smart cities

MDPI

Article

Digital Systems in Smart City and Infrastructure: Digital as a Service

Will Serrano

Intelligent Systems and Networks Group, Imperial College London, London SW7 2AZ, UK; g.serrano11@imperial@ac.uk

Received: 21 October 2018; Accepted: 5 November 2018; Published: 6 November 2018

check for updates

Abstract: Digitalization has enabled infrastructure and cities to be "smarter"; the use of physical space and energy, the transmission of information, the management of users, assets and processes, the operation of businesses and companies have been progressively digitalized. The main challenges of a Smart City is its definition, scope and interconnections; there are different approaches to Smart City implementations that vary from collaborative multidisciplinary environments, the addition of Information and Communications Technology (ICT) within its physical fabric to the use of Big Data for higher abstraction decisions. This paper presents the concept of Digital as a Service (DaaS), where any complete digitalization can be implemented independently of its associated physical infrastructure in a Cloud environment; DasS would enable an interoperable Virtual Digital Infrastructure (VDI). In addition, this paper reviews the current Digital Systems, Transmission Networks, Servers and Management Systems. The next Industrial Revolution will be founded on Artificial Intelligence that will entirely replace humans by taking production and management decisions based on the Internet of Things (IoT), the Cloud, BlockChain, Big Data, Virtual Reality and the combination of digital and real infrastructure or city. Digital as a Service would be its enabler by providing the entire interconnection, integration and virtualization of its Space, Services and Structure (3S).

Keywords: Digitalization; Cloud Environment; Smart Infrastructure; Smart City; Smart Grids; Artificial Intelligence; Telecommunication Networks

1. Introduction

Digitalization has enabled infrastructure to become smarter. The optimum use of physical space and energy, the proactive management of users, assets and processes, the efficient operation of businesses and companies have gradually benefited from the digitalization process. Countries that have introduced digitization not only in the manufacturing sector such as the use of Robotics or Internet of Things (IoT), but also in wider Smart Cities solutions, including e-healthcare or Smart Grids, have benefited from an increment of gross domestic product (GDP) [1] due to the reduction of the final Operational Cost (OPEX). The main challenge to implement a Smart City is its definition and scope; the concept of Smart City varies between pure electronic solutions integrated into the Smart city Information and Communications Technology (ICT) infrastructure such as IoT, the cloud or mobile phones and Big Data with Analytics that measures in real time its status usage that allows higher level decisions. In addition, Smart City can be implemented as frameworks and processes as government collaborative multidisciplinary environments that empower its citizens. The ICT component of the Smart City generates technical challenges based on the interoperability of the different enabling technologies, communication transmission protocols and architecture developed by independent manufactures.

The key service enabled by technology for the energy resources of a Smart City is applied on its electrical distribution or Smart Grids [2], based on its three drivers Decarbonization, Digitalization and

Decentralization [3]. The efficient monitoring and management of electricity through its entire process, generation, transmission, distribution and storage will enable Smart Cities and Infrastructure to meet their variable and increasing power demands in carbon free environments that protects its citizens and users against CO_2 emissions. Smart Cities are also represented as large scale combination of networks with interdependent interactions [4]; the Smart City model can be defined, analyzed and optimized in order to make it sustainable. The digital twin will not be only based on a Building Information Modeling (BIM) resembling the physical infrastructure; Smart City models will converge and merge into the artificial city: the Internet and the Web.

Smart cities must have drivers in order to be effective; success can be measured as increment of the quality of life of its citizens while providing a return of investment. Those drivers shall include a broad range of areas of expertise: applied social sciences, engineering, Earth sciences, and human sciences [5]. Project management applied to Smart Cities sets up stakeholder requirements via an independent and temporal delivery organization that supervises the design, construction, handover and operations [6]. The delivery organization shall produce fit-for-purpose and high quality deliverables with connections to the digital platform on Time, Budget and Scope, following the triangle of project management.

The Forth Industrial Revolution [7] started with the introduction of Digitalization in the IoT, the Cloud, Blockchain, Virtualization, Robotics and Driverless vehicles that have replaced humans in routine actions, increased productivity and reduced cost. The Fifth Industrial revolution will be founded on Artificial Intelligence and Deep Learning that will entirely replace humans by taking production and management decisions.

This paper presents the concept of Digital as a Service (DaaS) where any complete digitalization can be implemented independently of its associated physical infrastructure; DaaS would enable an interoperable Virtual Digital Infrastructure. Digital as a Service focuses in the Digitalization applied to the built infrastructure, or "Smart Infrastructure" that eventually will be the foundation of a Smart City or Smart Country where their independent elements and systems are interconnected, integrated and virtualized. Once the smart city functional parts are interconnected; higher abstraction structures can be developed to increase efficiency and complexity; this will increase performance, provide additional higher abstraction services while reducing operational and maintenance costs. Digital as a Service would be the Fifth Revolution enabler by providing the entire interconnection independent sensors, assets or components, integration of information or the "Big Data" and virtualization of its Space, Services and Structure (3S).

A review of Smart Cities and digitalization is presented on Section 2; this includes its different definitions, collaboration approaches, Information and Communication Technology consideration, Big Data application, Energy requirements and the Blockchain. The evolution of digitalization based on a Sensor, Network, Server and Workstation approach is described on Section 3. The concept and mathematical model of DaaS is defined on Section 4. Digital as a Service components: Digital Systems, Digital Transmission, Digital Servers and Digital Management are detailed from Section 5 to Section 8 respectively. Final challenges and conclusions are presented on Sections 9 and 10.

2. Research Background

2.1. Definition

Many definitions of Smart City exist, but no single definition has been universally accepted yet [8]. From literature analysis it appears that Smart City and Digital City are the most commonly used terms in academic research to define the "intelligence" of a city. An overview from different research publications focuses on what it means for cities to be "Smart" [9]; the study concludes the numerous claims are self-congratulatory with high dependency on a fixed distinctively entrepreneurial route map to develop them. A framework to understand the concept of smart cities is based on eight critical factors: management and organization, technology, governance, policy context, people and communities, economy, built infrastructure, and natural environment [10]; these factors form the basis of an integrative framework that proposes directions and agendas to local governments for foreseeing smart city initiatives. The concept of smart city and its relationship with digital city has been defined [11] based on the main content of application systems, the challenges of its constructability and its influences of its development. The smart city infrastructure is the first step for establishing the overall smart city framework and architecture [12]; its development framework and the positional accuracy of locating the assets as a base of the smart city development architecture integrated with all the facilities and systems are related to the smart city framework. The Smart City concept is not being used by the United Nations (U.N.) as it is still evolving and perceived as a branding exercise [13] by private corporations; the U.N. cultural agenda requires cities to be more "inclusive, safe, resilient, and sustainable" which includes values, cultural and historical profiles that some cities have inherited since their creation and evolution.

2.2. Collaboration

Smart Cities are analyzed as environments of open and user driven innovation for experimenting and validating future research Internet enabled services and city trial programmes [14]; an effective use of common resources for the purpose of establishing innovation ecosystems requires sustainable partnerships and collaboration strategies between stakeholders. Professional communities have been formed to promote mutual learning between multidisciplinary members of the architecture, planning, engineering, transportation, utilities, information technology, operations research, social sciences, geography and environmental science, public finance and policy, and communications [15]; the outcome is a new theory of cities based on innovative, and wide sources of information about what is happening in the city in almost real time. It seeks to analyze the consequences of information technology in the urban fabric and norms of behaviour. A set of the common multidimensional components underlying the smart city concept including (technology, people, and institutions) [16] and the core factors for a successful smart city initiative are described as integration of infrastructures and technology related services, social learning for strengthening human infrastructure, and governance for institutional improvement and citizen engagement.

2.3. Information and Communications Technology

A smart city is defined as a city in which ICT is merged with classic infrastructures, coordinated and integrated using new digital technologies [17]. The smart vision is sketched by defining goals, adding research challenges and considering scenarios within project areas. The concept of smart and connected communities is based on the IoT, crowd sensing and cyber-physical cloud computing to provide a comprehensive network of connected devices [18]; in addition smart sensors and big data analytics to enable the move from IoT to real-time control. An urban IoT is designed to support the Smart City vision that exploits the most advanced communication technologies to enable added value services for the administration of the city and for the citizens [19]; the urban IoT optimizes enabling technologies, protocols, and architecture with best technical solutions and practice guidelines. The smart mobile phones with sensor enabled technology such as Global Positioning System (GPS), gyroscope, microphone, camera, accelerometer [20] also provide new innovative services within the Smart City architecture and framework. The concept of Sensing as a Service is explored in technological, economic and social perspectives [21]; the research also identifies the major open challenges and issues including the methods to interconnect it in current IoT infrastructure, platforms and software applications offered as services using cloud technologies. The recent vision of the Future Internet (FI), and its particular components, IoT and Internet of Services (IoS) can become building blocks to progress towards a unified urban-scale ICT platform transforming a Smart City into an open innovation platform [22]; the proposed generic implementation is based on an Ubiquitous Sensor Network (USN) model that meets the requirements of open, federated and trusted platforms. The main challenges that may prevent the IoT to substantially support sustainable development of future smart cities are the disparity between connected objects and the unreliable nature of associated services [23];

a cognitive framework which dynamically changing real-world objects are represented in a virtualized environment, and where cognition and proximity are used to select the most relevant objects for the purpose of an application in an intelligent and autonomic way.

2.4. Big Data

A smart city infrastructure is based on the concept of the digital city that integrates the Internet of Things and cloud computing technologies [24], to enable automatic control and intelligence services for people and logistics in physical cities; the application of Big Data to smart cities includes an extensive sensor networks with problems and challenges that can be mitigated deploying cloud computing and data mining. There is a gap in combining the current state of the art in an integrated Big Data and Machine Learning analytical applications for IoT and Smart City application framework [25] that would help reducing development costs and enable new analytical services for citizens and urban decision makers. Big data analytics have a huge potential to enhance smart city services [26]; however, the understanding of the requirements that support its implementation and applications are key to the effective analysis and utilization to deliver success in smart city service domains. The combination of the IoT and Big Data is still an immature unexplored research with new and interesting challenges for achieving the goal of future smart cities [27]; the difficulties focus primarily on the awareness of the main smart environment characteristics and the collaboration between the technology and the business services that enable smart cities to improve their vision and principles.

Big Data Smart City applications and potentials will be able to understand its environment through analyzing its data in order to immediately make changes to solve issues and to improve the residents' quality of life [28]; data requires to be collected from all networks, devices and sensors embedded in its infrastructure; it becomes valuable by passing different processing stages, by applying advanced analyzing Big Data platforms on data and finally by exporting the data in useful platform in order to improve any city's system application. Urban big data streamed from city sensors will become a source for smart city information [29] that will enable longer term strategic planning instead to short-term thinking about how cities function and can be managed. Two closely related emerging technology frameworks, the Internet of Things and Big Data can make smart cities efficient and responsive [30]; however, these technological advances require to be integrated in terms of physical infrastructure where digital technologies translate into better public services for inhabitants and better use of resources while reducing environmental impacts.

2.5. Energy

The hierarchical, centrally controlled energy grid does not fit the needs of Smart Cities. Smart Grids increase throughput and efficiency by optimizing demand, energy and network availability. In order to provide reliable and real time monitoring information that enables a flexible operation, Smart Grids require Security, Quality of Service (QoS) in data transmission networks and Technology Standards for interoperability [31] where ICT plays a fundamental element in its growth and performance. A reliable and fast communication infrastructure [32] is necessary for the connection among the great number of distributed elements, such as generators, substations, distribution, transmission, storage and users [33]. Smart Grids can also be included into frameworks that seek a return of investment between producers, operators and customers; these frameworks are divided into three interactive smart components [34]: smart control centers, smart transmission networks, and smart substations. The key challenges for Smart Grids include the communications interoperability between the Smart Grid and the Smart Meter and the communications network reliability, availability, latency and QoS in wireless environments subject to Denial of Service (DoS) attacks [35]. The standardization effort to harmonize communications standards and protocols is coordinated through Europe, US and China [36]. A survey of Smart Grids [37] consists on its three major systems: smart infrastructure, management and protection. The survey covers the smart energy, information, security and communication subsystems in addition to management objectives such as improving energy efficiency, profiling demand, maximizing utility, reducing cost, and controlling emission.

In addition to Smart Cities, the enabler ICT also requires an increasing amount of dispersed energy for its data centres and communications transmission equipment. Energy Packet Networks (EPN) uses energy storage units to adapt to the irregular supply of renewable energy sources and intermittent demand of cloud computing servers [38]. The EPN model stores and distributes quantised energy units, or Energy Packets, to and from a large range of devices based on mechanisms analogue to computer networks [39]. Energy Packets are managed and optimized by energy dispatching centres which receive requests from consumer's storage centres that wish to be replenished [40].

2.6. Block Chain

BlockChain enables the digitalization of contracts as it provides authentication between parties and information encryption of data that gradually increments while it is processed in a decentralized network. The BlockChain technology has the potential to disrupt the world of banking through enabling cryptocurrencies [41] global money transfers, payment solution [42] smart contracts [43], automated banking records and digital assets [44] in addition to providing user anonymity [45]. Decentralized personal data management systems based on Blockchain ensure users the own control of their data [46] and digital content distribution operated by user rights [47]. The decentralization of a consensus method that uses a credibility score is applied to contracts management such as digital rights management [48].

The Blockchain has already been applied in Smart Grids by providing energy transaction security in decentralized trading [49], Intelligent Transport Systems on a seven layer conceptual model that emulates the OSI model [50], Smart Devices providing a secure communication platform in a Smart City [51], control and configure devices for the Internet of Things [52], Smart Homes [53] and Digital Documentation [54].

3. Digitalization Evolution

Digitalization has been incorporated gradually into Infrastructure in four different Stages: Silo Approach, Shared Network, Shared Workstation and Shared Server.

3.1. Silo Approach

Originally; ICT was developed in a silo approach where each digital system was independent and dedicated to a function with its own communications infrastructure, server and workstation. Although the first systems were electronic; they mostly used analogue methods to capture, transmit and process information therefore limiting integration (Figure 1).

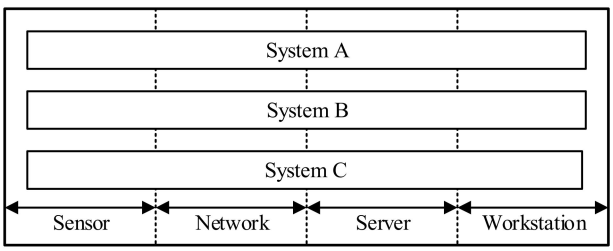

Figure 1. Digitalization: Silo Approach.

3.2. Shared Network

The first digital systems focused on the communications infrastructure. Internet Protocol (IP) and Local Area Networks (LAN) enabled the transmission of information on shared switches and routers, where each digital system had an associated Virtual LAN. The benefits of the shared network enabled the flexibility of common cabling, switching and routing infrastructure that allowed the protocol independency of digital IP systems as information was transmitted in a common IP Layer 3, Ethernet Layer 2 (Figure 2).

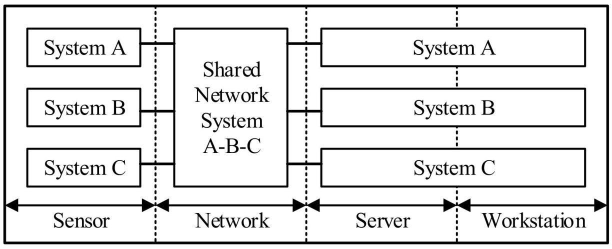

Figure 2. Digitalization: Shared Network.

3.3. Shared Workstation

The next digital stage was the combination of workstations into a single management desktop with the use of system integrator software that merges the data feeds from the different Systems showing to the user a single Graphical User Interface (GUI). This unification approach led to the development of Management Systems that perform data analytics, automate operators' tasks and filter alarms. In addition, management workstations do not have to be physically in the Smart infrastructure with the use of Virtual Private Networks. Remote Management, with increased level of resiliency, separates control and infrastructure (Figure 3).

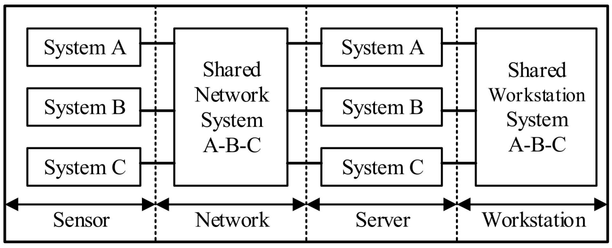

Figure 3. Digitalization: Shared Workstation.

3.4. Shared Server

Finally, server capacity, defined as CPU and memory, is shared in virtual private or public cloud applications hosted in datacenters. Server virtualization eliminates the requirement to deploy dedicated servers installed physically in the Smart Infrastructure. Shared servers can be privately hosted within the Smart Infrastructure in Communications Equipment Rooms or remotely installed in Datacenters. The benefits of the Shared server is reduces Operational Cost (OPEX) and Capital Expenditure (CAPEX) with a simple management as Server usage can be optimized based on user demand (Figure 4).

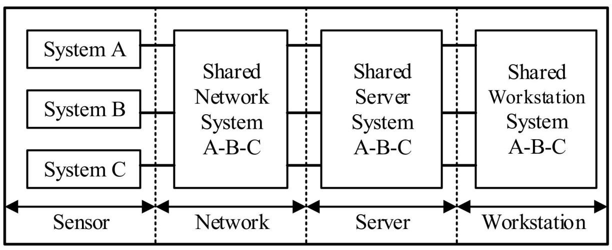

Figure 4. Digitalization: Shared Server.

3.5. Next Step

Gradually; independent Control Centres have been combined in dedicated remote locations with access via Virtual Private Networks. Virtual Reality, Laptops or Mobile devices eliminate the requirement for physical electronic components such as Telephones, Video Walls or monitors; the human operator does not need to be physically in the control centre to manage the smart infrastructure. Artificial Intelligence will finally remove entirely the need for a human itself; management will be hosted in the same Datacenters where the servers are hosted (Figure 5).

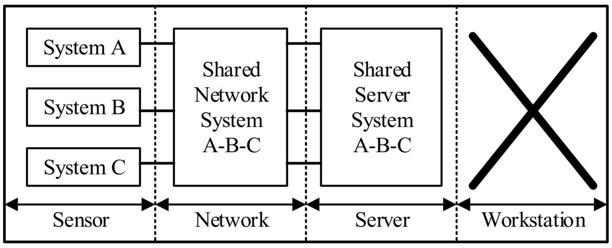

Figure 5. Digitalization: Next Step.

4. Digital as a Service

Digital as a Service, or DaaS, abstracts the Digital Infrastructure regardless of the Physical Infrastructure properties in a Cloud enviroment. Digital as a Service would enable an interoperable Virtual Digital Infrastructure providing a higher layer that manages and virtualizes the Digital Infrastructure divided into four elements described on the next sections: Digital Systems, Transmission, Servers and Workstations (Figure 6).

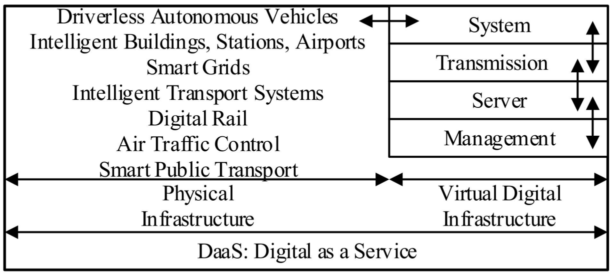

Figure 6. DaaS: Digital as a Service.

The Digital Systems will provide the sensors to the Physical Infrastructure in order to enable the interaction of information. The sensors functionality will range from managing assets, industrial processes and equipment to enable the communications between users via mobile devices. The Digital systems will be designed to adapt physically to the Smart Infrastructure while providing optimum coverage, resilience and performance (Appendix A).

The Digital Transmission will enable the communication between sensors using wired solutions such Local Area Networks, Private Wide Area Networks and public Internet Service Providers (ISP) or Wireless solutions including Global System for Mobile (GSM)/Long Term Evolution (LTE), Trunked Radio, Wi-Fi, Bluetooth, Radio Frequency Identification (RFID) and Near Field Communications (NFC). The Digital Transmission technology will adapt to the Digital Systems requirements such as Quality of Service (QoS), bandwidth, number of users and coverage.

The Digital Servers will manage the Digital Systems and Transmission Networks. Data interfaces between servers will enable the IoT, Software Defined Networks (SDN) with BlockChain to provide data security and decentralization when hosted virtualized in a cloud. The higher level of virtualization of CPU and Memory will provide additional reliability of the Smart Infrastructure at a reduced CAPEX cost.

The Digital Management will operate and manage the Smart Infrastructure via system integration where data feeds from the servers are combined. A higher level of integration will enable Big Data Analytics for holistic management decisions that will lead to a more efficient resource, asset and user management to reduce OPEX costs. Digital Management will enable the digital twin between real and virtual infrastructure.

The Digital experience provided by DaaS will abstract the Digital Systems, Transmission, Servers and Management (Figure 7). The Virtual Digital Infrastructure will be accessed via a common transparent platform tailored adapted to the user functionality and role.

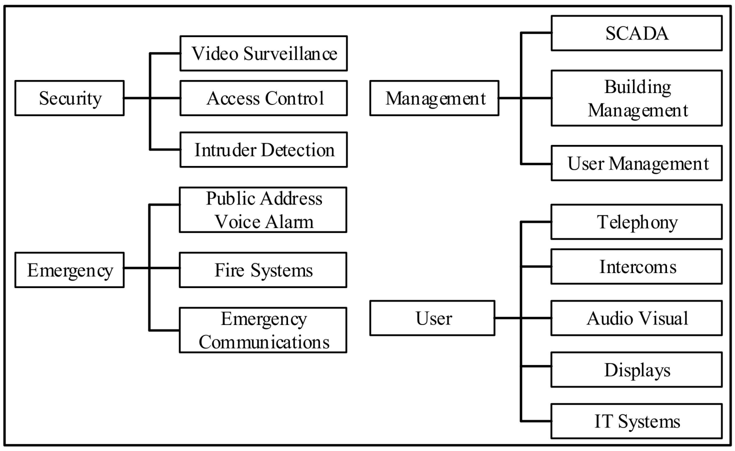

Figure 7. Digital as a Service (DaaS): Digital Experience.

Digital as a Service abstracts the underlying digital technologies in a Cloud environment to provide a flexible, expandable and modular interoperable Virtual Digital Infrastructure (VDI) where independent Physical Infrastructures (PI) will be integrated such as Autonomous Vehicles, Intelligent Buildings and the Smart Grid.

DaaS defines the Virtual Digital Infrastructure model:

- PI = $\{P_{\text{Infrastructure-1}}, P_{\text{Infrastructure-2}}, \ldots P_{\text{Infrastructure-m}}\}$ as a set a set of m Physical Infrastructures $P_{\text{Infrastructure}}$;
- VDI = $\{dvi_1, dvi_2, \ldots dvi_n\}$ as a set of n dvi vectors associated to one or several Physical Infrastructures $P_{\text{Infrastructure}}$;
- dvi = $\{v_{\text{System}}, v_{\text{Transmission}}, v_{\text{Server}}, v_{\text{Management}}\}$ as a set that consists of the four Virtual Digitalizations;
- $v_{\text{System}} = (v_{\text{System-1}}, v_{\text{System-2}}, v_{\text{System-p}})$ as a P dimensional vector that represents the Digital Systems;
- $v_{\text{Transmission}} = (v_{\text{Transmission-1}}, v_{\text{Transmission-2}}, v_{\text{Transmission-q}})$ as a Q Dimensional vector that represents the Digital Transmissions;
- $v_{\text{Server}} = (v_{\text{Server-1}}, v_{\text{Server-2}}, v_{\text{Server-r}})$ as a R Dimensional vector that represents the Digital Servers;
- $v_{\text{Management}} = (v_{\text{Management-1}}, v_{\text{Management-2}}, v_{\text{Management-s}})$ as a S Dimensional vector that represents the Digital Managements.

Theoretically; DaaS enables a single Virtual Digital infrastructure that manages the entire set of physical infrastructures with a modular Virtual Management layer (Figure 8).

Physical Infrastructure (PI)			
Digital System	Digital Transmission	Digital Server	Digital Management
Voice Video Data	Wired Radio Mobile Satellite	CPU Memory Power	Integration Artificial Intelligence User
Virtual System (v_{System})	Virtual Transmission $(v_{Transmission})$	Virtual Server (v_{Server})	Virtual Management $(v_{Management})$
Virtual Digital Infrastructure (VDI) Digital as a Service (DaaS)			

Figure 8. Virtual Digital Infrastructure.

5. Digital Systems

There are several Digital Systems, or sensors, that monitor the Smart Infrastructure enabling its interaction with the environment. The relevant Digital Systems are classified according to their function.

5.1. Security Systems

Security Systems protect and monitor electronically the Smart Infrastructure against threats, reducing risks and vulnerabilities and deterring potential attackers.

Closed Circuit TeleVision (CCTV) or Video Surveillance System (VSS) [55,56] capture images and video frames of the smart infrastructure for security purposes using video cameras. Video analytics enable automatic alarm generation that can be filtered according to its priority and event trace that retrieves frames with relevant properties, such as user faces. Usually video streams are recorded for crime evidential reasons. Once face recognition technology becomes widely adopted; this can enable the use of images as a biometric tool associated to other identification functionalities such as ticketing.

Access Control [57] manages the user access to the Smart Infrastructure via smart cards, mobile app certificates or user biometrics. Security Zones are established with different priorities where physical access is limited to user credentials. Access Control also enables to track user's room location in case of emergency or evacuation.

Intruder Detection [58] monitors unauthorized access to the Smart Infrastructure. The main sensors are based on physical properties such as infrared, sound, pressure and volumetric metrics inherent to any physical attacker. Usually, a combination of different sensors is applied to increase the defense on depth.

5.2. Voice and Telephony

Telephony systems transmit mostly voice that enables full duplex communications between two users, although the use of digital call centers and Artificial Intelligence may reduce the human input on the receiving call.

Intercoms enable Smart Infrastructure users to communicate with security operators or operations staff mostly to request access through a locked door such as back of house or car park. Normally Intercoms have an integrated video camera for audio visual communications. They are mostly used as a fall back operation if the Access Control credentials can not be validated such as when the user is a visitor or has forgotten the card. The increased use of tactile screens enables the use of intercoms with card readers where different buttons can prioritize and direct calls such as Information or Emergency.

Telephones allow voice communication between users. Originally Telephones were standalone handsets; however, the use of Session Internet Protocol (SIP) enabled the transmission of Voice over IP integrated in a Laptop or Mobile Phone.

5.3. Emergency Systems

Emergency Systems are required in case of fire evacuation, mostly used to guide users in emergency scenarios by emergency services. These systems follow very strict requirements and Standards such as the use of Uninterruptible Power Supply (UPS) and Fire grade cabling and equipment.

The Public Address/Voice Alarm (PA/VA) [59] system serves a dual functionality. The PA provides general information audio announcements related to the purpose of the Smart Infrastructure. The VA provides emergency announcements that will guide users in case of emergency or fire. Both PA/VA systems can be zoned to enable segregated acoustic information and announcements.

Emergency Communications [60] are installed in refuge areas or Fire lift lobbies to enable the communication between users and the Fire Brigade in fire protected environments. The handsets are fixed, wall mounted and normally hard wired to the server without the use of a Digital IP communications layer.

Fire System [61,62] detects fire using heat or smoke detectors. It provides an audio visual alarm via beacons and sounders to alert users of a fire and start an evacuation. If the Smart Infrastructure has also Voice Alarm, then both systems will be directly interconnected, therefore when fire is detected, it will automatically trigger intelligible alert.

5.4. Information Systems

Information Systems show data to users via visual sensors. Information varies from relevant to the user in order to navigate through the Smart Infrastructure, show real time notifications or data to generate revenue such as advertising.

Audio Visual Systems include provide the teleconferencing functionality in meeting, control and conference rooms, such as Smart boards and multipurpose voice devices.

Displays Systems provide the physical screens and the data feed with the information to be shown. The data feed can be privately generated by the Smart Infrastructure with a digital media department or public such as IP TV for news, weather updates or films. Displays can be clustered into Video Walls to provide wider video images to the Smart Infrastructure operations team in the control room.

5.5. Information Technology Systems

Information Technology (IT) systems enable the required services for the Smart Infrastructure business, operators and managers to perform their tasks. IT systems have gradually become more flexible; rather than dedicated access from a fixed computer, currently IT services can be accessed by mobile phones via specific apps. Although the boundaries of user accessibility are expanded, CyberSecurity risks and identity theft also increases as any attacker can get access remotely to private hosted systems.

Email Systems transmit digital information in the form of messages using Simple Mail Transfer Protocol (SMPT) protocols with additional calendar and event management applications. Email Systems permits remote computer or Mobile phone server access via Webmail, Internet Message Access Protocol (IMAP) or Post Office Protocol (POP); the difference between them is the synchronization with the email server.

Ticketing Systems invoices users of the Smart Infrastructure for accessing its services such as Railway Stations or Airports. Tickets are gradually evolving from paper based to Smart Cards or Mobile Apps. Usually ticketing required a physical Gateline, however with Digital technologies such as RFID and video analytics; those physical barriers are becoming virtual. In addition, the integration of private ticketing system and banking IT infrastructure enables the outsourcing of contactless bank debit cards.

Document Management System (DMS) stores digitally documents in the cloud for resilience; the documents can be shared and accessed simultaneously by a group of users in collaboratively working with automatic revisions. Although DMS systems manage documents in their native file format (.DOC, .XLS, .PDF), their Web interface also interacts content with a .HTML extension.

Timesheets System is used for automatic time management, billing and payroll. The Smart Infrastructure users can book holiday time, time off, sick days with integration to a digital calendar. Timesheet system enables integration with other online systems such as accounting, billing project management systems, payroll systems and resource scheduling.

Database Warehouse Systems (DWS) stores data from different resources of the Smart Infrastructure Business, produces reports and performs data analytics. The Smart Infrastructure Leadership is based on Data warehouse Systems to make the final management decisions.

Enterprise Resource Planning (ERP) System performs integrated management of Smart Infrastructure Business processes, functions and applications enabling data information flows between them. Enterprise Resource Planning Systems provides a real time and continuous updated monitoring of business parameters such as cash flow, asset management, purchase orders, and payroll.

Intranet System enables a shared Web Portal where information is stored and accessed via Web Pages. The Intranet provides the Smart Infrastructure with the interface for internal communication and collaboration, although Intranets have a vast amount of growing information where it is difficult to find relevant information. Intelligent Search methods can be developed and integrated as Interfaces to personalize information to user while providing search functionality.

6. Digital Transmission

Digital sensors require digital transmission systems to transmit information between each other in order to form a higher level of integration such us the Internet of Things (IoT). Although Artificial Intelligence (AI) seeks decentralized autonomous systems that can learn and take independent decisions, AI also seeks a shared and coordinated learning between agents.

Digital transmission systems are used in the Smart Infrastructure with two main technologies. Wired communications use physical cables to provide security and higher data rates, however, sensors are fixed to the location. Wireless communications provide user mobility and flexibility with the drawback of a lower data transmission rate and security.

6.1. Local and Wide Area Area Network

Local Area Networks [63] are restricted to a physical location enabling the Ethernet OSI Layer 2 wired connectivity to sensors that are normally fixed, such as CCTV Cameras or Wireless Access Points. Local Area Networks consist on copper Category (CAT) twisted pair or fibre data cables to connect devices and Ethernet Switches to transmit frames (Table 1). In addition, Power over Ethernet (PoE) allows the same cable to transmit data and power, reducing additional cabling requirements and space.

Table 1. Local Area Network (LAN) Specifications.

Name	Code	Standard	Data	Distance	Cable
Ethernet	10BASE-T	802.3i-1990	10 Mbits	100 m	Copper
Fast Ethernet	100BASE-T	802.3u-1995	100 Mbits	100 m	Copper
Fast Ethernet	100BASE-SX	802.3u-1995	100 Mbits	2000 m	Fibre
Giga Ethernet	1000BASE-T	802.3ab-1999	1000 Mbits	100 m	Copper
Giga Ethernet	1000BASE-LX	802.3z-1998	1000 Mbits	5 km	Fibre
10 Gigabit Ethernet	10GBASE-T	802.3an-2006	10 Gbits	100 m	Copper
10 Gigabit Ethernet	10GBASE-LR	802.3ae-2002	10 Gbits	10 km	Fibre
100 Gigabit Ethernet	100GBASE-LR4	802.3ba-2010	100 Gbits	10 km	Fibre
Terabit Ethernet	400GBASE-LR8	802.3bs-2017	400 Gbits	10 km	Fibre

Wide Area Networks (WAN) [64] connect the different Networks that cover the entire Smart Infrastructure (Table 2). WANs provide the OSI Layer IP 3 Connectivity to transmit IP Packets. Wide Area Networks can prioritize traffic with QoS. Routers are normally interconnected using public networks by ISP with several protocols and technologies such as Integrated Services Digital Network (ISDN), Multiprotocol Label Switching (MPLS), asynchronous transfer mode (ATM) and Frame Relay (FR). In addition, a Wide Area Network can be provided privately by the Smart Infrastructure by dedicated Routers with Routing Information Protocols (RIP), Interior Gateway Protocol (IGRP), Open Shortest Path First (OSPF) or Enhanced interior gateway routing protocol (EIGRP).

Table 2. Wide Area Network (WAN) data access.

Name	Code	Standard	Data Rate
Digital Subscriber Line	DSL	G.933.1	52 Mbit/s
Integrated Services Digital Networks	ISDN	EG 201 730	2.048 Mbit/s
European Trunk Carrier	E4 (CMI)	G.751	140 Mbit/s
Optical Carrier	OC-768/STS-768	G.803	39.81 Gbit/s
Asynchronous Transfer Mode	ATM	ANSI and ITU	10 Gbps
Frame Relay	FR	ANSI and ITU	45 Mbps
Multiprotocol Label Switching	MPLS	RFC 3031	1 Gbps

6.2. Wireless Area Networks

Wireless Area Networks (WLAN) [65] or Wi-Fi provide the OSI layer 2 Wireless connectivity via the use of Access Points that provide the wireless channel to the mobile user devices or sensors (Table 3). WLAN Controllers manage the configuration of the WLAN and provides the data roaming between the Access points and the external WLAN.

Table 3. Wireless Area Network (WLAN) protocols.

Protocol	Frequency	Bandwidth	Data Rate	Coverage
802.11a	5 GHz	20 MHz	54 Mbps	120 m
802.11b	2.4 GHz	22 MHz	11 Mbps	140 m
802.11g	2.4 GHz	20 MHz	54 Mbps	140 m
802.11n	2.4/5 GHz	20/40 MHz	285/600 Mbps	250 m
802.11ac	5 GHz	20/40/80/160 MHz	347/800 Mbps 1.7/3.5 Gbps	100 m
802.11ax	2.4/5 GHz	20/40/80/160 MHz	10.5 Gbps	100 m

6.3. Bluetooth

Bluetooth [66] enables the direct connectivity between devices at very short distances. It was developed as the wireless alternative to the RS-232 data cables and connectors. A Bluetooth network is a Personal Area Network (PAN), or piconet, configured as single master and slaves (Table 4). Bluetooth Low Energy (BLE) is used to provide a more accurate location than GPS which can be used to better manage the interaction with users within the physical space while transmitting positional information without a LAN or WLAN network.

Table 4. Bluetooth types.

Type	Frequency	Data Rate	Power	Range
Class 1	2.45 GHz	768 kbps	100 mW	100 m
BLE	2.45 GHz	1 Mbps	10 mW	30 m
Class 2	2.45 GHz	3 Mbps	2.5 mW	10 m
Class 3	2.45 GHz	24 Mbps	1 mW	1 m
Class 4	2.45 GHz	24 Mbps	0.5 mW	0.5 m

6.4. Near Field Communications

Near Field Communications (NFC) [67] enable the transmission of information between only two electronic devices at very short distances (Table 5). NFC devices supports card emulation, read/write tags and peer to peer data transmission. Near Field Communications technology is applied in contactless payment systems, advertising boards and collaborative networking via data sharing within the Smart Infrastructure.

Table 5. Near field communications (NFC) specification.

Type	Frequency	Data Rate	Power	Range
Active Passive	13.56 MHz	106/212/424 Kbps	10 mW	4–20 cm

6.5. Radio Networks

Trunked Radio Networks [68] provide a two radio system that multiplexes user conversations into a few dedicated frequencies (Table 6). Radio Networks enable talk groups and fleet maps to be used for external communications and mission critical applications within the Smart Infrastructure such as Police, Fire Brigade and Rail. Due its low Frequency, Radio Networks provide high levels of geographic coverage such as city scale at reduced infrastructure costs. In addition, Radio Handsets can communicate directly without the need of a radio infrastructure and be used as tracking device for user management.

Table 6. Radio networks.

Radio	Frequency (MHz)	Bandwidth	Data Rate	Use	Area km^2
TETRA	350–370 380–430 450–470 806–870	4 Channels 25 KHz TDMA	28.8 kbit/s	Small Area High Density	25
P25	380–512 764–806 806–870	1–2 Channels 6.25 KHz 12.5 KHz 25 KHz FDMA	9.6 kbit/s	Wide Area Low Density	100

6.6. Mobile Networks

Mobile Networks [69] support voice and data transmissions to user mobile phones, tablets and laptops enabling its connection to a Public Switched telephone Network (PSTN) or Internet Service Provider (ISP). Mobile Networks provide an extensive coverage at country scale when the distributed cells served by base stations are interconnected (Table 7). Mobile Networks perform better than Radio Networks in wider and congested environments since they have more capacity than a single large transmitter, as the same frequency can be used for multiple links in different cells. In addition mobile devices also consume less power. Mobile Networks are very expensive to provide as they require additional circuit and packet switching networks for voice and data transmission respectively.

Table 7. Mobile networks.

Technology	Frequency	Bandwidth	Data Rate	Access	Cell
GSM (2G)	1800 MHz	200 kHz	270.833 kbit/s	TDMA	7 km
UMTS (3G)	1900 MHz 2100 MHz	5 MHz	42 Mbit/s	CDMA	6 km
LTE/WIMAX (4G)	1800 MHz 2100 MHz 2600 MHz	20 MHz	299.6 Mbit/s	OFDMA	2 km
5G	<6 GHz 24–86 GHz	100 MHz 400 MHz	20 Gbit/s	NOMA	1 km

6.7. Satellite Communications

Satellite Communications enable a telecommunication link between a source transmitter and a receiver at different positions on planet Earth; satellites only retransmit and amplify the radio signals via a transponder (Table 8). Satellite transmission requires line of sight, therefore obstructed by the curvature of the planet. Satellite Communication for the Smart Infrastructure will be used to interconnect two remote locations where physical cabling is not possible, in locations such as deserts or islands. Satellite Communications are used for television, telephone, radio, internet, GPS and other security applications.

Table 8. Satellite communications.

Band	Frequency	Use
L	1–2 GHz	GPS, satellite mobile phones and radio
S	2–4 GHz	Weather radar, surface ship radar
C	4–8 GHz	Satellite TV networks
X	8–12 GHz	Military radar, Weather monitoring, Air Traffic Control, Maritime Vessel Traffic Control
Ku	12–18 GHz	Satellite Communications Direct Broadcast Satellite Services
Ka	26–40 GHz	Satellite Communications High Resolution close range Radars

7. Digital Server

Digital Servers manage the Digital Systems sensors, Digital Transmission QoS and Service Level Agreements (SLA) in addition of the status of the physical equipment. Digital Servers are logically interconnected to enable system integration and data analytics via digital interfaces. Digital servers can be installed locally in the same physical location of the Smart Infrastructure or centralized in clusters hosted remote locations such as Datacentre in private or public clouds. Autonomous smart devices such as vehicles, trains and airplanes that will use the Smart Infrastructure will have integrated dedicated servers following edge cloud solutions to enable.

7.1. Server Virtualization

Servers are required to be operational at very high speed for long periods of time without interruption; servers shall be high availability and high reliability. Servers can be virtualized via sharing hardware and software resources with other virtual servers to allow a more efficient use, reduce cost while increasing reliability. Virtual Servers are normally hosted on modular blade servers managed by hypervisors that abstract the virtual server from its physical hardware and software.

7.2. Memory Virtualization

Memory and storage can be block virtualized presenting a logical memory composed from the physical storage resources delivered via Fibre Channel or Internet Small Computer Systems Interface (iSCSI) protocols. In addition, file virtualization eliminates the dependency between the location where the files are physically stored and the data accessed at the file level on a decentralized memory via Network File System (NFS) or Server Message Block (SMB) protocols. Storage Area Networks (SANs) can be also hosted in the Datacentres with the Smart Infrastructure Servers.

7.3. Software Defined Networks

Software Defined Networks (SDN), or Virtual Network, enables efficient network management and configuration that improves network performance and monitoring in a streamlined physical infrastructure. SDN separates the network packet transmission process (data plane) managing centrally the packet routing process (control plane) in a datacentre. SDN enables on demand real time network resources with automated load balancing able to scale in order to meet application and data requirements.

7.4. Time Syncronization

Network Time Synchronization establishes a reference time for the entire Smart Infrastructure Digital Systems, Transmission, Servers and Management via the use or Network Time Protocol (NTP) or Precision Time Protocol (PTP) that achieves milliseconds or microseconds of Coordinated Universal Time respectively. Time synchronization is based on a hierarchical stratum level where Stratum 0 is the reference high precision timekeeping clock synchronized to atomic clocks, GPS, Global Navigation Satellite System (GNSS) or Low Frequency radio sources and lower Stratums corresponds to the Digital Transmission equipment topology.

8. Digital Management

The data and information captured by the Sensors of the Digital Systems, transmitted by the Digital Infrastructure and processed by the Digital Servers is managed by the Smart Infrastructure Digital Management in real time. The management will not only include the information captured by the sensors but also the status of the Digital Systems, Digital Transmission and Digital Server infrastructure.

Digital Management provides a hierarchical layer of software, middleware, Application Programming Interface (API) that performs system and interface integration, Big Data Analytics, Alarm Management with Graphical User Interface (GUI) on workstations or Mobile app where the end user can be human or Artificial Intelligence. Digital management requires the use of Video Walls or Virtual Reality to efficiently display the complexity of the retrieved information in order for humans to make accurate decisions, however, as Artificial Intelligence progresses; equipment and facilities dedicated to human will be gradually obsolete.

8.1. Supervisory Control and Data Acquisition

Supervisory control and data acquisition (SCADA) monitors and manages the Smart Infrastructure equipment and assets, including industrial and manufacturing processes, via Programmable Logic Controller (PLC), Remote Terminal Units (RTU) and Remote Inputs Outputs (RIO). Originally SCADA was based on proprietary protocols such as Modbus, Conitel although newer versions IEC and DNP3 are standardized and vendor agnostic based on Transmission Control Protocol / Internet Protocol (TCP/IP).

8.2. Building Management

Building management system (BMS), controls and monitors the station, airports or building's mechanical and electrical equipment of the Smart Infrastructure including heating, ventilation, and air conditioning (HVAC), lighting, power, lifts, escalators and fire systems. Similar to the SCADA System, originally the BMS protocols were vendor specific such as C-Bus, Profibus; however, the migration and integration with IP has developed open standards such as DeviceNet, SOAP, XML, BACnet, LonWorks and Modbus. BMS is key to manage the energy consumption of the Smart Infrastructure.

8.3. User Management

A User Management System (UMS) manages the users of the Smart Infrastructure such as Staff, Contractors, Customers or Passengers via the use of Telecommunications Systems and Digital Information such as Help Points, VSS Cameras, Intercoms, Mobile Phones, Telephones and Displays. In addition, in case of emergency, users can be guided via the PA/VA Systems and managed via the VSS System and Mobile Phone or Radio geolocation.

The use of dedicated Smart Infrastructure Mobile Apps and Social Media such as Instagram or Facebook also enables the personalization and segregation of user announcements in real time where notifications can also be sent to a selected group of friends or contacts.

9. Virtual Infrastructure: Discussion and Challenges

There are several challenges to implement Digital as a Service:

(1) The key risk, as Digitalization and Big Data becomes more relevant and fundamental, CyberSecurity threats and attacks will generate major impacts. There are currently Cybersecurity guidelines [70] that cover the seven layers of the OSI model. The use of proxy servers, firewalls, cryptography, authentication, authorization and accounting (AAA) servers reduces the risk of Cyber attacks. In addition, the block chain will add a layer of security with a decentralized model where key information is distributed in a shared network therefore removing single or double points of failure.

(2) As Digitalization enables services to become more integrated, companies may not allow access from manufacturer independent protocols or interactions with third party software in order to protect their intellectual property, assets or economic interests.

(3) System virtualization will be another challenge where business and economic interests between competing companies shall be managed by regulators. Internet Service Providers (ISPs) or Mobile Network Operators (MNOs) will not be willing to make their services virtual because virtualization will remove the need for competition where service providers offer similar and reductant coverage in the same area with duplicated equipment.

(4) Digitalization and virtualization will also raise ownership and maintenance issues; it shall be clearly determined and assigned what each stakeholder owns including its responsibilities Aspects to agree are the procurement of the equipment and software and the payment for its maintenance such as energy bills and software upgrades. Lack of proactive maintenance will increase the risk of a cyber-attacks.

(5) The reduction of cost (CAPEX and OPEX) will be the main driver for Digital as a Service; the success of DaaS will depend on successful economic business cases that include stakeholder and user requirements in addition to the whole life cycle cost: design, procurement, installation and operational stages.

(6) There will be an increasing level of dependency to technology: Big Data; Artificial Intelligence and Machine Learning Algorithms. However this dependency will be balanced with an increment of reliability, performance and redundancy on services and equipment.

10. Conclusions

This paper has presented the concept of Digital as a Service: DaaS, which virtualizes Smart Infrastructure and Cities on four levels: Systems, Transmission, Server and Management. Any complete Digitalization can be implemented independently of its associated physical infrastructure. DasS would enable an interoperable Virtual Digital Infrastructure. Independent systems and solutions are becoming smarter; this paper proposes their full interconnection, integration and virtualization into a higher layer of abstraction. The fifth industrial revolution, based on the progress of Artificial Intelligence, will completely remove humans from operative and management decisions.

The implementation of Digital as a Service brings major challenges. As the Big Data becomes the most valuable asset; it shall be protected against cybersecurity attacks. In addition, commercial and economic interests from competing individuals, products and organizations need to be efficiently managed. DaaS business cases shall consider stakeholder and user requirements and the entire whole life cycle, both CAPEX and OPEX. Technology has already started to change the layout of Smart Cities: Robotics and automatization have caused shops on the high street to close when interconnected with e-commerce; the fixed functionality and space of office buildings and residential developments is migrating to multipurpose, multiservice, co-working environments.

Future trends in Smart Cities will see the continuous automatization of its transport with autonomous vehicles and self-management assets. Infrastructure will be increasingly interconnected with the digitalization of its energy requirements represented on Smart Grids. Big Data will enable citizens or users to make better use of the Smart City Space, Services and Structures (3S).

Author Contributions: This article has only one author.

Funding: This research received no external funding.

Conflicts of Interest: The author declares no conflict of interest.

Appendix A —Digital as a Service Schematic

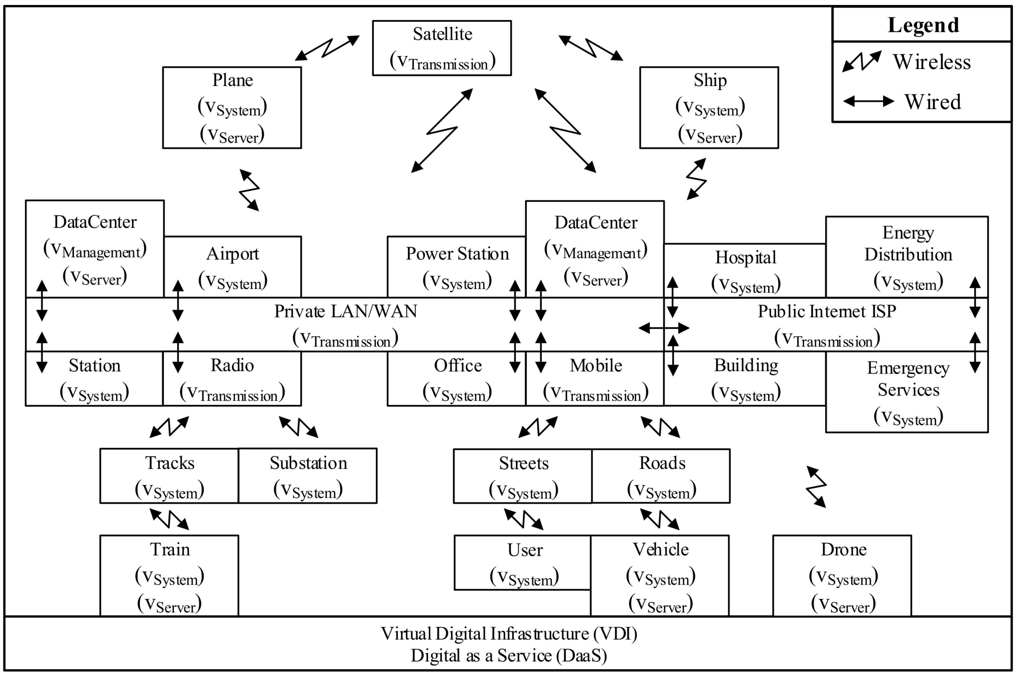

Figure A1. Digital as a Service Schematic.

References

1. Kagermann, H. Change through Digitization—Value Creation in the Age of Industry 4.0. In *Management of Permanent Change*; Springer Fachmedien Wiesbaden: Wiesbaden, Germany, 2015; pp. 23–32.
2. Astarloa, B.; Kaakeh, A.; Lombardi, M.; Scalise, J. *The Future of Electricity: New Technologies Transforming the Grid Edge*; World Economic Forum: Geneva, Switzerland, 2017; pp. 1–32.
3. Di Silvestre, M.L.; Favuzza, S.; Sanseverino, E.R.; Zizzo, G. How Decarbonization, Digitalization and Decentralization are changing key power infrastructures. *Renew. Sustain. Energy Rev.* **2018**, *93*, 483–498. [CrossRef]
4. Amini, H.; Boroojeni, K.; Iyengar, S.; Blaabjerg, F.; Pardalos, P.; Madni, A. A Panorama of Future Interdependent Networks: From Intelligent Infrastructures to Smart Cities. *Sustain. Interdepend. Netw. Stud. Syst. Decis. Control* **2018**, *145*, 1–10.
5. Guedes, A.L.A.; Alvarenga, J.C.; Goulart, M.d.S.S.; Rodriguez, M.V.; Soares, C.A.P. Smart Cities: The Main Drivers for Increasing the Intelligence of Cities. *Sustainability* **2018**, *10*, 3121. [CrossRef]
6. Schipper, R.; Silvius, G. Characteristics of Smart Sustainable City Development: Implications for Project Management. *Smart Cities* **2018**, *1*, 5. [CrossRef]
7. Schwab, K. *The Fourth Industrial Revolution*; World Economic Forum: Geneva, Switzerland, 2016.
8. Cocchia, A. Smart and Digital City: A Systematic Literature Review. In *Smart City*; Springer: Cham, Switzerland, 2014; pp. 13–43.
9. Allwinkle, S.; Cruickshank, P. Creating Smart-er Cities: An Overview. *J. Urban Technol.* **2011**, *18*, 1–16. [CrossRef]
10. Chourabi, H.; Nam, T.; Walker, S.; Gil-Garcia, R.; Mellouli, S.; Nahon, K.; Pardo, T.; Jochen, H.; Chourabi, S. Understanding Smart Cities: An Integrative Framework. In Proceedings of the 2012 45th International Conference on System Sciences, Maui, HI, USA, 4–7 January 2012; pp. 2289–2297.
11. Su, K.; Li, J.; Fu, H. Smart city and the applications. In Proceedings of the International Conference on Electronics Communications and Control, Ningbo, China, 9–11 September 2011; pp. 1028–1031.
12. Al-Hader, M.; Rodzi, A. The Smart City Infrastructure Development and Monitoring. *Theor. Empir. Res. Urban Manag.* **2009**, *4*, 87–94.
13. Allam, Z.; Newman, P. Redefining the Smart City: Culture, Metabolism and Governance. *Smart Cities* **2018**, *1*, 2. [CrossRef]
14. Schaffers, H.; Komninos, N.; Pallot, M.; Trousse, B.; Nilsson, M.; Oliveira, A. Smart Cities and the Future Internet: Towards Cooperation Frameworks for Open Innovation. In Proceedings of the Future Internet Assembly, Budapest, Hungary, 17–19 May 2011; pp. 431–446.
15. Harrison, C.; Donnelly, I.A. A Theory of Smart Cities. In Proceedings of the 55th Annual Meeting of the International Society for the Systems Sciences, Hull, UK, 17–22 July 2011; pp. 1–15.
16. Nam, T.; Pardo, T. Conceptualizing smart city with dimensions of technology, people, and institutions. In Proceedings of the 12th Annual International Digital Government Research Conference: Digital Government Innovation in Challenging Times, College Park, MD, USA, 12–15 June 2011; pp. 282–291.
17. Batty, M.; Axhausen, K.; Giannotti, F.; Pozdnoukhov, A.; Bazzani, A.; Wachowicz, M.; Ouzounis, G.; Portugali, Y. Smart cities of the future. *Eur. Phys. J. Spec. Top.* **2012**, *214*, 481–518. [CrossRef]
18. Sun, Y.; Song, H.; Jara, A.; Bie, R. Internet of Things and Big Data Analytics for Smart and Connected Communities. *IEEE Access* **2016**, *4*, 766–773. [CrossRef]
19. Zanella, A.; Bui, N.; Castellani, A.; Vangelista, L.; Zorzi, M. Internet of Things for Smart Cities. *IEEE Internet Things J.* **2014**, *1*, 22–32. [CrossRef]
20. Balakrishna, C. Enabling Technologies for Smart City Services and Applications. In Proceedings of the International Conference on Next Generation Mobile Applications, Services and Technologies, Paris, France, 12–14 September 2012; pp. 223–227.
21. Perera, C.; Zaslavsky, A.; Christen, P.; Georgakopoulos, D. Sensing as a service model for smart cities supported by Internet of Things. *Transa. Emerg. Telecommun. Technol. Spec. Issue Smart Cities Trends Technol.* **2014**, *25*, 81–93. [CrossRef]
22. Muñoz, J.H.; Vercher, J.B.; Muñoz, L.; Galache, J.; Presser, M.; Gómez, L.H.; Pettersson, J. Smart Cities at the Forefront of the Future. In Proceedings of the Future Internet Assembly, Budapest, Hungary, 17–19 May 2011; Volume 6656, pp. 447–462.

23. Vlacheas, P.; Giaffreda, R.; Stavroulaki, V.; Kelaidonis, D.; Foteinos, V.; Poulios, G.; Demestichas, P.; Somov, A.; Biswas, A.R.; Moessner, K. Enabling smart cities through a cognitive management framework for the internet of things. *IEEE Commun. Mag.* **2013**, *51*, 102–111. [CrossRef]
24. Li, D.; Cao, J.; Yao, Y. Big data in smart cities. *Sci. China Inf. Sci.* **2015**, *58*, 1–12. [CrossRef]
25. Strohbach, M.; Ziekow, H.; Gazis, V.; Akiva, N. Towards a Big Data Analytics Framework for IoT and Smart City Applications. In *Modeling and Processing for Next-Generation Big-Data Technologies*; Springer: Berlin, Germany, 2015; Volume 4, pp. 257–282.
26. Al Nuaimi, E.; Al Neyadi, H.; Mohamed, N.; Al-Jaroodi, J. Applications of big data to smart cities. *J. Internet Serv. Appl.* **2015**, *6*, 1–25. [CrossRef]
27. Abaker, I.; Hashem, T.; Chang, V.; Anuar, N.B.; Adewole, K.; Yaqoob, I.; Gani, A.; Ahmed, E.; Chiroma, H. The role of big data in smart city. *Int. J. Inf. Manag.* **2016**, *36*, 748–758.
28. Alshawish, R.; Alfagih, S.; Musbah, M. Big data applications in smart cities. In Proceedings of the International Conference on Engineering & MIS, Agadir, Morocco, 22–24 September 2016; pp. 1–7.
29. Batty, M. Big data, smart cities and city planning. *Dialogues Hum. Geogr.* **2013**, *3*, 274–279. [CrossRef] [PubMed]
30. Mohanty, S.P.; Choppali, U.; Kougianos, E. Everything you wanted to know about smart cities: The Internet of Things is the backbone. *IEEE Consum. Electron. Mag.* **2016**, *5*, 60–70. [CrossRef]
31. Gungor, V.; Sahin, D.; Kocak, T.; Ergut, S.; Buccella, C.; Cecati, C.; Hancke, G. Smart Grid Technologies: Communication Technologies and Standards. *IEEE Trans. Ind. Informat.* **2011**, *7*, 529–539. [CrossRef]
32. Wang, W.; Xu, Y.; Khanna, M. A survey on the communication architectures in smart grid. *Comput. Netw.* **2011**, *55*, 3604–3629. [CrossRef]
33. Gungor, V.; Sahin, D.; Kocak, T.; Ergut, S.; Buccella, C.; Cecati, C.; Hancke, G. A Survey on Smart Grid Potential Applications and Communication Requirements. *IEEE Trans. Ind. Inform.* **2013**, *9*, 28–42. [CrossRef]
34. Li, F.; Qiao, W.; Sun, H.; Wan, H.; Wang, J.; Xia, Y.; Xu, Z.; Zhang, P. Smart Transmission Grid: Vision and Framework. *IEEE Trans. Smart Grid* **2010**, *1*, 168–177. [CrossRef]
35. Colak, I.; Sagiroglu, S.; Fulli, G.; Yesilbudak, M.; Covrig, Ca. A survey on the critical issues in smart grid technologies. *Renew. Sustain. Energy Rev.* **2016**, *54*, 396–405. [CrossRef]
36. Fan, Z.; Kulkarni, P.; Gormus, S.; Efthymiou, C.; Kalogridis, G.; Sooriyabandara, M.; Zhu, Z.; Lambotharan, S.; Chin, W.H. Smart Grid Communications: Overview of Research Challenges, Solutions, and Standardization Activities. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 21–38. [CrossRef]
37. Fang, X.; Misra, S.; Xue, G.; Yang, D. Smart Grid—The New and Improved Power Grid: A Survey. *IEEE Commun. Surv. Tutor.* **2012**, *14*, 944–980. [CrossRef]
38. Gelenbe, E. Energy Packet Networks: ICT Based Energy Allocation and Storage. In *Proceedings of the International Conference on Green Communications and Networking*; Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering; Springer: Berlin, Germany, 2011; Volume 51, pp. 186–195.
39. Gelenbe, E. Energy packet networks: Smart electricity storage to meet surges in demand. In Proceedings of the 5th International ICST Conference on Simulation Tools and Techniques, Sirmione-Desenzano, Italy, 19–23 March 2012; pp. 1–7.
40. Gelenbe, E. Energy packet networks: Adaptive energy management for the cloud. In Proceedings of the 2nd International Workshop on Cloud Computing Platforms, Bern, Switzerland, 10 April 2012; Volume 1, pp. 1–5.
41. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008; pp. 1–10. Available online: Bitcoin.org.
42. Peters, G.; Panayi, E. Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money. In *Banking Beyond Banks and Money*; New Economic Windows Springer International Publishing: Cham, Switzerland, 2016; pp. 239–278.
43. Kosba, A.; Miller, A.; Shi, E.; Wen, Z.; Papamanthou, C. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. In Proceedings of the IEEE Symposium on Security and Privacy, San Jose, CA, USA, 22–26 May 2016; pp. 839–858.
44. Beck, R.; Stenum, J.; Lollike, N.; Malone, S. Blockchain—The Gateway to Trust-Free Cryptographic Transactions. In Proceedings of the European Conference on Information Systems, Istanbul, Turkey, 12–15 June 2016; pp. 1–14.

45. Heilman, E.; Baldimtsi, F.; Goldberg, S. Blindly Signed Contracts: Anonymous On-Blockchain and Off-Blockchain Bitcoin Transactions. In *Proceedings of the International Conference on Financial Cryptography and Data Security Financial Cryptography and Data Security*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 1–15.
46. Zyskind, G.; Nathan, O.; Pentland, A. Decentralizing Privacy: Using Blockchain to Protect Personal Data. In Proceedings of the Security and Privacy Workshops, San Jose, CA, USA, 21 May 2015; pp. 180–184.
47. Kishigami, J.; Fujimura, S.; Watanabe, H.; Nakadaira, A.; Akutsu, A. The Blockchain-Based Digital Content Distribution System. In Proceedings of the IEEE Fifth International Conference on Big Data and Cloud Computing 2015, Dalian, China, 26–28 August 2015; pp. 187–190.
48. Watanabe, H.; Fujimura, S.; Nakadaira, A.; Miyazaki, Y.; Akutsu, A.; Kishigami, J. Blockchain contract: Securing a Blockchain applied to smart contracts. In Proceedings of the International Conference on Consumer Electronics, Las Vegas, NV, USA, 7–11 January 2016; pp. 467–468.
49. Aitzhan, N.Z.; Svetinovic, D. Security and Privacy in Decentralized Energy Trading through Multi-signatures, Blockchain and Anonymous Messaging Streams. *IEEE Trans. Dependable Secure Comput.* **2016**, *15*, 1–14. [CrossRef]
50. Yuan, Y.; Wang, Fe. Towards Blockchain based intelligent transportation systems. In Proceedings of the International Conference on Intelligent Transportation Systems, Rio de Janeiro, Brazil, 1–4 November 2016; pp. 2663–2668.
51. Biswas, K.; Muthukkumarasamy, V. Securing Smart Cities Using Blockchain Technology. In Proceedings of the International Conference High Performance Computing and Communications/Smart City/Data Science and Systems, Sydney, Australia, 12–14 December 2016; pp. 1392–1393.
52. Huh, S.; Cho, S.; Kim, S. Managing IoT devices using BlockChain platform. In Proceedings of the International Conference on Advanced Communication Technology, Pyeongchang, Korea, 19–22 February 2017; pp. 464–467.
53. Dorri, A.; Kanhere, S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the Pervasive Computing and Communications Workshops, Big Island, HI, USA, 13–17 March 2017; pp. 1–6.
54. Serrano, W. The Random Neural Network with a BlockChain Configuration in Digital Documentation. In Proceedings of the International Symposium on Computer and Information Sciences, Poznan, Poland, 20–21 September 2018; pp. 196–210.
55. Cohen, N.; Gattuso, J.; MacLennan Brown, K. *CCTV Operational Requirements Manual*; Publication No. 28/09; Home Office Scientific Development Branch: St. Albans, UK, 2009.
56. BS EN 62676. *Video Surveillance Systems for Use in Security Applications*; European Union: Brussels, Belgium, 2018.
57. BS EN 60839. *Alarm and Electronic Security Systems. Electronic Access Control Systems. System and Components Requirements*; European Union: Brussels, Belgium, 2013.
58. BS EN 50518. *Monitoring and Alarm Receiving Centre. Technical Requirements*; European Union: Brussels, Belgium, 2014.
59. BS 5839-8. *Code of Practice for the Design, Installation, Commissioning and Maintenance of Voice Alarm Systems*; European Union: Brussels, Belgium, 2013.
60. BS 5839-9. *Code of Practice for the Design, Installation, Commissioning and Maintenance of Emergency Voice Communication Systems*; European Union: Brussels, Belgium, 2011.
61. BS 5839-1. *Fire Detection and Fire Alarm Systems for Buildings. Code of Practice for Design, Installation, Commissioning and Maintenance of Systems in Non-Domestic Premises*; European Union: Brussels, Belgium, 2017.
62. BS EN 54. *Fire Detection & Alarm Systems*; European Union: Brussels, Belgium, 2016.
63. IEEE 802.3. *Physical Layer and Data Link Layer's Media Access Control (MAC) of Wired Ethernet*; IEEE: Piscataway, NJ, USA, 2018.
64. RFC 791. *Internet Protocol*; DARPA Internet Program Protocol Specification; DARPA: Arlington County, VA, USA, 1981.
65. IEEE 802.11. *Standards for Media Access Control and Physical Layer for Wireless Local Area Network*; IEEE: Piscataway, NJ, USA, 2018.
66. *Bluetooth*; Bluetooth Special Interest Group: Kirkland, WA, USA.
67. ISO/IEC 18092. *Information Technology—Telecommunications and Information Exchange between Systems—Near Field Communication*; ISO/IEC: Geneva, Switzerland, 2013.
68. ETS/EN 300 392. *Terrestrial Trunked Radio—TETRA-Voice + Data*; European Union: Brussels, Belgium, 2017.

69. IEEE 802.16. *Standards for Broadband for Wireless Metropolitan Area Networks*; WirelessMAN and WiMax; IEEE: Piscataway, NJ, USA, 2017.
70. National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2018.