A., Kitsak, M., Keisler, J., & Linkov, I. (2019). Resilience in intelligent transportation systems (ITS). *Transportation Research Part C: Emerging Technologies, 100*, 318–329.

Giffinger, R., Fertner, C., Kramar, H., Kalasek, R., Pichler-Milanovic, N., & Meijers, E. (2007). *Smart cities—Ranking of European medium-sized cities*. Centre of Regional Science. Retrieved June 8, 2021, from http://www.smart-cities.eu

Gong, B., Wang, Y., Liu, X., Qi, F., & Sun, Z. (2018). A trusted attestation mechanism for the sensing nodes of internet of things based on dynamic trusted measurement. *China Communications, 15*(2). https://doi.org/10.1109/CC.2018.8300276

Gupta, K., & Hall, R. (2020). Exploring smart city project implementation risks in the cities of Kakinada and Kanpur. *Journal of Urban Technology, 28*(1–2), 155–173.

Gupta, P., Chauhan, S., & Jaiswal, M. P. (2019). Classification of smart city research—A descriptive literature review and future research agenda. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-019-09911-3

Hayat, P. (2016). Smart cities: A global perspective. *India Quarterly: A Journal of International Affairs, 72*(2), 177–191.

International Organization for Standardization. (2018a). *Risk management (ISO 31000:2018)*. [online] Retrieved June 14, 2021, from https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

International Organization for Standardization. (2018b). *Risk management—Guidelines (ISO 31000:2018)*. [online] Retrieved July 11, 2021, from https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

International Risk Governance Council. (2015). *Guidelines for emerging risk governance*.

Jiménez-Bravo, D., De Paz, J., Villarrubia, G., & Bajo, J. (2018). Dealing with demand in electric grids with an adaptive consumption management platform. *Complexity, 2018*. https://doi.org/10.1155/2018/4012740

Kitchin, R., & Dodge, M. (2019). The (in)security of smart cities: Vulnerabilities, risks, mitigation, and prevention. *Journal of Urban Technology, 26*(2), 47–65. https://doi.org/10.1080/10630732.2017.1408002

Krämer, M., Frese, S., & Kuijper, A. (2019). Implementing secure applications in smart city clouds using microservices. *Future Generation Computer Systems, 99*, 308–320.

Krundyshev, V. (2020). Neural network approach to assessing cybersecurity risks in large-scale dynamic networks. In *13th International Conference on Security of Information and Networks*. doi:https://doi.org/10.1145/3433174.3433603.

Le, P. T., Kirytopoulos, K., Chileshe, N., & Rameezdeen, R. (2019). Taxonomy of risks in PPP transportation projects: A systematic literature review. *International Journal of Construction Management*. https://doi.org/10.1080/15623599.2019.1615756

Lee, J. H., Phaal, R., & Lee, S.-H. (2013). An integrated service-device-technology roadmap for smart city development. *Technological Forecasting and Social Change, 80*(2), 286–306. https://doi.org/10.1016/j.techfore.2012.09.020

Mainzer, K. (2020). Technology foresight and sustainable innovation development in the complex dynamical systems view. *Foresight and STI Governance, 14*(4), 10–19. https://doi.org/10.17323/2500-2597.2020.4.10.19

Marx, J., & de Swardt, C. (2019). Towards a competency-based undergraduate qualification in risk management. *Qualitative Research in Financial Markets, 12*(1), 96–117.

Mat Ludin, K. R., Mohamed, Z. M., & Mohd-Saleh, N. (2017). The association between CEO characteristics, internal audit quality and risk-management implementation in the public sector. *Risk Management, 19*(4), 281–300. https://doi.org/10.1057/s41283-017-0022-z

Mell, P. M., & Grance, T. (2011). *The NIST definition of cloud computing, tech. Rep., SP 800–145*. National Institute of Standards & Technology.

Nightingale, A. (2009). A guide to systematic literature reviews. *Surgery (Oxford), 27*(9), 381–384.

Nižetić, S., Šolić, P., López-de-Ipiña González-de-Artaza, D., & Patrono, L. (2020). Internet of things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. *Journal of Cleaner Production, 274*. https://doi.org/10.1016/j.jclepro.2020.122877

Page, M., Moher, D., Bossuyt, P., Boutron, I., Hoffmann, T., Mulrow, C., et al. (2021). PRISMA 2020 explanation and elaboration: Updated guidance and exemplars for reporting systematic reviews. *BMJ*. https://doi.org/10.1136/bmj.n160

Prater, J., Kirytopoulos, K., & Ma, T. (2017). Optimism bias within the project management context: A systematic quantitative literature review. *International Journal of Managing Projects in Business, 10*(2), 370–385.

Project Management Institute. (2017). *A guide to the project management body of knowledge* (6th ed.). Project Management Institute.

Pym, D. V. (1987). Risk Management. *PM Network, 1*(3), 33–36.

Rathore, M., Ahmad, A., & Paul, A. (2015). Big data and internet of things. In *Proceedings of the 2015 international conference on big data applications and services*. doi: https://doi.org/10.1145/2837060.2837067.

Sengan, S., Subramaniyaswamy, V., Nair, S., Indragandhi, V., Manikandan, J., & Ravi, L. (2020). Enhancing cyber–physical systems with hybrid smart city cyber security architecture for secure public data-smart network. *Future Generation Computer Systems, 112*, 724–737.

Shamsuzzoha, A., Nieminen, J., Piya, S., & Rutledge, K. (2021). Smart city for sustainable environment: A comparison of participatory strategies from Helsinki, Singapore and London. *Cities, 114*. https://doi.org/10.1016/j.cities.2021.103194

Sheehan, B., Murphy, F., Kia, A., & Kiely, R. (2021). A quantitative bow-tie cyber risk classification and assessment framework. *Journal of Risk Research*.https://doi.org/10.1080/13669877.2021.1900337

Shen, L., Shuai, C., Jiao, L., Tan, Y., & Song, X. (2016). A global perspective on the sustainable performance of urbanization. *Sustainability, 8*(8), 783.

Silva, B., Khan, M., & Han, K. (2018). Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities. *Sustainable Cities and Society, 38*, 697–713.

Soyata, T., Habibzadeh, H., Ekenna, C., Nussbaum, B., & Lozano, J. (2019). Smart city in crisis: Technology and policy concerns. *Sustainable Cities and Society*. https://doi.org/10.1016/j.scs.2019.101566

Srivastava, S., Bisht, A., & Narayan, N. (2017). Safety and security in smart cities using artificial intelligence—A review. *2017 7th International Conference on Cloud Computing, Data Science & Engineering - Confluence*. doi:https://doi.org/10.1109/CONFLUENCE.2017.7943136.

Tariq, M., Wai, C., & Muttil, N. (2020). Vulnerability assessment of ubiquitous cities using the analytic hierarchy process. *Future Internet, 12*(12). https://doi.org/10.3390/fi12120235

Ullah, F., Qayyum, S., Thaheem, M., Al-Turjman, F., & Sepasgozar, S. (2021). Risk management in sustainable smart cities governance: A TOE framework. *Technological Forecasting and Social Change, 167*. https://doi.org/10.1016/j.techfore.2021.120743

Vincent, R., Ait-Ahmed, M., Houari, A., & Benkhoris, M. (2020). Residential microgrid energy management considering flexibility services opportunities and forecast uncertainties. *International Journal of Electrical Power & Energy Systems, 120*. https://doi.org/10.1016/j.ijepes.2020.105981

Vitunskaite, M., He, Y., Brandstetter, T., & Janicke, H. (2019). Smart cities and cyber security: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership. *Computers & Security, 83*, 313–331.

Vu, K., & Hartley, K. (2018). Promoting smart cities in developing countries: Policy insights from Vietnam. *Telecommunications Policy, 42*(10), 845–859.

Xiao, Y., & Watson, M. (2019). Guidance on conducting a systematic literature review. *Journal of Planning Education and Research.*https://doi.org/10.1177/0739456X17723971

Yan, X., Fan, Y., Lee, H., & Qiu, R. (2020). Research on personal information risk assessment model in smart cities. *Tehnicki vjesnik - technical. Gazette, 27*(5). https://doi.org/10.17559/TV-20190104101416

Yang, Y., Ng, S., Xu, F., & Skitmore, M. (2018). Towards sustainable and resilient high density cities through better integration of infrastructure networks. *Sustainable Cities and Society, 42*, 407–422.