# Smart Cities and Cyber Security: Are We There Yet?
# A Comparative Study on the Role of Standards, Third Party Risk Management and Security Ownership.

Morta Vitunskaite, Ying He*, Thomas Brandstetter and Helge Janicke

*School of Computer Science and Informatics, De Montfort University, UK*

## Abstract

Smart cities have brought a variety of benefits aiming to revolutionise people's lives. Those include but are not limited to, increasing economic efficiency, reducing cost and decreasing environmental output. However, the smart city itself is still in its infancy. As it heavily relies on technologies, it opens up doors to cyber attackers and criminals, which can lead to significant losses. An outstanding problem concerns the social and organisational aspects of smart cities security resulting from competing interests of different parties, high levels of interdependence, and social and political complexity. Our review shows that current standards and guidelines have not clearly defined roles and responsibilities of different parties. A common understanding of key security requirements is not shared between different parties. This research assessed the smart cities and their cyber security measures, with a particular focus on technical standards and the regulatory framework. It comprehensively reviewed 93 security standards and guidance. It then performed a comparative case study of Barcelona, Singapore and London smart cities on their governance models, security measures, technical standards and third party management. Based on the review and the case study, this research concluded on a recommended framework encompassing technical standards, governance input, regulatory framework and compliance assurance to ensure that security is observed at all layers of the smart cities.

*Keywords:* Smart Cities, Security Standards, Governance Models, Security Measures, Third Party Approach.

## 1. Introduction

More than half of the world's population is currently living in cities. This has meant that urban development has had to adapt to the population demands; however, frequently this has happened inadequately. The stress on the aging cities' infrastructure combined with excessive population has created a number of significant problems. Chourabi et al. identifies two key types of problems that current cities are experiencing [1]. The first problem concerns physical and material aspects of the city, which encompasses waste management, scarcity of resources, pollution, human health, and traffic congestions. The second problem concerns social and organisational issues, which affect the current cities - multiple and diverse stakeholders, high levels of interdependence, competing objectives and values, and social and political complexity. However, current research has placed an imbalanced focus on the former than the latter.

[*] Corresponding author: ying.he@dmu.ac.uk

Large amount of research has been done about smart cities physical issues and how the new technologies can facilitate them [2–5]. These benefits have been seconded by smart city examples of Barcelona (smart lighting, transport, waste management), Stockholm (smart waste management system), Manchester (real time water monitoring solution) and other cities.

However, there is less research work about the social and organisational aspects. An outstanding problem concerns the social and organisational aspects of smart cities security resulting from competing interests of different parties, high levels of interdependence, and social and political complexity. Existing work shows that current standards and guidelines have not clearly defined roles and responsibilities of different parties [6]. A common understanding of key security requirements is not shared between different parties. There are some exiting work exploring the complexity of knowledge sharing, governing shared resources and addressing shared goals within network organisations [7, 8], it is yet to be appropriately transposed to fit the smart city ecosystem, in particular within the cyber security context.

This research fills in this gap by analysing cyber security challenges of smart cities with particular focus on the smart city ecosystem risks, technical and security standards related to smart cities, and security regulatory framework. In order to validate our findings, this research also performs a comparative case study of Barcelona, Singapore and London smart cities and assesses their governance models applied, security measures implemented, security standards used and third party approaches adopted. This research finally proposes an appropriate framework to ensure that cyber security is embedded across all layers of the smart city ecosystem whilst preserving the innovative nature of the technology at hand.

This research makes the following contributions,

- reviews and analyses a full list of 93 currently available technical and security standards relevant to smart cities and identified the security elements covered in relation to smart cities.
- performs a comparative case study of Barcelona, Singapore and London smart cities on their governance models, security measures, technical and security standards and third party management.
- proposes a smart city security framework to ensure that cyber security is embedded across all layers of the smart city ecosystem.

The article is set out as follows: section 2 introduces the related work of smart cities, smart city ecosystem, and the key security concerns; section 3 reviews and analyses a full list of 93 currently available technical and security standards related to smart cities and the regulatory framework currently in place and their defeciencies and gaps; section 4 reviews and assesses the smart cities using case studies of Barcelona, Singapore and London; section 5 consists of discussion and a recommended framework for smart city development to ensure that cyber security is embedded by design; and section 6 summarises conclusions and future work.

## 2. Related work

### *2.1. Smart City Ecosystem and Risks*

The term of smart city has been used freely and encapsulates a number of varying definitions [1]. Some definitions focus on collective intelligence [9], some on sustainability [4] and others on smart computing technologies [10]. In this paper, the Washburn and Sindhu definition will be adopted, which reads: “The use of Smart Computing technologies to make the critical infrastructure components and services of a city-which include city administration, education, healthcare, public safety, real estate, transportation, and utilities - more intelligent, interconnected, and efficient" [10].

The smart city is a large infrastructure with a number of key and non-key actors. The complexity arises from the city being a public entity, however placing significant reliance and integration on private companies and end users. The complexity of the ICT supply chain has also been recognised by Lu et al. [11]. It includes suppliers, buyers, manufacturers, warehouse and transportation managers, wholesalers, retailers and customers. A disruption at any one side can mean tremendous consequences for the whole ecosystem [11].

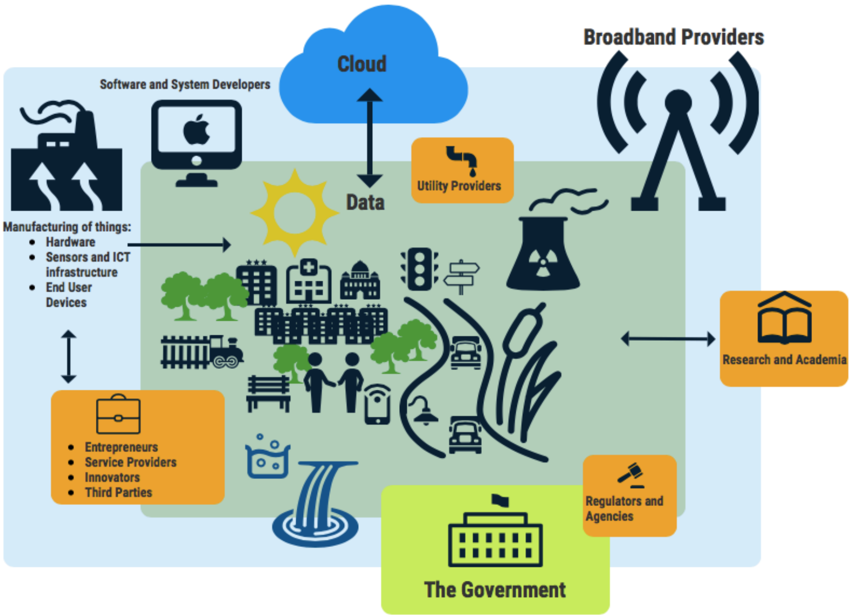

Figure 1: The Ecosystem of a Smart City

Figure 1 illustrates how intertwined the ecosystem of a smart city is. It highlights the high number of different stakeholders and in turn additional security risks. Kennedy has noted that many traditional organisations suffer security incidents stemming from inadequately managed third party or supplier risk [6]. Moreover, the third party risk is increasing due to Internet of Things (IoT) and Cloud prevalence as noted by Ponemon Institute report [12, 13]. It is frequent that access to critical organisation assets and information is given to third parties with little or no security review prior [6]. The reason for such an approach within traditional companies is to speed up the delivery of service and facilitate integration and interoperability. These are the foundational features of a successful smart city and IoT, however if not done right could also lead to being the foundational security weaknesses.

However, the real difficulty for securing the wider smart city ecosystem stems from fourth and fifth parties' involvement in the ecosystem. These include the companies producing end-user devices, which are then directly plugged into the ecosystem by the consumer. The management of the smart city is powerless against these security risks and have to purely rely on their own defences and take on full responsibility if a breach takes place.

Unfortunately, even though the cyber attack or data breach may originate from the third party, the primary organisation is responsible and pays the price. Whilst the liability can often be managed contractually, the responsibility and reputational damage will fall on the parent organisation. This can be illustrated by the Target incident where a breach originating from its third party vendor lead to $162 million loss, excluding the cost of legal fees and other mitigating measures [14]. Another example of third party failure is Stuxnet worm penetration of the Siemens industrial control systems for nuclear power plants in Iran. Similarly, the airliner Boeing 787 was grounded across the world due to failure of the batteries, which were produced in Japan [15]. Whilst the examples may not be directly applicable to the IoT or the smart city, the risks and principles of organisational responsibility are still valid. It reiterates the difficulty of security risk management in a highly complex organisation such as a smart city due to the number of actors and stakeholders involved.

Public-Private Partnerships (PPP) has been used for the smart city management to transfer and clearly define the responsibility if the risk is materialised. However, there are a number of disadvantages that are noted against the PPP, primarily a potential rise in cost for the consumers to ensure sustainability. Further, they require careful consideration during the contract drafting to ensure the full benefits for the city [16]. The rhetoric of a ‘private city’, ‘corporate smart city’ has been used by academia to note the potential drawbacks of the private involvement in public services [17]. These include neglecting public and citizen needs and requirements, limited level of involvement and a profit-above-all approach [17].

### *2.2. Security of Smart Cities*

The key enabling technologies for smart cities are smart computing technology citehollands2008will, IoT [18] and wireless identification, sensing, localisation and connectivity [19]. The IT infrastructure for the smart city consists of fibre-optic channels, wireless networks and hotspots and other information systems, which are the traditional elements of the IT system. Explicitly to the smart city, the infrastructure includes sensors, end point devices and allows for user devices to be connected to the outer layers of the infrastructure. Whilst technology is the key component, it also introduces a number of security risks. The possible impacts on the affected city can be but are not limited to: power outage resulting in loss of economic activity, water pollution due to an attack on a water treatment facility, traffic incidents; financial loss, loss of sensitive information and even endangering of life through building control system manipulation.

Li et al. has recognised that the key weak link for smart cities is the security and trustworthiness of data [18]. The trustworthiness of data is fundamental to a successful operation of the smart city; however a potential cyber attack could alter or generate misleading data [18]. As a result, falsified reports on smart grid or traffic could lead to inappropriate controls to the systems. This could have far reaching and even life-threatening implications, such as car accidents or inappropriate water treatment. Additional security challenges that IoT is facing are vulnerable and error-prone transmission mediums, which rely on radio frequency, and an ever-changing network topology [18]. Whilst Li et al. [18] recognises the appropriate technical difficulty in ensuring the security, the author did not acknowledge the stakeholder complexity and difficulties within the supply chain, third parties and other involved actors. As different products and services will be governed and produced by different manufacturers, ensuring appropriate level of security across all layers may prove difficult. This is due to competing interests and different operational approaches to security and risks that supply chain and stakeholders have.

However, the data is not the only security concern for smart cities. According to a study conducted by International Data Corporation, 212 billion “things” will be installed based on IoT technology with an estimated market value of $8.9 trillion in 2020, which translates to 212 billion potential attack doors [20]. IoT devices can be compromised in a number of ways e.g. connected into a botnet, made inoperable by a worm or used to penetrate the inner networks and systems. This has been evidenced by one of the key cyber attacks in 2016, where IoT appliances were connected into a botnet sending DDoS attacks [21]. This threat derives from the internet connectivity, which allows for a remote attack and code execution. The threat is amplified by the inherent accessibility of technology used such as TCP/IP or Zigbee protocols. Information on the protocols' vulnerabilities and attack tools are easily accessible via a basic search browser. As TCP relies on a unique user's IP address, an attacker may easily trace to specific individuals [22].

In addition to the inherent vulnerabilities of various protocols, the devices are commonly deployed with little security measures and default generic passwords. The information concerning connected to the Internet devices is accessible using the Shodan search engine. The National Crime Agency (NCA) has highlighted that this security problem concerns a number of manufacturers and IoT appliances [21]. Specific examples include botnets such as Mirai targeting insecure IoT devices and connecting them to a botnet [23]; Persirai, connecting internet protocol cameras [24]; and Brickerbot, a worm rendering insecure IoT devices unusable [25]. As a result, a number of IoT devices get consistently recalled [21].

The above analysis evidences the significant amount of threats that the city may experience. Unsurprisingly, the attacks do not require sophisticated skill to cause significant damage. Figure 2 provides an illustration and an overview of threats to smart city.

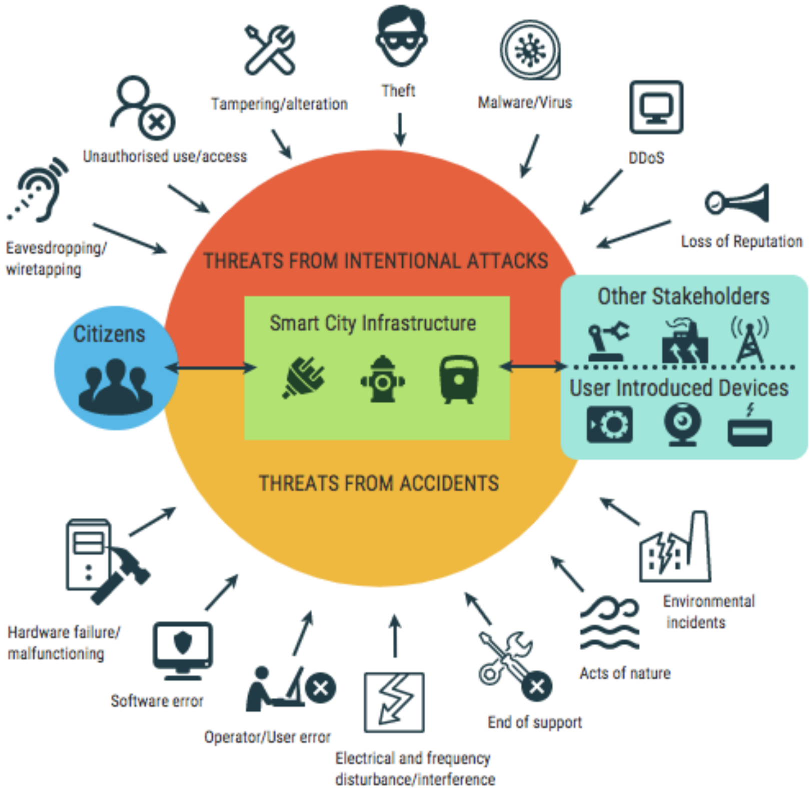

Figure 2: Smart City Threat Landscape

It is difficult to adequately quantify the impact of cyber threats on public city infrastructure due to lack of real-time data. However, in 2015 a cyber incident on a Ukrainian energy distribution companies showcased the disruption and the impact that attacks on smart city infrastructure may bring [21]. It draws an appropriate perspective on the damage that can be caused economically and to the citizens themselves. As a result of a cyber attack on the company's network and industrial control systems (ICS), approximately 225000 people have lost electricity and companies lost automated control of their systems [21].

Due to a critical impact of cyber attacks on smart cities and their probable likelihood caused by a high number of end-point devices, the security of smart cities must be at the forefront of a smart city strategy. The vast evidence reviewed above suggests that the threats to a smart city are extremely common and can lead to a significant damage. Also untargeted attacks, which are not designated primarily against smart cities may pose nonetheless a significant risk in the sense of collateral damage, if they exploit vulnerabilities in core technology building blocks or platforms. This was shown in 2017 through the NotPetya destructive ransomware outbreak, that although designated mainly against specific systems in the Ukraine, spread globally and affected e.g. the transportation and logistics sector heavily, creating harsher supply conditions problems especially in cities. Therefore, the key question is to ensure that security by design is embedded across all layers of the ecosystem, including private companies, the supply chain, as well as the lifecycle of smart city elements which may range from months to decades. This requires appropriate industry standards and regulations. The current framework of standards and regulation will be discussed in the next section.

## 3. Review of Smart City Related Standards and Regulatory Framework

### *3.1. Smart City Related Standards*

The section above has highlighted the issue that the smart cities require effective technical and security standards. This view has also been seconded by the British Standards Institution (BSI) report on smart city data, which highlighted that smart cities across the world are dealing with different problems and require standards/data to facilitate the decision making [26]. We have reviewed a full list of 93 currently available IoT and security standards (See Appendix 1). The evaluation exercise has found a number of standards, which have been defined by industry and standard bodies, technology companies, researchers and cities.

Among the 93 standards, 13 out of 93 cover cyber security elements, listed in Table 1. We found that one out of 93 is currently being developed to address security and privacy of wireless consumer devices [27]. A high number of technical standards are pre-existent and apply to the infrastructure technology of smart cities. Standards are tailored and address either a specific industry or specific component of infrastructure. British Standards Institution (BSI) is leading the development of smart city standards in the UK. To date it has developed eight standards/guidelines. We noted that all standards facilitate the development and conceptualisation of smart cities and their strategy, but offer little guidance on security of the infrastructure.

IEEE is a major player in defining technical and security elements for the IoT. A number of standards had been defined prior the term IoT or smart city was even coined. In addition to pre-existent standards, IEEE is leading the project IEEE P2413 - Standard for an Architectural Framework for the Internet of Things (IoT), with a sub-group focused on end-to-end approach to ensuring protection, security, privacy and safety of IoT technology [28]. In addition, IEEE has taken steps to standardize physical and medium access control layers, wireless networks and wireless devices with end-to-end security in mind.

There is a strong input of standards derives from Europe (DIN, NEN, CEN, CENELEC, ETSI). The leaders within the technical standards are ISO and IEC. American input is mainly via ANSI and IEEE standards. Russia has developed some standards and they are mainly released via GOST R [29]. A number of standards are tailored to specific industries. For example, NERC-CIP was developed for electric utility industry; NIST Cybersecurity framework was developed for financial, energy, healthcare and other systems [30].

As the findings above suggest, there are a number of technical standards developed or currently in development globally for IoT technology and industries. Yet, despite the numerous attempts coming from different bodies to provide clarity and standardize the model, the smart city remains an ambiguous playground [31]. The review also showed that the standards are not comprehensive and often focused on very specific technical features. Whilst 13 standards cover security to some extent, few offer a comprehensive set of principles to ensure security by design.

The standards have not yet been adopted by the industry and have not been noted as mandatory requirements. Application of these standards will be further assessed by the case studies in Section 4. Lack of adaptation and poor security can be further illustrated by a study conducted by HP of 10 IoT devices in use today for security vulnerabilities. The study found that on average a device had 25 vulnerabilities, totalling 250 vulnerabilities across 10 IoT devices [32]. The study has initiated and contributed to the OWASP Internet of Things (IoT) Project [33].

UK has released guidance on key security principles for connected and automated vehicles for manufacturers to ensure the security by design for smart transportation in the UK and a security characteristic for smart metering and communications hub[34, 35]. Automated vehicle guidelines are so far the most comprehensive and prescriptive approach to security-in-depth released by a national government. It recognises the complexity of multi-stakeholder environment and aims to provide a benchmark to all parties involved in the manufacturing and supply chain.

Governmental and non-governmental bodies have released security guidance for transport. Whilst the British guidance is particularly comprehensive and it is first to acknowledge the real complexity of security due to the multi-stakeholder environment, it is limited to smart vehicles only and will require time embed. At the moment, the guidance is not mandatory and there is no information available showing the manufacturers will embrace it. However, at this point it is clear that the industry is leading the way and thus shaping the standards rather than the other way around. Whilst some proprietary solutions or frameworks may become the de facto benchmark for others to follow, the standards will require time and appropriate approach from the city councils in order to bring the desired effect to the field of secure IoT.

Table 1: Security Elements covered by Security Standards

| Standard | Description | Security Elements covered |
|---|---|---|
| EIA TSB 4940 | Smart device communications - Security aspects | The standard series cover security aspects of device communications, with particular focus on protocols in use [36]. |
| NEN 7512:2005 nl | Health informatics - Information security in the healthcare sector - Basis for trust for exchange of data | The standard is specific to healthcare sector in the Netherlands. It is focused on ensuring the security of data exchange [37]. |
| PAS 555:2013 | Cyber security risk - Governance and management - Specification | UK based standard issued by the BSI, aimed at ensuring appropriate cyber security government and management at an organisation. The standard is not specific to smart cities or IoT [38]. |
| SS-ISO/IEC 27005:2013 | Information technology - Security techniques - Information security risk management | This ISO standard is focused on information security risk management. The standard is not specific to smart cities or IoT [39]. |
| IEEE P24151-1-4 | Standard for Smart Transducer Interface for Sensors, Actuators and Devices - eXtensible Messaging and Presence Protocol (XMPP) - currently being developed, specifically addresses security | N/A - has not been released yet. The standard will cover security features of sensors, actuators and devices that use XMPP protocol [40]. |
| IEEE P1912 | Standard for Privacy and Security Architecture for Consumer Wireless Devices - currently being developed | N/A - has not been released yet. The standard will cover privacy and security aspects of end user devices [27]. |
| IEEE 802.1AE-2006 | EEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security; Security capabilities expanded by IEEE 802.1AEbw-2013. | These series of standards are focused on networks security, with particular focus on MAC security [41]. |
| IEEE 802.21a-2012 | IEEE Standard for Local and Metropolitan Area Networks: Media Independent Handover Services - Amendment for Security Extensions to Media Independent Handover Services and Protocol | These series of standards are focused on security mechanisms to protect media independent handover services and mechanisms to use MIH to assist proactive authentication to reduce the latency due to media access authentication and key establishment with the target network [42]. |
| IEEE 1888 series | IEEE Standard for Ubiquitous Green Community Control Network Protocol and its security | The standard series identify gateways for field-bus networks, data storage for archiving and developing data sharing platforms, and application units as important system components for developing digital communities, i.e., building-scale and city-wide ubiquitous facility networking infrastructure. [43] |

Table 1: (continued)

| Standard | Description | Security Elements covered |
|---|---|---|
| IEEE 692-2013 | IEEE Standard for Criteria for Security Systems for Nuclear Power Generating Stations | Criteria for the design of an integrated security system for nuclear power generating stations are provided in this standard. Requirements are included for the overall system, interfaces, subsystems, and individual electrical and electronic equipment. This standard addresses equipment for security-related detection, surveillance, access control, communication, data acquisition, and threat assessment [44]. |
| IEEE C37.240-2014 | IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems | The standards presents a balanced approach to security of automation, protection and controls systems [45] |
| IEEE 1686-2013 | IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities | The functions and features to be provided in intelligent electronic devices (IEDs) to accommodate critical infrastructure protection programs are defined in this standard. Security regarding the access, operation, configuration, firmware revision and data retrieval from an IED are addressed. Communications for the purpose of power system protection (teleprotection) are not addressed in this standard [46]. |

### *3.2. Regulatory Framework*

Legal regulation and policy tend to take time to catch up with the innovation and new technology. The key legal regulation currently in place is Computer Misuse Act 1990, which introduced criminal offences for incidents regarding unauthorised access to computer material, commission of offences using computers or unauthorised modification of computer material. This act will remain valid in the emergence of smart cities and will capture any intentional security incidents regarding smart city technology. However, this offers a very traditional view to cyber crime/attacks. The act is unable to encompass the emerging legal issues from the IoT and smart cities due to their inherent complexity.

Dowden has noted where potential legal challenges may arise. To date, there is no guidance found on liabilities concerning a product failure, i.e. a crash involving a self-driving car or failure to administer medication due to a cyber breach [47]. This suggests that in cases where incidents are caused by a fault or vulnerability in a third party product, there is no law to ensure that the manufacturer presumes responsibility. As a result, this places the end user with no guarantees to be compensated. In cases where a third party product is directly embedded in the smart city infrastructure, the responsibility and damages will be absorbed by the smart city council.

There have not yet been any cases regarding product liability in the IoT/smart city context; therefore it is hard to predict how the courts would react. However, due to lack of specific regulations in place for product failure, the courts are likely to invoke the contractual duty of care, as defined in the landmark case of AC 562 [48]. The case established that a manufacturer owes a duty of care if it is reasonably foreseeable that a failure in ensuring product's safety would lead to harm of the user. However, this would only apply to individual end users as organisations, including the smart cities would have contractual agreements in place taking precedence over the duty of care. It is difficult to determine whether this would be a cause of action or whether the courts may see IoT/smart city as a completely different issues, however it may render a possible remedy to affected users.

Another area of uncertainty lays with data privacy, in particular ownership, processing, use and security of data generated by the IoT devices in view of multiple commercial and public stakeholders. The Data Protection Act (DPA) 1998 is the data protection regulation that is currently in place in the UK. The key take away from the DPA is its duty to notify users of any loss of personal data. The act is a direct transposition of a EU data protection Directive 95/46/EC.

However, the 1995 Directive has been superseded by the General Data Protection Regulation (GDPR), which comes into force in 2018 May. As it is a Regulation rather than a Directive, it does not require a local transposition into laws but rather is effective immediately. It applies to all businesses and bodies dealing with personal data. GDPR is applicable to both controllers and processors of data. Information Commissioner's Office (ICO) has defined the controller as a body that defines how and why personal data is processed and the processor as the body that acts on the controller's instructions [49]. Essentially, it requires that all parties involved in data handling (storage and transfer included) comply with the Regulation.

Contrary to the DPA, the Regulation ascertains significantly more liability to the processor of data rather than placing the responsibility and liability for breaches on the controller entirely. The processor is required to maintain records of data and the processing that has taken place. However, where the processor is deemed to be responsible for the breach, this will not alleviate the controller from responsibility. The Regulation puts forward additional requirements on the processor to ensure that the contracts comply with the GDPR [49].

UK has now confirmed that it will uphold the GDPR despite leaving the EU. Lack of compliance with the regulation will mean not only reputational damage but also a ground-breaking 4% of the annual turnover in financial fines. This regulation is a step forward in defining the ownership of security and data protection for Smart City and IoT. It clearly sets out the importance of clear contractual agreements and demands compliance with the regulation by all parties involved. However, it also reiterates that the contracting party, in this case, the City, will always bear some level of responsibility when breaches happen. Importantly, this Regulation applies internationally, where the data processed is of EU nationals. This will allow ascertaining some level of liability to third parties operating outside the EU, but serving the citizens within the EU [49].

In addition to the liability challenges, further issues regarding security and data protection stem from public-private partnerships and the involvement from the commercial actors. The overall concepts of privacy by design, which are being presented by the GDPR, seem contrary to the idea of Smart City, where big data and its analytics are the key enablers for the IoT and Smart City initiatives. More importantly, due to the cloud prevalence and data storage worldwide, it is debatable whether privacy and data security are even feasible in practice [47].

To illustrate the complexity, the EU is persistent on consent when it comes to data sharing and data privacy. Requirement of consent was introduced as part of the e-Privacy Directive (2002/58/EC), which solidified into a click-through consent to cookie tracking on websites. Questions are raised regarding how the equivalent would be addressed in the field of IoT, in particular wearable technology which may film or record outsiders and process data on the streets [50].

Another aspect of law, which may require a reshuffle, is privacy law. The landmark decision of Von Hannover [51] concerning photographs of the princess playing tennis, which were later published, constitutes a breach on the grounds of expectation of privacy. Questions are raised regarding how such principles will be transformed to accommodate data collected in the smart city or even in a smart home.

These legal questions currently remain unanswered. Whilst there is no specific regulation or official guidance that directly apply to IoT and smart cities, it can only be speculated what approach will be taken to stretch the current regulations into the digital space. The complexity arises where the government is keen to protect its critical assets and the industry continues desiring to operate freely and without imposed restrictions [52]. However, due to the immense data and privacy implications that the smart cities bring, it is important that the regulators start thinking about these challenges and help shape innovation ensuring that privacy and security are observed by design, without stifling it.

## 4. Case Studies: Barcelona, Singapore and London

### *4.1. Research Method*

A quantitative case study of Barcelona, Singapore and London using publicly available information has been conducted. The goal of this study is to quantify and confirm findings identified by the literature review and analysis above. We selected Barcelona, Singapore and London as these cities have been reported as the most developed smart cities [53]. Factors such as adoption of smart grid technologies, smart lighting, smart traffic, Wi-Fi access points, use of smartphones and available applications were assessed as part of this research. In addition, these cities are at the forefront of smart city development and therefore will have the most publicly available data for the study.

The research method consists of review and inspection of publicly available information including academic articles, official websites, news reports focusing on (1) governance model applied, (2) security measures implemented, (3) standards used in the development and (4) third party approach adapted. The purpose of this study is to provide first hand evidence to support the above-identified findings. Specifically, the study will provide insight into how smart cities are being developed; whether the governance approach is defined at the beginning of the development; whether technical standards have been upheld or adhered to, noting the leading standards if any; and finally it will show whether security and risk within the third party management has been assessed and appropriate measures taken on the onset. The data is collected using a search of academic databases and the open source.

### *4.2. Barcelona*

Barcelona is deemed as one of the smart city pioneers. Barcelona's smart city project started in 2012 with the deployment of IoT technology across public transit, parking, street lighting and waste management [54]. The overall initiative consisted of 83 individual projects and utilized the fiber optic internet across the city. It serves as the key enabler for the integrated IoT systems. Barcelona has a defined strategy in place and considers the following [55],

- To define the city model "mantra" ;

  ("mantra" is defined as "a city of productive neighbourhoods, at human speed, interconnected, eco-efficient, re-naturalized, energetically self-sufficient, and regenerated at zero emissions, inside a high-speed interconnected Metropolitan Area" )
- To analyse the structure of the city and define action plans;
- To rethink the systems of the city;
- To develop the economy of the city services along with the ecosystem;
- To make the city more resilient and promote long-term investment;
- To make the city liveable, increasing public space for people;
- To change the organisation, breaking the "silos" ;
- To work with other cities and to be part of the City Protocol Society.

To date, the project has resulted in significant cost savings and increased quality of life for the citizens. It is estimated that the 'smartification' has led to $58 million on water savings, boosted parking revenues by $50 million and savings of $37 million due to smart lighting a year [54]. Barcelona's key smart city innovations are focused on its transport system, smart shelters and bus stops, smart bicycle sharing system, smart parking, pneumatic waste management, smart lighting, use of renewable energy and use of apps for urban mobility [56]. Barcelona Smart city aims to define, design and develop a reference model of a network management platform and sensor data for a Smart city and validate it in a major city [57]. It relies on open source rather than proprietary platforms.

#### *4.2.1. What governance model has been applied?*

Gasco has analysed Barcelona's management and organisation following Chourabi's integrated framework [55]. The analysis has showed that Barcelona's management is part of a broader model, which encourages territorial decentralization, service externalization and the adoption of managerial tools.

The Mayor of the city has actively supported the development of the city. Specific offices have been established to deal and develop the strategy. Those are Urban Habitat, The Computer Municipal Institute, and Smart City Personal Management Office. Further, Barcelona has involved a number of stakeholders in the development and defining of the strategy, including businesses and universities. However, the leadership lies in the hands of the City Council. Gasco noted that public-private partnerships played a key role in developing the city [55].

The city has been set up to ensure that citizens are involved and the governance model is transparent. This model is expressed via a citizens' complaints bureau, Bustia Ciutadana, which allows reporting breakages or making suggestions. It also has developed an application named IDBCN, which enables citizens to digitally and remotely identify themselves. Further, Open Data Barcelona is accessible to all, which contains data on election, population, economy and other, which facilitates citizens with inception of new services and businesses [56].

### *4.2.2. What security measures have been implemented?*

Review of available data (in English) has not indicated what security measures have been adapted by the City. Further, our review of the open source documents noted that cyber security does not feature frequently in a high level discourse of the Barcelona smart city.

### *4.2.3. What standards have been used in the development?*

Review of available data has not indicated what specific standards have been used in the development of the Barcelona smart city. In addition, no specific standards have been mandated going forward. The study has found that one of the key lessons from Barcelona's smart city projects is in fact lack of standards; this has been corroborated by the development of an open source solution rather than relying on proprietary solutions. Furthermore, lack of standards for data handling and encoding has resulted in a difficulty, especially due to a number of invested interests and requirements - public administration, citizens and third parties [57].

### *4.2.4. What third party approach has been adapted?*

The city's strategy suggested that programmes and projects should be implemented as part of the public-private partnerships, including academia and other research centres [55]. Barcelona places a lot of emphasis on innovation by the citizens and enterprises. This can be evidenced by the 22@Barcelona. 22@Barcelona is a regeneration project and it provides a space for urban planning and entrepreneurialism. It is a space for municipal leaders to collaborate with the private sector, universities and communities to speed up innovation. For example, the city' irrigation system is a joint venture [58].

Other examples of public-private partnerships include Barcelona GIX project, the Integrated Management of Municipal IT Networks. Due to the public-private partnership, the project was well governed and the cost was found to be lower. Similarly, Worldsensing and its smart parking system is also a joint venture between the city and a private enterprise, which was developed at 22@Barcelona. The city provided space for developing and allowed for the product to be piloted on Barcelona streets [58].

Whilst this approach is highly collaborative and fosters innovation, review found little data to suggest a comprehensive assurance model towards third parties. This view can be corroborated by previously discussed and self-identified issue of lack of encoding and data handling standards.

## *4.3. Singapore*

Singapore has taken a slightly different approach towards 'smartification'. Specifically, it aims to involve the full government and the full nation in developing it [59]. Singapore's smart city project dubbed as 'Smart Nation' initiative is coordinated by the Smart Nation and Digital Government Office in the Prime Minister's Office, with support of other governmental agencies. It aims to transform five key domains:

- Transport
- Home & Environment

- Business productivity
- Health and enabled ageing
- Public sector services

The project was established in 2014 [60]. It involves universities, cultivates a community of start-ups, partners with the industry and corporations to sponsor labs and R&D. Further, it is enabling the population with the skills necessary for the Smart Nation [59]. The examples of the initiatives that have been implemented by Singapore include smart home technologies, autonomous road transport, and healthcare. Similarly to Barcelona, it has an open data platform, which is accessible by the public and private companies, and a Living Laboratory - a district designed for fostering innovation and piloting solutions [61]. To achieve these initiatives, the city is implementing an advanced info-communications infrastructure and has created a platform for data sharing, which is accessible by all.

### *4.3.1. What governance model has been applied?*

The city governance lies in the hands of the Government. Singapore has established the Smart Nation and Digital Government Group (SNDGG), a centralised agency, under the Prime Minister's Office to deal with agencies involved in Singapore's digital transformation [62]. The SNDGG consists of the Smart Nation and Digital Government Office (SNDGO) and GovTech. SNDGO is responsible for policy formation and GovTech is responsible for policy implementation. SNDGO consists of Smart Nation Programme Office, Digital Governance Directorate (MOF) and Government Technology Policy Department (MCI). Singapore government aims to digitise public service delivery through its 'e-government' drive. It aims to implement and supply the infrastructure, policies and enablers to foster innovations, encouraging the citizens and businesses to get involved [60].

Singapore as a smart city is slightly different to other cities due to its deregulated economic market. As a result, it is willing to experiment and does so in an agile way [23]. However, Singapore is also taking a different approach to data handling and management. Rather than setting up a Data Operation Centre, it is aiming to develop policies and regulations supported by a common platform for data, which in turn can be used by different governmental agencies [63].

Singapore has observed some challenges due to the differing stakeholder interests. For example, Seng has stated that whilst both the police and transport could use CCTV cameras, steps must be taken to break down the silos, understand how duties of maintenance and data connectivity should be shared /citeseng2016singapore. Research suggests that measures that could facilitate such management have not been implemented yet.

### *4.3.2. What security measures have been implemented?*

Singapore has addressed the need for cyber security and recognises that everyone has a part to play [61]. Singapore has developed a clear cyber security strategy, which underpins four core pillars: resilient infrastructure, a safe cyberspace, creation of cyber security ecosystem and strong international partnerships. This approach is seen as a fundamental part in becoming a truly smart city [59]. As such, one of the key measures coming out of this strategy is strengthening and expansion of the National Cyber Incident Response Team and the National Cyber Security Centre [64].

In addition to the Singapore's cyber security strategy, the city has also established a Cyber Security Lab as a joint venture by University of Singapore and Singtel. The lab has two key objectives: to develop a more advanced data analytics techniques and a novel approach to design and implementation of systems that observe a 'Security by design' approach. The lab will work across four different areas of network, data and cloud security; predictive security analytics; IoT and Industrial Control Systems and cyber security based on quantum technology [65].

Whilst the cyber strategy is a huge step forward and indicates Singapore's seriousness towards having a secure smart city, however, review of available data including academic papers, cyber security strategies and other publicly available documentation and news reports have provided little detail on what security measures have been adopted by Singapore.

### *4.3.3. What standards have been used in the development?*

The study found no data to suggest that specific standards have been adhered to as part of the development to date. As a result, Singapore has recognised a necessity for technical standards to ensure that data flows seamlessly and all involved actors speak the common language and operate in harmony. Information Technology Standards Committee (ITSC) and Internet of Things Technical Committee (IoTTC) have roles to play in defining the technical specifications for the Smart Nation. The committees work to identify what standards need to be defined alongside the strategy [59]. So far it has developed and defined technical reference documents for the sensor network (TR 38 and TR 40). The standards, once defined, will be applicable to public and private bodies and will help to improve the collaboration. The final goal is to develop standards that will cover the end-to-end IoT architecture [66].

In addition, Singapore has taken steps to release a new Cyber Security Act. The act will be made mandatory for the operators to take cyber security steps and report incidents. In addition, it will empower the Cyber Security Agency and will help raise the standards of cyber security across all layers. The Act will focus on providing a set of standards, protocols and rules for organisations providing services to the city. It has not yet established how it is best to enforce the rules [64].

Whilst the study suggests that few measures may have been implemented as part of the initial initiative, it is strongly evidenced that Singapore takes cyber security seriously and is taking all steps necessary to embed 'security by design' approach.

### *4.3.4. What third party approach has been adapted?*

Singapore stands out as a city placing significant reliance on private companies to innovate and the government itself presumes the role of an enabler and supporter, rather than an innovator itself [60]. It thrives and encourages an attitude of creating and innovating together, with an involvement of its citizens and the private sector [61].

As part of this, Singapore has developed a start up ecosystem, where venture capitalists and entrepreneurs may work and experiment. As a result, Singapore has been ranked as No. 1 for ease of doing business by the World Bank [60].

Whilst this approach is great for collaboration, the review has found little data to suggest a comprehensive assurance approach to data and service integration. However, as discussed above, the city has taken steps to establish regulations and laws, dictating that standards must be followed by all parties involved in the development. As such, this approach will facilitate and help reduce the third party risks.

## *4.4. London*

London smart city initiative was started with the opening of an extensive open data store in 2010 and was fully embedded with the inception of the Smart London Board in 2013. The Mayor of London formed the Smart London Board. The board created the Smart London Plan [67] and define a vision for a smarter London [31]. The strategic smart city plan included a number of smart initiatives for citizen engagement, data and innovation enhancement. This has been supplemented by a number of labs and innovation districts [31]. The notable successful projects include widespread Wi-Fi, smart transport and prevalent use of applications.

*4.4.1. What governance model has been applied?*

Smart London Board is the key advisor on the smart city matters. The Board comprises of academics (e.g. from University College London, Imperial College London, etc.), businesses and entrepreneurs (e.g. from Siemens, McKinsey, Accenture Health and Public Service, etc.). The Board does not have any government representative. They are responsible for advising the smart city matters for Greater London Authority. The board also advises on how technology could influence the mayoral strategies and policies. It also helps improve existing public services and create opportunities for new digital public services. The smart city plan as devised by the Board covers key seven areas [68],

- Placing Londoners at the heart of the innovation
- Having open and accessible data
- Utilising London's research abilities and talent
- Networking amongst city's stakeholders
- Developing smart infrastructure
- Having better and more integrated City Hall services
- Enabling smarter London experience for all

The plan is focused on the implementation of projects and initiatives and does not provide guidance on stakeholder management or security. However, it places focus on the bottom-up approach. Similarly to Singapore, it sees the citizens, businesses and entrepreneurs as key partners for innovation and suggests a cooperative climate [68].

The projects are promoted via the government sites, however they have little detail on how they are managed or run. The key challenges for the overall initiatives have been identified as connecting people and creating communities, navigation and transportation, capturing and using data [69].

*4.4.2. What security measures have been implemented?*

UK has released a national cyber security strategy for 2016-2021. The strategy did not include the cyber security requirements specific to smart cities [34]. Review of other publicly available documentation and news reports have provided little detail on what security measures or requirements have been observed as part of the Smarter London initiative. Contrary to Singapore, cyber security does not feature significantly in the rhetoric of Smart London.

*4.4.3. What standards have been used in the development?*

United Kingdom and London have a few bodies, which have taken the lead with defining technical standards relevant to the Smart City and IoT. Specifically, a joint collaboration of Cities Standards Institute (CSI) and British Standards Institute (BSI) has so far released four standards. These are:

- PAS 181, Smart City Framework Guide to establish strategies for smart cities and communities

- PAS 182, Smart City Concept Model Guide to establish a model for data interoperability
- PAS 183, Smart Cities Guide to establish a decision-making framework for sharing data and information services
- PAS 184, Smart Cities Guide to develop project proposals for delivering smart city solutions

As reviewed above in section 2, these standards are high level and provide a more operational or project-based guidance, rather than dictate what technical or cyber security elements must be observed. In addition to the BSI-CSI standards, UK government has released cyber-security focused principles for connected and automated vehicles and a security specification for smart metering. The guidance is the most comprehensive in the industry so far, however it is yet to be embedded. Via a review of available documentation, the author found little information on what technical standards were complied with during the research period.

#### *4.4.4. What third party approach has been adapted?*

London is aiming to support the innovation by offering facilities such as ultra-fast broadband, digital and physical space to small and medium enterprises. The smart city approach includes the support of commercialisation of technology innovation [68].

However, there is little information publicly available that can shed some light on how London is managing its third party risk. The key development, as discussed above, is the guidance on automated vehicles. The principles are applicable to manufacturers and other actors of the supply chain, which should provide some level of assurance regarding the security. However, the principles are limited to automated cars and are yet to be embedded.

### *4.5. Key findings and discussion on case studies*

The comparative case study of smart cities quantifies the identified findings. The case study findings are summarised in Table 2. This will lead to the formulation of the recommended framework for secure smart city development in section 5.

Table 2: Case Study Findings

| | Governance Model | Security Measures | Technical Standards | Third Party Management |
|---|---|---|---|---|
| **Barcelona** | • Leadership is at the hands of the City Council<br>• Part of the broader model of governance<br>• Encourages decentralisation<br>• Specific governmental offices created to lead the initiative<br>• Citizens and innovators at the core of the initiative<br>• Utilisation of PPPs | • No data to suggest preexistent measures<br>• No data to suggest the 'go-forward' approach | • No data to suggest preexistent measures<br>• No data to suggest the 'go-forward' approach<br>• Recognised as a key challenge | • Private innovation is at the heart of the initiative;<br>• No data to suggest that the city has implemented a comprehensive assurance model towards third party risk |
| **Singapore** | • Whole government, whole nation approach<br>• The government is the enabler and sets policies and regulations<br>• Citizens and innovators at the core of the initiative<br>• Utilisation of PPPs | • No data to suggest preexistent measures<br>• Cyber Security heavy 'go-forward' approach defined<br>• Cyber Security Strategy<br>• Cyber Security Act<br>• Cyber Security Lab | • No data to suggest preexistent measures<br>• 'Go-forward' approach includes end-to-end architecture IoT standards<br>• Standards committee has developed two standards thus far | • Private innovation is at the heart of the initiative;<br>• No data to suggest that the city has implement a comprehensive assurance model towards third party<br>• Third party risk will be reduced by the introduction of the new Cyber Security Act |

Table 2: (continued)

| | Governance Model | Security Measures | Technical Standards | Third Party Management |
|---|---|---|---|---|
| **London** | • Smart London Board acts as an advisor to the Greater London Authority<br>• Little data available to suggest how projects are run | • No data to suggest pre-existent measures<br>• Principles for cyber security of automated cars have been released by the Government<br>• Security characteristic for smart metering has been released by the Government | • No data to suggest pre-existent measures<br>• Two bodies working on developing standards<br>• 4 standards developed thus far; however high level and project focused | • Private innovation is at the heart of the initiative;<br>• No data to suggest that the city has implement a comprehensive assurance model towards third party<br>• The risk will be reduced to some extent by the implementation of cyber security principles for automated vehicles and smart meters |

The case studies have showed that many cities fail to have comprehensive and long-term smart city strategies in place [68]. The strategies in place do not take into account management of security risks, use of standards or a comprehensive approach towards third party risk management. However, the study has showed that the cities do start thinking about these risks as they become more and more developed. All cities have specific bodies in place that drive the initiatives. However, all three cities had a different approach.

*Governance Model.* Barcelona had a single governmental department responsible for the wider initiative; Singapore has a 'fully in' approach in place, which means that the whole government is involved and driving the 'smartification'; Barcelona and Singapore placed citizens and innovations at the core of the smart city initiative while little information was available regarding this aspect for London; finally, London has a Smart London Board in place which advises the Greater London Authority on smart city matters. Interestingly, the Board heavily consists of big corporate leaders, some academia and no government representatives. This is slightly worrisome as such a one-sided approach may steer London to a corporate city side rather than a smart city for all citizens.

*Security Measures.* Among the three cities studied, Singapore appeared as the most collaborative and the most advanced in its approach to cyber security. Whilst still in its infancy, it forms Singapore's long-term approach to embedding cyber security by design. Specifically, the committee it has in place alongside the Cyber Security Act is building a base of rules and standards that third parties and other private companies must adhere to. Contrary to Singapore, Barcelona and London do not seem as vocal about what cyber security measures are being implemented or what the strategy going forward is. Although UK has released a national cyber security strategy for 2016-2021, the strategy did not include the cyber security requirements specific to smart cities [34].

*IoT and Security Standards Relevant to Smart Cities.* Review of available data has not indicated what specific standards have been used in the development of the Barcelona smart city. Singapore takes cyber security seriously and is taking all steps necessary to embed 'security by design' approach. It has developed two standards for the sensor network (TR 38 and TR 40). London has two bodies, CSI and BSI, taking the lead with defining technical standards relevant to the Smart City and IoT. They released four standards; however these standards are high level and provide a project-based guidance. Whilst all cities are taking steps to define the standards, they are high level and lack the technical aspects that are so necessary for a security-by-design approach. Further, little information was available to show what standards all three cities have already implemented or used as part of their infrastructure development. This corroborates with the previously identified findings regarding non-existent and inconsistent use of technical standards.

*Third Part Management.* Barcelona places an emphasis on innovation by the citizens and enterprises, evidenced by the 22@Barcelona. Whilst this approach is highly collaborative and fosters innovation, review found little data to suggest any risk reduction strategies towards third parties. Singapore has taken steps to establish regulations and laws, which will facilitate and help reduce the third party risks. The key development in London is the guidance on automated vehicles. The principles are applicable to manufacturers and other actors of the supply chain, which should provide some level of assurance regarding the security. However, the principles are limited to automated cars and are yet to be embedded. All three cities are focused on a highly collaborative approach and see the citizens and businesses at the heart of its innovation. However, limited information was available to demonstrate those cities have implemented a comprehensive assurance model towards third party risk. This can be explained by either a lack of a defined process or by a limitation of data available. These findings combined with the literature review, which has showed that little attention is being paid to managing the stakeholders and third party appropriately, suggest that smart cities studied are yet to define an appropriate process.

To conclude, the above analysis and the case studies have showed that unless the ecosystem for the smart city is highly cooperative and collaborative, the innovation will be stifled and the smart city idea will not succeed. Lee and Whang has recognised the difficulty between the flexible integration and security among third parties in the more traditional supply chain context [70]. However, this complexity is ever increasing in the smart city framework as illustrated by the literature review and the case studies above. Therefore there are two key points, which have to be satisfied to render a valid security framework for smart cities: a) easy collaboration and data sharing amongst the ecosystem; and b) security is observed at all levels and stages of the ecosystem without slowing down the collaboration.

## 5. Recommendations

As the industry is still in its infancy, the smart cities globally and the City Councils behind them learn as they go. Experiment and by trial and error find ways that prove effective and efficient in developing the initiatives. Unsurprisingly, the academia and technical standards trail behind whilst the industry are creating de facto frameworks and guidelines to follow. However, whilst in some cases this may prove appropriate, it often neglects the security by design and puts the infrastructure and its citizens at risk of cyber-physical breaches. Furthermore, lack of appropriate framework could lead to the city being overly centralized or overly privatised, resulting in an imbalanced approach, stifled innovation or an uncontrolled environment, placing the infrastructure and citizens at risk. Therefore, it is paramount that the right balance is struck ensuring that responsible innovation continues at a speed whilst observing security by design principles (Hoe, 2016). As the government is the main owner, it is important it takes appropriate steps to ensure security and minimise liability in cases incidents happen.

### *5.1. Technical Standards*

The case study shows that the standards have not yet been adopted by the industry and have not been noted as mandatory requirements. IEEE has also noted that security elements are often not developed as part of the initial design, but rather is considered as an afterthought of the IoT initiatives [71]. Prescriptive standards are paramount to smart cities as the tech vendors contributing and providing solutions will frequently be small and medium enterprises and start ups. Kaspersky lab has noted that 57% of small businesses do not invest into security solutions [72]. This could lead to a compromise of a whole platform or a smart city. A study conducted by HP of 10 IoT devices in use today shows that on average a device had 25 vulnerabilities, totalling 250 vulnerabilities across 10 IoT devices [32].

Pishva stated that the security issues cannot be dealt with by a single vendor or manufacturer [22]; instead, an adherence to certain standards must become as the norm of smart city appliance development. As the analysis has showed, there are a high number of technical standards that are related to the IoT or Smart City. The variety of standards is overwhelming, they are not sufficiently comprehensive and there is little guidance on which standards are key. Therefore, it is paramount that a set of baseline security standards is drafted, which apply principles rather than rules, ensuring they can be scaled up or down, depending on the product or service. It is important that technical standards provide coverage for application and code development to embed the security by design principles.

### *5.2. Government Input*

The NCA report on cyber threat to business has noted that the government has a part to play in embedding the 'security by design' principles. This has materialised to an extent and resulted in the development of a standard by the National Cyber Security Centre (NCSC) and the Department for Business, Energy & Industrial Strategy on a secure smart metering system. This is one of the first steps for the government on the road to 'secure by design' destination [21]. However, to date, there has not been an appropriately defined strategy in place for smart cities in the UK [73].

The government should define a harmonised cyber security framework, which includes all stakeholders including operators, manufacturers and other actors. The government should act as a coordinator and the framework would integrate cyber security standards and an appropriate risk management approach [74]. Specifically it should,

- Whilst the government is able to release specific security standards it may not always be best equipped to do so. Therefore, it is important the government sets out clearly which standards are mandatory for all actors of the ecosystem of smart city.
- Following the identification and definition of key standards, the government should define the standard operating processes for data management and handling for smart city. These guidelines should be mandatory and apply to all actors of the ecosystem of smart city.
- As the owner of the smart city, the government must also define a set of procedures for the supply chain. Specifically, defined timely assurance requirements and clear contractual agreements are paramount to ensure that only secure third party providers are integrated in the critical smart city infrastructure.
- The government should also define the minimum security requirements or a security level for all smart home and personal devices and require for that level to be clearly noted on the packaging to appropriately inform the user. As it is impossible to enforce specific security standards to fourth or fifth parties, labelling may be an appropriate step to allow end users to make choices when it comes to purchasing gadgets and technology. As a result, the government must also produce clear guidance for the end user to secure their internal networks. As IEEE has noted, it is the responsibility of the owner to train its citizens to protect first their data and secondly the integrity and security of the smart city as a whole.
- It must specifically define the responsibilities of the senior management in cyber security at the framework level. It must also define the requirements of a well-equipped Security Operations Centre and a Cyber Security Incident Response Team (CSIRT). This would allow increasing the readiness against the cyber attacks [74].
- Roles and responsibilities of every actor within the smart city ecosystem must be identified at both business-as-usual state and in a cyber attack case. This would allow the actors to better understand the rights and duties and ensure business continuity and safety of the citizens [74]
- Finally, it must ensure that cyber knowledge and information of breaches are shared within the ecosystem in a collaborative and timely manner to ensure that the effect of such incidents is minimised.

The framework must consist of principles rather than guidelines to ensure that new technologies are captured and it can be scaled easily. However, where certain standards are defined, adherence to them should be strict and mandatory.

### *5.3. Regulatory Framework*

Whilst the regulators should start thinking how the current regulatory framework could be adapted, it is likely it will change organically on a case-to-case basis. Currently, there seems to be sufficient regulation in place regarding data protection; however the difficulty may arise with the extensive data handling and consent that inevitably will come with IoT and Smart city.

### *5.4. Compliance Assurance*

Finally, compliance testing and certifications should form part of the cyber security framework for smart cities. As adherence to technical standards should start at the application or code development stages, it should lead to security by design approach in all products that will form the smart city ecosystem. However, to confirm compliance the third parties should complete annual testing and certification. An independent party, such as an internal or external auditor, should perform testing and certification. This would give a reasonable level of assurance to the regulator that all key smart city ecosystem actors observe security by design.

## 6. Conclusion and Future Work

Not that long ago smart cities seemed like a utopian dream. However, with the technology improving faster than ever before, it is no longer just a dream but a reality. Whilst still in its infancy, it promises to revolutionise the lives of the people, increase economic efficiency and decrease environmental output. However, with all these significant benefits, there also come security risks. As the smart cities are entirely reliant on technology, this opens up more doors to cyber attackers and criminals, leading to significant material, economic and at times even fatal losses. As such, it is paramount to observe cyber security at all layers of the city.

Collaboration, open innovation as well as acertain a agility despite complex intertwined structure is fundamental to the success of any smart city. However, as the analysis has shown, this is also often the culprit of security deficiencies. The real difficulty for observing security stems from the complexity of the smart city ecosystem and involvement of a high number of competing actors and stakeholders. As the cities are still developing, many fail to take these risks into account and develop an appropriate third party management approach. One of the key symptoms of this deficiency is lack of appropriate standards and guidance, clearly defined roles and responsibilities and a common understanding of key security requirements.

The case studies of Barcelona, Singapore and London has emphasised and corroborated the importance of technical standards, cyber security measures and an effective third party management approach. In turn, this paper has suggested a framework of recommendations to ensure that security is observed by design from the onset of the smart city development.

The framework suggests that the government acts as a policy setter and a coordinator in order to define and mandate the technical standards and define the minimum security requirements. Further, the government should require a clear definition of roles and responsibilities, key processes and procedures for data handling and management and a set of procedures and requirements for third party and supply chain management. Introduction of the suggested framework would allow and encourage collaboration in a secure capacity without unnecessarily stifling any innovation. It would lead to security being observed by design and drive good security practices in other companies and manufacturers.

Smart cities are the way forward, however as they are still amidst their infancy, steps should be taken to ensure that they are secure, robust, resilient and managed continuously during operations. Only if security is observed by design, will smart cities improve the lives of the citizens and deliver on the promised benefits. The research conducted is based on publicly available information review. As smart cities may not share information openly, a field study or interviews with developers of the smart cities will compliment and confirm our findings, which will be our next stage work.

## References

[1] H. Chourabi, T. Nam, S. Walker, J. R. Gil-Garcia, S. Mellouli, K. Nahon, T. A. Pardo, H. J. Scholl, Understanding smart cities: An integrative framework, in: System Science (HICSS), 2012 45th Hawaii International Conference on, IEEE, 2012, pp. 2289–2297.

[2] J. Borja, Counterpoint: Intelligent cities and innovative cities, Universitat Oberta de Catalunya (UOC) Papers: E-Journal on the Knowledge Society 5.

[3] J. Marceau, Innovation in the city and innovative cities, Innovation: Management, Policy, & Practice 10 (2-3) (2008) 136–146.

[4] D. Toppeta, The smart city vision: how innovation and ict can build smart,"livable", sustainable cities, The Innovation Knowledge Foundation 5 (2010) 1–9.

[5] E. Kabalci, A smart monitoring infrastructure design for distributed renewable energy systems, Energy Conversion and Management 90 (2015) 336–346.

[6] J. Kennedy, Cyber risk management of third party suppliers and partners, `http://www.continuitycentral.com/index.php/news/technology/1220-cyber-risk-management-of-third-party-suppliers-and-partners`, [Accessed 2 Aug 2017] (2016).

[7] S. S. Dawes, A. M. Cresswell, T. A. P. COMMENTATORS, L. B. BINGHAM, S. L. CAUDLE, From "need to know" to "need to share": Tangled problems, information boundaries, and the building of public sector knowledge networks, in: Debating public administration, Routledge, 2012, pp. 93–114.

[8] E. P. Weber, A. M. Khademian, Wicked problems, knowledge challenges, and collaborative capacity builders in network settings, Public administration review 68 (2) (2008) 334–349.

[9] C. Harrison, B. Eckman, R. Hamilton, P. Hartswick, J. Kalagnanam, J. Paraszczak, P. Williams, Foundations for smarter cities, IBM Journal of Research and Development 54 (4) (2010) 1–16.

[10] D. Washburn, U. Sindhu, S. Balaouras, R. A. Dines, N. M. Hayes, L. E. Nelson, Helping cios understand "smart city" initiatives: defining the smart city, its drivers, and the role of the cio. cambridge, ma: Forrester research, Inc. Retrieved April 12 (2010) 2014.

[11] T. Lu, X. Guo, B. Xu, L. Zhao, Y. Peng, H. Yang, Next big thing in big data: the security of the ict supply chain, in: Social Computing (SocialCom), 2013 International Conference on, IEEE, 2013, pp. 1066–1073.

[12] P. Institute, Data risk in the third-party ecosystem, `https://www.ponemon.org/local/upload/file/Data\%20Risk\%20in\%20the\%20Third\%20Party\%20Ecosystem\_BuckleySandler\%20LLP\%20and\%20Treliant\%20Risk\%20Advisors\%20LLC\%20Ponemon\%20Research\%202016\%20-\%20FINAL2.pdf`, [Accessed 2 Aug 2017] (2016).

[13] P. Institute, Tone at the top and third party risk, `https://sharedassessments.org/summit/SA-2016-Ponemon-Study-Tone-At-The-Top-And-Third-Party-Risk-Final.pdf`, [Accessed 2 Aug 2017] (2016).

[14] I. Magazine, Target hackers may have gotten in through the air conditioner, `https://www.infosecurity-magazine.com/news/target-hackers-may-have-gotten-in-through-the-air/`, [Accessed 2 Aug. 2017] (2017).

[15] B. Sarlioglu, C. T. Morris, More electric aircraft: Review, challenges, and opportunities for commercial transport aircraft, IEEE Transactions on Transportation Electrification 1 (1) (2015) 54–64.

[16] F. R. Medda, G. Carbonaro, S. L. Davis, Public private partnerships in transportation: Some insights from the european experience, IATSS research 36 (2) (2013) 83–87.

[17] R. G. Hollands, Will the real smart city please stand up? intelligent, progressive or entrepreneurial?, City 12 (3) (2008) 303–320.

[18] W. Li, H. Song, F. Zeng, Policy-based secure and trustworthy sensing for internet of things in smart cities, IEEE Internet of Things Journal 5 (2) (2018) 716–723.

[19] J. Ma, Internet-of-things: Technology evolution and challenges, in: Microwave Symposium (IMS), 2014 IEEE MTT-S International, IEEE, 2014, pp. 1–4.

[20] L. Dignan, Internet of things: $8.9 trillion market in 2020, 212 billion connected things, October 3 (2013) 2013.

[21] N. C. Agency, The cyber threat to uk business, National Crime Agency (2016).

[22] D. Pishva, Internet of things: Security and privacy issues and possible solution, in: Advanced Communication Technology (ICACT), 2017 19th International Conference on, IEEE, 2017, pp. 797–808.

[23] Wired.com., What the uk can learn from singapore's smart city, `http://www.wired.co.uk/article/sara-watson-singapore-smart-cities`, [Accessed 6 Sep. 2017] (2017).

[24] G. Masters, New iot bot persirai ensnaring ip cameras, `https://www.scmagazine.com/new-iot-bot-persirai-ensnaring-ip-cameras/article/655875/`, [Accessed 10 Jul 2017] (2017).

[25] J. Biggs, Brickerbot is a vigilante worm that destroys insecure iot devices, `https://techcrunch.com/2017/04/25/brickerbot-is-a-vigilante-worm-that-destroys-insecure-iot-devices/`, [Accessed 10 Jul. 2017] (2017).

[26] B. S. Institution, City data survey report, London: BSI Standards Limited, [Accessed 31 Jul. 2017 (2015).

[27] I. S. Association, et al., Privacy and security architecture for consumer wireless devices working group (com/sdb/p1912 wg).

[28] T. Cherry, Security and iot in ieee standards — ieee standards university, https://www.standardsuniversity.org/e-magazine/march-2016/security-and-iot-in-ieee-standards/, [Accessed 31 Jul 2017] (2017).

[29] I. C. London, Mapping smart city standards, https://www.bsigroup.com/LocalFiles/en-GB/smart-cities/resources/BSI-smart-cities-report-Mapping-Smart-City-Standards-UK-EN.pdf, [Accessed 21 Jul. 2017] (2017).

[30] A. Grau, Iot security standards–paving the way for customer confidence, IEEE Standard University.

[31] L. Anthopoulos, Smart utopia vs smart reality: Learning by experience from 10 smart city cases, Cities 63 (2017) 128–148.

[32] D. Miessler, Hp study reveals 70 percent of internet of things devices vulnerable to attack, Retrieved June 30 (2014) 2015.

[33] owasp.org., Owasp internet of things project - owasp, https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project, [Accessed 8 Sep 2017] (2017).

[34] P. Hammond, National cyber security strategy 2016 to 2021 (2016).

[35] C.-E. S. Group, Cpa security specification: Smart metering - communications hub, https://www.ncsc.gov.uk/content/files/protected_files/document_files/SMLT\%20SC0003\%20Communications\%20Hub\%20v1-1.pdf, [Accessed 8 Sep. 2017] (2017).

[36] Global.ihs.com, Smart device communications; protocol aspects; introduction, https://global.ihs.com/doc_detail.cfm?\&csf=TIA\&item_s_key=00601371\&item_key_date=861031, [Accessed 7 Sep 2017] (2017).

[37] NEN, The cyber threat to uk business, https://www.nen.nl/NEN-Shop/Norm/NEN-75122005-nl.htm, [Accessed 8 Sep 2017] (2017).

[38] B. S. Institution, Pas 555:2013 cyber security risk, Governance and management, [Accessed 8 Sep. 2017] (2017).

[39] ISO/IEC, Iso/iec 27005:2018 - information technology – security techniques – information security risk management, https://www.iso.org/standard/75281.html, [Accessed 13 Jan. 2019] (2018).

[40] Standards.ieee.org., P21451-1-4 - standard for smart transducer interface for sensors, actuators and devices - extensible messaging and presence protocol (xmpp) - currently being developed, specifically addresses security, https://standards.ieee.org/project/21451-1-4.html, [Accessed 8 Sep 2017] (2012).

[41] Standards.ieee.org., Ieee sa - 802.1ae-2006 - ieee standard for local and metropolitan area networks: Media access control (mac) security, https://standards.ieee.org/findstds/standard/802.1AE-2006.html, [Accessed 8 Sep 2017] (2006).

[42] Standards.ieee.org., Ieee sa - 802.21a-2012 - ieee standard for local and metropolitan area networks: Media independent handover services - amendment for security extensions to media independent handover services and protocol, https://standards.ieee.org/findstds/standard/802.21a-2012.html, [Accessed 8 Sep 2017] (2012).

[43] Standards.ieee.org., Ieee std 1888.2-2014 : Ieee standard for ubiquitous green community control network: Heterogeneous networks convergence and scalability, (electronic resource), https://standards.ieee.org/standard/1888-2014.html, [Accessed 13 Jan 2019] (2013).

[44] Standards.ieee.org., 692-2013 - ieee standard for criteria for security systems for nuclear power generating stations, https://standards.ieee.org/standard/692-2013.html, [Accessed 13 Jan 2019] (2013).

[45] Standards.ieee.org., Ieee sa - c37.240-2014 - ieee standard cybersecurity requirements for substation automation, protection, and control systems, https://standards.ieee.org/findstds/standard/C37.240-2014.html, [Accessed 8 Sep 2017] (2017).

[46] Standards.ieee.org., Ieee sa - 1686-2013 - ieee standard for intelligent electronic devices cyber security capabilities, https://standards.ieee.org/findstds/standard/1686-2013.html, [Accessed 8 Sep 2017] (2013).

[47] M. Dowden, Rise of the machines, New Law Journal 166 (7714).

[48] D. v Stevenson, Donoghue v stevenson (1932) (1932).

[49] I. C. Office, Overview of the general data protection regulation (gdpr), https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/, [Accessed 20 Aug. 2017] (2017).

[50] R. Corbet, Internet of things - where are we now?, Privacy and Data Protection (2015).

[51] N. Nohlen, Von hannover v. germany. app. no. 59320/00.2004-vi eur. ct. hr, American Journal of International Law 100 (1) (2006) 196–201.

[52] K. S. Review, Securing the smart city, http://harvardkennedyschoolreview.com/securing-the-smart-city/, [Accessed 21 Jul. 2017] (2017).

[53] S. Sorrell, Worldwide smart cities: Energy, transport & lighting 2016-2021, Tech. rep., Tech. report, Juniper Research, 2016. 42 (2016).

[54] L. Adler, How smart city barcelona brought the internet of things to life, Retrieved from Data Smart City Solutions: http://datasmart. ash. harvard. edu/news/article/how-smart-city-barcelona-brought-the-internet-ofthings-to-life-789.

[55] M. Gascó, What makes a city smart? lessons from barcelona, in: System Sciences (HICSS), 2016 49th Hawaii International Conference on, IEEE, 2016, pp. 2983–2989.

[56] B. D. City, Barcelona digital city, http://ajuntament.barcelona.cat/digital/en, [Accessed 6 Sep. 2017] (2017).

[57] T. Gea, J. Paradells, M. Lamarca, D. Roldan, Smart cities as an application of internet of things: Experiences and lessons learnt in barcelona, in: Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2013 Seventh International Conference On, IEEE, 2013, pp. 552–557.

[58] L. Laursen, City saves money, attracts businesses with smart city strategy, https://www.technologyreview.com/s/532511/barcelonas-smart-city-ecosystem/, [Accessed 2 Aug 2017] (2017).

[59] C. E. Seng, Singapore's smart nation program—enablers and challenges, in: System of Systems Engineering Conference (SoSE), 2016 11th, IEEE, 2016, pp. 1–5.

[60] Smartnation.sg., About smart nation — enablers, https://www.smartnation.sg/about-smart-nation/enablers, [Accessed 6 Sep. 2017] (2017).

[61] S. L. Hoe, Defining a smart nation: the case of singapore, Journal of Information, Communication and Ethics in Society 14 (4) (2016) 323–333.

[62] J. J. Woo, Singapore's smart nation initiative–a policy and organisational perspective, Lee Kuan Yew School of Public Policy, National University of Singapore.

[63] S. Keon, H. Rain, H. Cho, J. Kim, D. Lee, International case studies of smart cities–singapore, republic of singapore, inter-american development bank, Recuperado de https://publications. iadb. org/handle/11319/7723.

[64] C. NewsAsia, National cybersecurity strategy aims to make smart nation safe: Pm lee, http://www.channelnewsasia.com/news/singapore/national-cybersecurity-strategy-aims-to-make-smart-nation-safe-p-7743784, [Accessed 8 Sep. 2017] (2017).

[65] S. C. World, Cyber security lab opens in singapore, https://smartcitiesworld.net/news/news/cyber-security-lab-opens-in-singapore-1047, [Accessed 7 Sep 2017] (2017).

[66] S. Singapore, Setting the standard worldwide: intelligent city, smart nation.

[67] S. L. Board, Smart london plan, Retrieved August.

[68] M. Angelidou, Four european smart city strategies, Int'l J. Soc. Sci. Stud. 4 (2016) 18.

[69] S. L. I. Networks, The challenges – smart london innovation networks, http://smarterlondon.co.uk/the-challenges/, [Accessed 7 Sep. 2017] (2017).

[70] H. L. Lee, S. Whang, Information sharing in a supply chain, International Journal of Manufacturing Technology and Management 1 (1) (2000) 79–93.

[71] I. S. Association, Internet of things (iot) ecosystem study, [Accessed 24 Jun. 2015] (2015).

[72] I. Global, Security risks survey 2015: The current state of play [ ], : http://media. kaspersky. com/en/business-security/it-security-risks-survey-2015. pdf (11.01. 2017).

[73] Phys.org., 'worrying lack of strategy' for u.k. smart cities, https://phys.org/news/2017-05-lack-strategy-uk-smart-cities.html, [Accessed 24 Jun 2017] (2017).

[74] D. BACHLECHNER, M. FRIEDEWALD, T. MITCHENER-NISSEN, M. LAGAZIO, A. KUNG, Cyber security for smart cities, https://www.google.co.uk/url?sa=t\&rct=j\&q=\&esrc=s\&source=web\&cd=2\&cad=rja\&uact=8\&ved=0ahUKEwiulIX3qI7VAhVsJsAKHQHeCmIQFggoMAE\&url=https\%3A\%2F\%2Fwww.enisa.europa.eu\%2Fpublications\%2Fsmart-cities-architecture-model\%2Fat_download\%2FfullReport\&usg=AFQjCNF2ONtjlM8qwPL7n7QXIoeJRyzVqQ, [Accessed 16 Jul 2017] (2017).

## Appendix A. Standards Related to IoT or Smart Cities

Table A.3: Standards Related to IoT or Smart Cities

| No. | Document ID | Title | Body |
|---|---|---|---|
| 1. | ANSI/ASQ E 4 | Specifications and guidelines for quality systems for environmental data collection and environmental technology programs | ANSI |
| 2. | BS EN 14908-5:2009 | Open data communication in building automation, controls and building management implementation guideline - Control network protocol - Implementation | CEN |
| 3. | BS EN 60730-1:1992 | Specification for automatic electrical controls for household and similar use - General requirements | CEN |
| 4. | BS ISO 14813-1:2007 | Intelligent transport systems - Reference model architecture(s) for the ITS sector - ITS service domains, service groups and services | ISO |
| 5. | CR 205-006:1996 en | Home and building electronics system (HBES) - Technical report 6: Protocol and data integrity and interfaces | NEN |
| 6. | CSN ISO/IEC TR 15067-3 | Information technology - Home electronic system (HES) application model - Part 3: Model of an energy management system for HES | ISO/IEC |
| 7. | CWA 14947:2004 en | European eConstruction architecture (EeA) | CEN |
| 8. | CWA 15264-3:2005 | User requirements for a European interoperable eID system within a smart card infrastructure | CEN |
| 9. | DD CEN/TS 13149-6:2005 | Public transport - Road vehicle scheduling and control systems - CAN message content | CEN |
| 10. | DIN SPEC 33440 | Ergonomic design of user-interfaces and products for smart grid and electro-mobility | DIN |
| 11. | DS/EN 61970-1 | Energy management system application program interface (EMS-API) - Part 1: Guidelines and general requirements | IEC |
| 12. | EIA TSB 4940 | Smart device communications - Security aspects | EIA |
| 13. | ETSI GS OSG 001 V 1.1.1 | Open smart grid protocol (OSGP) | ETSI |
| 14. | ETSI TR 102935 V 2.1.1 | Machine-to-Machine communications (M2M) - Applicability of M2M architecture to smart grid networks - Impact of smart grids on M2M platform | ETSI |
| 15. | GOST R 55060 | Automatized control systems of buildings and structures. Terms and definitions | GOST R |
| 16. | IEC 62290-1 | Railway applications - Urban guided transport management and command/control systems Part 1: System principles and fundamental concepts | IEC |
| 17. | IEEE 1851 | IEEE standard for design criteria of integrated sensor-based test applications for household appliances | IEEE |

Table A.3: (continued)

| No. | Document ID | Title | Body |
|---|---|---|---|
| 18. | ISO 15118-1 | Road vehicles - Vehicle to grid communication interface - Part 1: General information and use-case definition | ISO |
| 19. | ISO 16484-5 | Building automation and control systems - Part 5: Data communication protocol | ISO |
| 20. | ISO/PAS 22720 | Association for standardization of automation and measuring systems open data services 5.0 | ISO |
| 21. | ISO/TS 24533 | Intelligent transport systems - Electronic information exchange to facilitate the movement of freight and its intermodal transfer - Road transport information exchange methodology | ISO |
| 22. | ITU-T X.207 | Information technology - Open systems interconnection - Application layer structure | ITU |
| 23. | NEMA SG-AMI 1 | Requirements for smart meter upgradeability | NEMA |
| 24. | NEN 7512:2005 nl | Health informatics - Information security in the healthcare sector - Basis for trust for exchange of data | NEN |
| 25. | NEN-EN-ISO 24534-3:2013 | Intelligent transport systems - Automatic vehicle and equipment identification - Electronic registration identification (ERI) for vehicles - Part 3: Vehicle data | CEN |
| 26. | NPR-CEN/TR 16427:2013 en | Intelligent transport systems - Public transport - Traveller information for visually impaired people (TI-VIP) | CEN |
| 27. | OEVE B/EN 60555-1/1987 | Disturbances in supply systems caused by household appliances and similar electrical equipment - Part 1: Definitions | OVE |
| 28. | PAS 1018 | Essential structure for the description of services in the procurement stage | DIN |
| 29. | PAS 1090 | Demands on information systems for collecting, communicating and serving of relevant service information within the technical customer service | DIN |
| 30. | PAS 555:2013 | Cyber security risk - Governance and management - Specification | BSI |
| 31. | SS-ISO 15784-1:2008 | Intellligent transport systems (ITS) - Data exchange involving roadside modules communication - Part 1: General principles and documentation framework of application profiles (ISO 15784-1:2008, IDT) | ISO |
| 32. | UTE C15-900U*UTE C15-900 | Coexistence between communication and power networks - Implementation of communication networks | UTE |
| 33. | VDI 3814 Blatt 7 | Building automation and control systems (BACS) - Design of user interfaces | VDI |

Table A.3: (continued)

| No. | Document ID | Title | Body |
|---|---|---|---|
| 34. | VDI 4201 Blatt 1 | Performance criteria on automated measuring and electronic data evaluation systems for monitoring emissions - Digital interface - General requirements | VDI/DIN |
| 35. | BS ISO 20121 | Event sustainability management systems - Requirements with guidance for use | ISO |
| 36. | ASTM E 1121 | Standard practice for measuring payback for investments in buildings and building systems | ASTM |
| 37. | BIP 2207 | Building information management - A standard framework and guide to BS 1192 | BSI |
| 38. | BS 8587:2012 | Guide to facility information management | BSI |
| 39. | BS 8903:2010 | Principles and framework for procuring sustainably - Guide | BSI |
| 40. | CAN/CSA-ISO/TS 14048:03 (R2012) | Environmental management - Life cycle assessment - Data documentation format | CSA |
| 41. | CWA 15666:2007 en | Business requirement specification - Cross industry e-Tendering process | CEN |
| 42. | CWA 15971-1 | Discovery of and access to eGovernment resources - Part 1: Introduction and overview | CEN |
| 43. | CWA 16649:2013 en | Managing emerging technology-related risks | CEN |
| 44. | CWA 50487:2005 en | SmartHouse Code of Practice | CEN |
| 45. | DS/ISO/IEC 18012-2 | Information technology - Home electronic system - Guidelines for product interoperability - Part 2: Taxonomy and application interoperability model | ISO/IEC |
| 46. | ISO 16484-1 | Building automation and control systems (BACS) - Part 1: Project specification and implementation | ISO |
| 47. | ITU-T L.1410 | Methodology for the assessment of the environmental impact of information and communication technology goods, networks and services | ITU |
| 48. | NEN-ISO 29481-2:2012 en | Building information models - Information delivery manual - Part 2: Interaction framework | ISO |
| 49. | NPR-ISO/TR 12859:2009 en | Intelligent transport systems - System architecture - Privacy aspects in ITS standards and systems | ISO/TR |
| 50. | RAL-UZ 170 | Basic criteria for award of the environmental label - Energy services provided under guaranteed energy savings contracts | RAL Güte |
| 51. | SS-ISO/IEC 27005:2013 | Information technology - Security techniques - Information security risk management | ISO/IEC |

Table A.3: (continued)

| No. | Document ID | Title | Body |
|---|---|---|---|
| 52. | VDI 3814 Blatt 5 | Building automation and control system (BACS) - Advices for system integration | VDI |
| 53. | VDI 4466 Blatt 1 | Automatic parking systems - Basic principles | VDI |
| 54. | VDI 7000 | Early public participation in industrial and infrastructure projects | VDI |
| 55. | VDI/GEFMA 3814 Blatt 3.1 | Building automation and control systems (BACS) - Guidance for technical building management - Planning, operation, and maintenance - Interface to facility management | GEFMA |
| 56. | BS ISO 37120 | Sustainable development and resilience of communities - Indicators for city services and quality of life | ISO |
| 57. | BS ISO/TR 37150 | Smart community infrastructures - Review of existing activities relevant to metrics | ISO |
| 58. | ABNT NBR 14022 | Accessibility in vehicles of urban characteristics for public transport of passengers | ABNT |
| 59. | BIP 2228:2013 | Inclusive urban design - A guide to creating accessible public spaces | BSI |
| 60. | BS 7000-6:2005 | Design management systems - Managing inclusive design - Guide | BSI |
| 61. | BS 8904:2011 | Guidance for community sustainable development | BSI |
| 62. | CLC/FprTR 50608 | Smart grid projects in Europe | CENELEC |
| 63. | CWA 15245 | EU e-Government metadata framework | CEN |
| 64. | CWA 16030:2009 | Code of practice for implementing quality in mobility management in small and medium sized cities | CEN |
| 65. | CWA 16267:2011 | Guidelines for sustainable development of historic and cultural cities - Qualicities | CEN |
| 66. | DIN SPEC 91280 | Ambient assisted living (AAL) - Classification of ambient assistant living services in the home environment and immediate vicinity of the home | DIN |
| 67. | GOST R 54198 | Resources saving - Industrial production - Guidance on the application of the best available technologies for increasing the energy efficiency | GOST R |
| 68. | PAS 181:2014 | Smart city framework - Guide to establishing strategies for smart cities and communities | BSI |
| 69. | UNI 10951:2001 | Systems of information for the maintenance management of buildings - Guidelines | UNI |
| 70. | Z762-95 (R2011) | Design for the environment (DFE) | CSA |

Table A.3: (continued)

| No. | Document ID | Title | Body |
|---|---|---|---|
| 71. | IEEE 1363 series | Standards define specifications for public key cryptography | IEEE |
| 72. | IEEE 1619 series | Standards define specifications for encryption in storage media | IEEE |
| 73. | IEEE P24151-1-4 | Standard for Smart Transducer Interface for Sensors, Actuators and Devices - eXtensible Messaging and Presence Protocol (XMPP) - currently being developed, specifically addresses security | IEEE |
| 74. | IEEE 1451/21450/21451 | Series of standards for sensors and actuators | IEEE |
| 75. | IEEE 2410-2015 | IEEE standard for Biometric Open Protocol | IEEE |
| 76. | IEEE P1912 | Standard for Privacy and Security Architecture for Consumer Wireless Devices - currently being developed | IEEE |
| 77. | IEEE 802.1X-2020 | IEEE Standard for Local and metropolitan area networks-Port-Based Network Access Control | IEEE |
| 78. | IEEE 802.1AE-2006 | IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security; Security capabilities expanded by IEEE 802.1AEbw-2013. | IEEE |
| 79. | IEEE 802.1AR-2009 | Standard for Local and metropolitan area networks - Secure Device Identity | IEEE |
| 80. | IEEE 11-2012 series | IEEE Standard for Information technology-Telecommunications and information exchange between systems Local and metropolitan area networks-Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications | IEEE |
| 81. | IEEE 802.15.4-2015 | IEEE Standard for Local and metropolitan area networks-Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) | IEEE |
| 82. | IEEE 802.21a-2012 | IEEE Standard for Local and Metropolitan Area Networks: Media Independent Handover Services - Amendment for Security Extensions to Media Independent Handover Services and Protocol | IEEE |
| 83. | IEEE 1888 series | IEEE Standard for Ubiquitous Green Community Control Network Protocol and its security | IEEE |
| 84. | IEEE 692-2013 | IEEE Standard for Criteria for Security Systems for Nuclear Power Generating Stations | IEEE |
| 85. | IEEE C37.240-2014 | IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems | IEEE |
| 86. | IEEE 1686-2013 | IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities | IEEE |

Table A.3: (continued)

| No. | Document ID | Title | Body |
|---|---|---|---|
| 87. | PAS 180 | Smart city terminology | BSI |
| 88. | PAS 182 | Data concept model for smart cities | BSI |
| 89. | PAS 184 | Project proposals for delivering smart city | BSI |
| 90. | PD 8100 | Smart city overview document BSI | |
| 91. | PD8101 | Smart city planning guidelines document | BSI |
| 92. | BS ISO/IEC30182:2017 | Smart city concept model | BSI |
| 93. | PD ISO/TR 37121:2017 | Standard on inventory of existing guidelines and approaches on sustainable development and resilience in cities | BSI |