sustainability

MDPI

Review

Integrated Operation Centers in Smart Cities: A Humanitarian Engineering Perspective

Basem Almadani [1,†], Farouq Aliyu [2,†,*] and Abdulrahman Aliyu [3]

1 Computer Engineering Department, King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia; mbasem@kfupm.edu.sa
2 Center of Excellence in Development of Nonprofit Organizations, King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia
3 Applied Research Center for Metrology, Standards and Testing, King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia; abdulrahman.aliyu@kfupm.edu.sa
* Correspondence: farouq.muhammad@kfupm.edu.sa; Tel.: +966-13-860-5129
† Current Address: Alfozan Academy, King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia.

Abstract: The United Nations predicted that 68% of the world's population will live in urban areas by 2050. Currently, the resources in urban areas are barely enough to cater to the inhabitants' needs. Scientists believe that automation is the solution. Hence, they believe that Smart Cities could offer a sustainable solution for the increasing rural-to-urban migration because they improve the quality of service by efficiently managing the limited resources the citizens share. However, community laws stipulate when and who governs the cities. These officials are responsible for decision making, which limits the quality of automation and smartness of the city. Integrated Operation Centers (IOCs) help to minimize this limitation. They gather information, process it, and visualize it for the managers. Thus, IOCs enable them to make informed and quick decisions on critical issues. This paper processed 64 conferences and journals on IOCs using the PRISMA method. The systematic literature review investigates the applications of IOCs, and we present a taxonomy for them. Also, we looked at how they impact humanity and environmental sustainability. We found that IOCs help to coordinate automation, disaster response, and security. They also help to conserve natural resources. Finally, we uncover some challenges of implementing IOCs and possible research directions.

Keywords: Smart City; Integrated Operation Centers; Humanitarian Computing; Internet of Things

Citation: Almadani, B.; Aliyu, F.; Aliyu, A. Integrated Operation Centers in Smart Cities: A Humanitarian Engineering Perspective. *Sustainability* **2023**, *15*, 11101. https://doi.org/10.3390/su151411101

Academic Editors: Luca Carrubbo and Leonard Walletzký

Received: 9 June 2023
Revised: 11 July 2023
Accepted: 14 July 2023
Published: 17 July 2023

1. Introduction

Rural-to-urban migration is on the rise. According to the United Nations, it will reach 68% by 2050 [1]. The current population increase has outpaced urban development in many countries, especially developing ones [2]. This results in overcrowding and increased strain on public facilities and infrastructure in many urban areas [2], which is evident in the overloading of their much-needed facilities, like bus stops, train stations, and hospitals. Although this rapid urbanization poses significant challenges for city planners and governments, it contributes to sustainable growth through increased productivity and innovation if managed well [2].

Researchers argue that sustainable urbanization is possible with the help of information and communication technologies (ICTs) [3–5]. A Smart City (SC) is a modern urban area that uses various ICTs to improve the efficiency and sustainability of public services and overall quality of life for its citizens [6]. It includes innovative approaches to infrastructure, environmental initiatives, highly functional public transportation, and other urban services that integrate technology and data to create a more efficient, sustainable, and livable city. The concept of an SC goes beyond using ICTs for better resource management and emissions reduction. It encompasses a range of upgrades and innovations to public services and urban infrastructure [6].

SCs amalgamate a Smart Economy, Smart Environment, Smart Governance, Smart Mobility, Smart Human/Smart People, and Smart Living [7]. Bellini et al. [8] added Smart Healthcare and Smart Industry and Production. A Smart Economy is that part of an SC that interconnects the local and global market to increase productivity and delivery [9]. A Smart Environment employs ICTs to monitor and manage the city [10]. Smart Mobility refers to using ICTs to improve transportation's safety, cost, efficiency, and reliability [11]. The term Smart People refers to those people who use ITCs to better their society [12]. In [13], Smart People use wearable sensors to send their movement and health-related data to the human resource department for real-time analysis. Thus, Smart Living refers to how Smart People live in an SC [14]. Smart Industry and Production is defined as using ICTs to increase the efficiency of manufacturing goods and services, whereas Smart Healthcare uses ICTs to establish a system of healthcare that is both cheap and effective [15]. Smart Governance is the application of ICTs in decision making [10]. It includes the government, industry, academia, non-governmental organizations (NGOs), and the people [16].

An Integrated Operation Center (IOC) is necessary for efficient Smart Governance. An IOC is a centralized platform that integrates data from various sources and uses advanced analytics to provide real-time insights to help users make informed decisions [17]. It acts as the central nervous system by integrating information and processes from various departments/sources to help officials manage and optimize city operations and infrastructure [18,19]. Some applications of IOCs are environmental monitoring [20], security [21,22], transportation [23], and other aspects of society. However, IOCs find applications in both public and private sectors (see Section 2.3). Many industries also use IOCs to unify operational control of all devices, systems, and applications, thereby reducing management complexity and increasing efficiency [24]. However, to achieve a sustainable Smart City, the collaboration of all the components of a city (public and private) is necessary [25].

An ideal IOC must be flexible. It should have the ability to connect with existing and future systems, thus making upgrade and downgrade easy. Other features of ideal SC-based IOCs are [17] reporting and tracking events; data analysis, assessing, and displaying KPIs; situational awareness support and reporting; support for standard operating procedures creation and use; resource and critical asset management; and real-time collaboration. These features allow easy adoption of IOC at a low cost. Table 1 shows IOCs and their cities from the papers studied in this survey. There are many benefits to deploying IOC in SC [17,18]:

1. IOCs provide city officials with insight into the city's inner workings for better management and monitoring.
2. The centralization of information and control enables officials to adjust systems to achieve timely results.
3. It allows the government to be proactive by predicting issues that may affect the smooth running of the city, which leads to an uninterrupted and high quality of service.
4. It encourages collaboration between departments and between the government and the citizens through instant communication infrastructure, which allows the government to work more efficiently, especially during a natural disaster.
5. Its holistic reporting and monitoring capabilities optimize planned and unplanned operations. It also reduces corruption and waste of resources.

Table 1. IOCs and their cities studied in the literature.

Ref.	Country	City	Operation Center
[26–28]	Brazil	Rio de Janeiro	Rio de Janeiro Operations Center
[29]	Brazil	Porto Alegre	Integrated Centre of Command
[29]	Brazil	Belo Horizonte	Centre of Operations at Belo Horizonte
[20]	UK	London	Smart City Board
[20]	Spain	Barcelona	Big Data Center of Excellence
[30]	S. Korea	Daejeon	Daejeon Smart City Operation Center
[31]	Indonesia	Jambi	Jambi City Operation Center
[32]	Indonesia	Bandung	Bandung Command Center
[28]	US	New York City	New York City's operations center
[33]	US	Texas	Texas emergency operations centers
[27]	Portugal	Porto	Integrated Management Centre of Porto
[34]	-	-	IBM Intelligent Operation Center
[35,36]	Russia	Novgorod	COS Operation Center
[37]	India	Tumakuru	Tumakuru Command and Control Center
[38]	India	Bhopal	Bhopal's Integrated Control & Command Center

Currently, tech companies have realized SCs' IOCs' potential to improve governance and citizens' quality of life (QoL), which is the third component of the Sustainable Development Goals (SDGs) [5]. Table 2 shows some tech companies and their IOC solutions. Most vendors focus on IOCs for Smart Industry and Production compared to SCs because (1) industries are often more willing to invest in technology and innovation to improve their operations and increase profitability; (2) developing new technologies for industries is easier than cities because they have more centralized and controlled environments; (3) also, developing profitable SC solutions is challenging due to the uniqueness of the legislature and culture of cities worldwide. Nonetheless, Table 1 shows the case studies of some successful SCs. Furthermore, companies and cities around the globe are collaborating to develop SC solutions [39,40].

Table 2. High market capitalization companies with IOC solutions.

Ref.	Company	IOC Solution	Year	Area
[41]	Cisco Systems	Cisco Kinetic for Cities [1]	2015	SC, SIP
[42]	Honeywell	Honeywell City Suite Software	2020	SC
[43]	Siemens	Building X, Xcelerator	2022	SB, SIP
[44]	IBM	Intelligent Operations Center 5.2.3	2012	SC
[45]	General Electric	Remote Operations Command Center	2021	SIP
[46]	Schneider Electric	AVEVA Unified Operations Center	2019	SIP
[47]	Hitachi	Hitachi Smart Spaces	2018	SC
[48]	Motorola Solutions	Network and Security Operations Center	2021	SC
[49]	Emerson Electric	iOps Workspace Solution	2014	SIP
[50]	Johnson Controls	OpenBlue	2020	SB

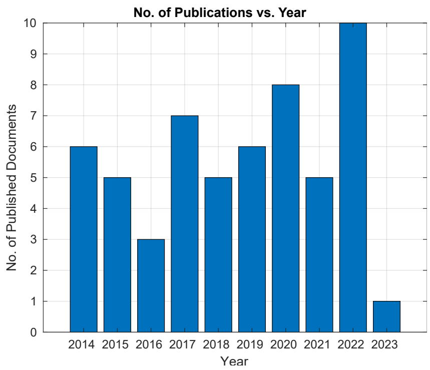
SC = Smart City, SIP = Smart Industry and Production, and SB = Smart Building. [1] Discontinued.

1.1. Problem Statement

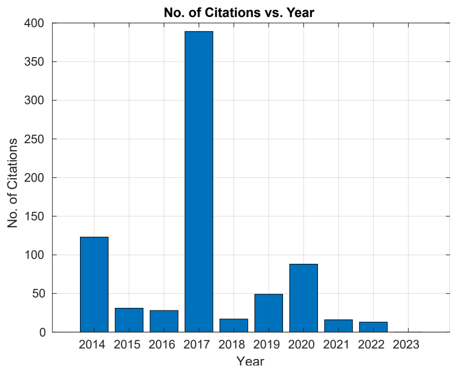
Figure 1a,b show the number of papers published in IOCs for SCs and their citations, respectively. The figure shows that the IOC is gaining researchers' attention, especially after the COVID-19 pandemic. The network shows that researchers are returning to SCs for solutions to some of our societies' latest problems and that IOCs are one of the most effective ways of managing them [32,37,38].

However, although the figures show an increasing interest in IOC research, the scale is small. Many cities are cash-strapped and rely on legislatures to decide how they spend their money. Hence, it is difficult for them to spare funds to implement SCs. In 2021, Cisco

Systems discontinued its IOC solution, Cisco Kinetic for Cities, which is previously known as Cisco® Smart+Connected™ City Operations Center, citing low customer demand [51]. Thus, there is a need for cheap IOCs for SCs. This paper aims to present the different IOC solutions and how they affect citizens' QoL. Moreover, it presents challenges and opens research areas that will allow for the development of cheap IOC solutions.



(**a**) Annual publications on IOC



(**b**) Annual citation for papers on IOC

Figure 1. Annual publications and citations on IOC.

1.2. Methodology

The SC command and control center (CCC) [26,37], Unified Operation Center (UOC) [46], City Operation Center (COC) [52], Municipal Operation Center (MOC) [53], Intelligent Operation Center (InOC) [44], or Integrated Operation Center (IOC) [24,54] is a center that gathers data from an SC and stores and processes them to enable officials to make timely and informed decisions. In some cases, this helps them in the decision implementation.

We used the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA [55]) technique to write a systematic literature review of IOCs for SCs. Figure 2 shows the flowchart of our work. We searched for papers with "command center" or "operation center" and "smart cities" in their title, abstract, or keywords on the Scopus database [56]. The search returned 64 publications, out of which we removed 15 because their title did not match our research or they were not readable. We studied the abstract of the remaining 53; 2 were about SCs but not IOCs for SCs, so they were excluded. At last, we analyzed 45 publications for this research.

In addition to PRISMA, we used VOSviewer to gain insight into the relationship between the papers. It is a text-mining tool that uses Visualization of Similarities (VOS) and analyzes bibliometric networks, including co-authorship, co-citation, and co-occurrence networks [57]. VOSviewer allows users to create network visualizations that reflect the relationships between entities, such as authors, papers, or keywords, based on their similarities. It clusters closely related keywords, while the distance between a pair of keywords is proportional to the number of papers in which they appear together [58]. Furthermore, the size of the vertex reflects its importance. For example, Figure 3 shows the network visualization of the papers we studied. In the figure, the SC vertex is the largest and at the center of the network because it appears in more publications than any other keywords. The clusters also helped us during the taxonomy process. Each one gives us an idea of how its members relate to the IOC. Thus, they create the taxonomy's branches, while the IOC is the root.

Interestingly, IOC does not belong to the dominant SC cluster. Researchers are more likely to discuss intelligent systems, traffic control, public facilities, or public administrations in SC. Although IOC is the second largest, IoT is closer to the core (i.e., SC). It is true because IOC is impossible without IoT, which is responsible for generating data. Furthermore, the figure shows that the IOC cluster has few vertices. Its cluster contains e-governance, case study, monitoring, IoT, and developing countries because several papers carried out case studies of IOCs that monitor cities with the help of IoT [26,37,59,60].

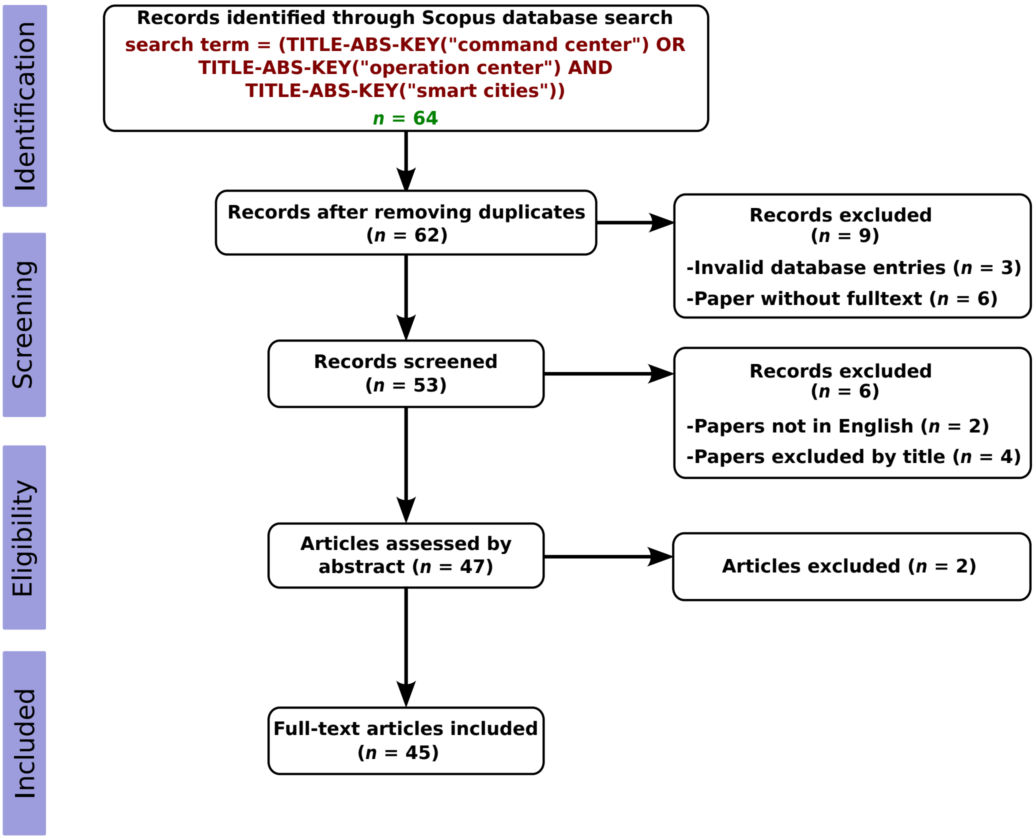


Figure 2. Systematic review of IOC publications using PRISMA method.

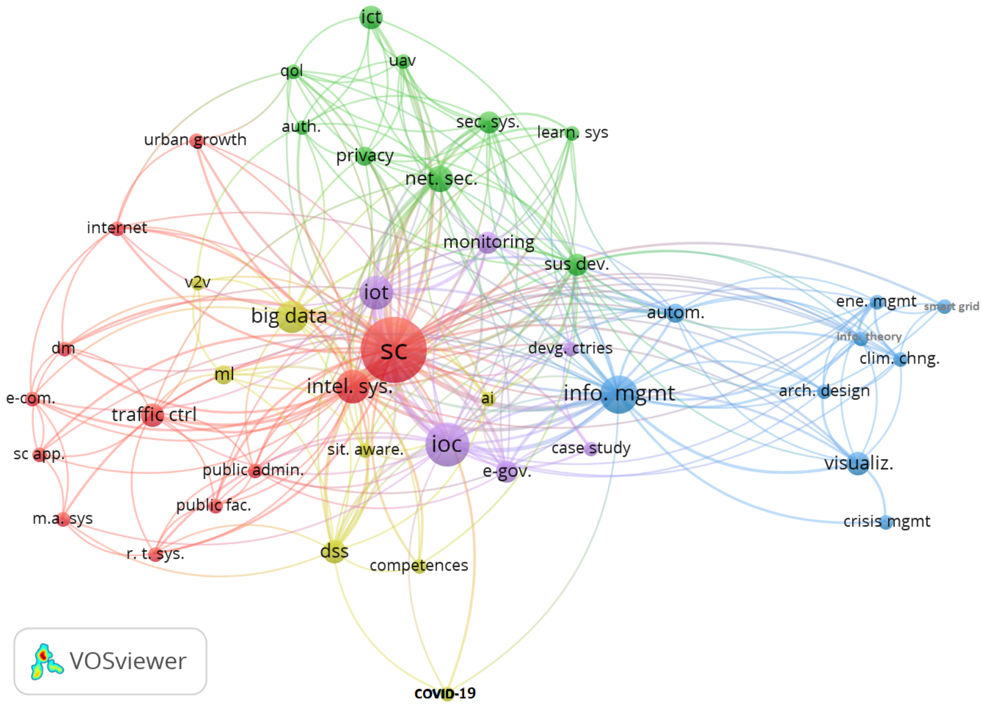


Figure 3. Network visualization of the studied papers.

1.3. Related Works and Contribution

Few papers presented a literature review of IOCs. In [34], the authors introduced the Internet of Things (IoT) and explained the problem with traditional cities. However, they only presented IBM Intelligent Operation Center (InOC) [44], which is inadequate to cover the subject matter. In [61], the authors discussed Security Operations Centers (SOCs). They also proposed a classification and rating scheme for them. However, the paper is limited to cybersecurity SOCs that provide services to organizations. It has not studied SOCs for physical security and cyber–physical security. Fadli and Sumitra presented a case study of Bandung Smart City, West Java, Indonesia [52]. The authors used semi-structured interviews with government officials and managers responsible for the initiatives to investigate the inner workings and success of the center. The paper highlighted the importance of the availability of a Network Operation Center (NOC), Data Center, and City Operation Center control room (COC) in an SC. Similar works in Table 1 report case studies of IOC implementations for SCs.

As far as we know, no survey studied the IOC solutions and proposed them a taxonomy. Thus, we aim to shed light on current trends and challenges of IOCs in SCs. The contributions of this paper are as follows:

1. We studied IOC solutions proposed in the literature, how they affect the citizens' QoL, and how they perform in some SCs.
2. We also presented the first taxonomy of SC IOCs and their use cases. Currently, there is no taxonomy for SC IOCs in the literature. We also discuss their impact on the environment, ease of governance, and the citizens.
3. Finally, we presented the challenges that IOCs face, which include factors that hinder their proliferation worldwide. These challenges can serve as potential research directions that ensure efficient and cheap IOCs.

The remaining parts of this paper are structured as follows: Section 2 presents a taxonomy of the IOCs in SCs. It also discusses the different types of IOCs and how they affect humanity. Section 4 discusses the challenges that IOCs face. It helps researchers to understand why IOCs face market resistance and opens research areas for more acceptable versions. Finally, Section 5 concludes the paper with lessons learned from the study and the possible future direction of IOCs in SCs.

2. Taxonomy of IOCs

Figure 4 shows a taxonomy of IOCs in SCs. The root is the IOC itself. The first-level branch shows the different methods of categorizing an IOC. Our studies have shown that there are currently four ways to classify SC IOCs. They can be classified based on the number of functions or the type of functions they offer, the scope or areas covered by the IOC, the size of the IOC in terms of hardware and software, and the orientation of the IOC—how the IOC is configured to manage the incoming information.

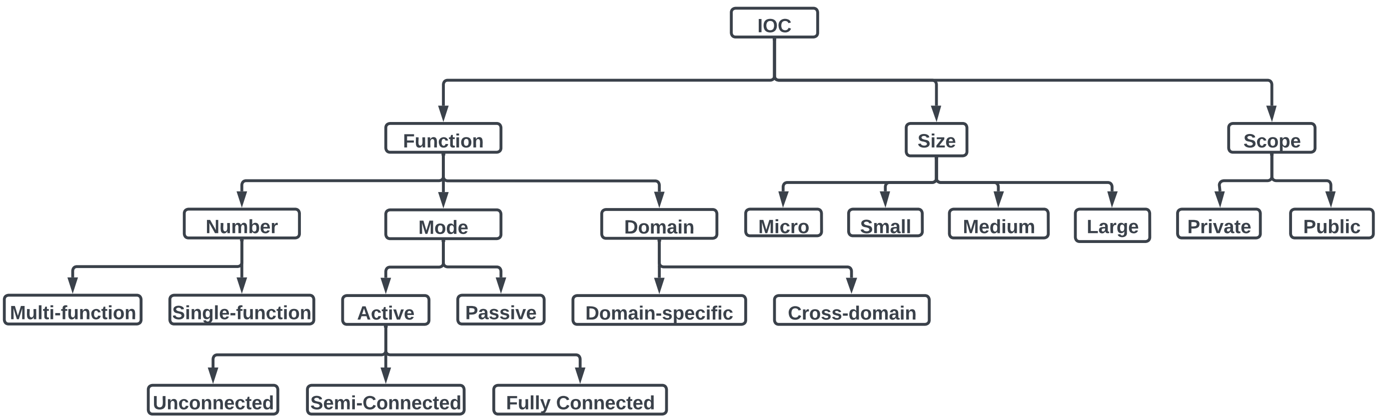


Figure 4. Taxonomy for IOCs in SCs.

2.1. Function

Organizations and the government develop IOCs to serve specific functions. Some functions of IOCs are collecting and unifying data from various sources, automation, facilitating decision making, managing city services, enabling CCTV surveillance, crime prediction, and disaster preparation. Our research shows that IOCs can further be classified by function based on the number or the type of function they offer.

2.1.1. Classification by Number of Functions

Based on the number of functions IOCs offer, they can be either single-function or multi-function IOCs. A single-function IOC (SFIOC) is an IOC designed to offer only one service. Bouleft et al. [62] proposed a cost-effective technique for waste collection that sends smart bins' status to an IOC. The IOC then uses a hybridized genetic algorithm (GA) to plan a cost-effective schedule containing the route for waste collection. An SFIOC does not mean the IOC strictly carries out one function. Instead, it means that, although the IOC has one role in mind, it performs other low-priority functions. For example, Beg et al. [63] proposed a traffic system for Smart Cities, where UAVs, traffic lights, traffic police, and crowdsensing via Google Maps server help to manage the traffic system and expedite emergency responses. Thus, the primary function of the SFIOC is traffic system management, while emergency response is a secondary feature; if the primary function fails, the whole system fails.

Multi-function IOCs (MFIOCs), as the name implies, are IOCs that perform more than one function. They are more common than SFIOCs because of the multi-faceted requirements of cities. In [37], the authors report the success of the Tumakuru Command and Control Center. It is an example of a multi-function IOC that carries out environmental monitoring, solid waste management, emergency response system, and traffic management system. Governments prefer MFIOCs because they allow officials to integrate all departments and agencies into one entity, which enables collaboration and efficiency. A few companies, like Cisco Systems [41], Honeywell [42], and IBM [44], build IOCs that gather information from IoT devices, process it, and use it for several functions. However, other companies only focus on IOCs related to their product line. For instance, Hitachi's IOC processes mainly video data [47]. It allows the company to incorporate its existing solutions into the IOC, thus reducing its production cost.

Both MFIOCs and SFIOCs have several benefits. On the one hand, MFIOCs are larger. Thus, they can integrate several departments and agencies into one virtual body, by which top officials have more control over government workings. It also increases the government's agility since all government agencies (including citizens) are within reach. MFIOCs' large size and complexity mean that more human resources are needed, which means more job opportunities for citizens.

On the other hand, SFIOCs are cheaper to develop. They can be the first step of a phased implementation of an MFIOC, which allows the public to observe its benefits and gain more supporters to move to the next phase. They are also easier to convert from one function to another because they are smaller than MFIOCs, have a less complex structure, and have fewer employees to train than MFIOCs. Furthermore, MFIOCs often have more layers of bureaucracy and a more rigid organizational structure, making it harder to implement changes. A case study [38] shows how the Indian government successfully converted the well-equipped Bhopal Integrated Command and Control Center from environmental monitoring IOC to a COVID-19 emergency response IOC.

2.1.2. Classification by Mode

Figure 4 shows that IOCs can also be classified according to the mode of interaction between the IOC and the Region of Interest (ROI). IOCs can have a passive or active mode of operation. Passive IOCs (PIOCs) do not directly alter their ROI. They do not dispatch professionals or control actuators. They only monitor, archive, and process data. Thus, they mainly function as decision support systems. In [64], the authors proposed a PIOC that uses virtual reality and blockchain technology to improve IOC performance. The system uses Hyperledger fabric blockchain technology [65] to record data from the environment. Then, a virtual reality system is used to visualize the data and help the government make informed decisions in real time. PIOCs are easy and cheap to develop and deploy. They also help in decision support and policy development. However, they are limited in their application since they can only gather data and process them.

Active IOCs (AIOCs) are a superset of PIOCs; all AIOCs have some passive components, but all PIOCs do not have any active ones. Thus, AIOCs conduct data acquisition and processing for decision support, and they also help officials actuate their decisions. We did not include decision automation as a criterion because some decisions are legally required to be carried out by city officials. Moreover, the system's maintenance is not a criterion because it is not part of its goals. There is more demand for AIOCs because they allow the coordination of activities on the ground. Figure 4 shows that there are three types AIOCs:

1. Unconnected AIOCs: These are IOCs that monitor the environment but cannot directly control it. They are the earliest form of AIOCs. They aim to monitor the ROI and send instructions from a centralized area called a "War Room" [37]. Sometimes, they use Participatory Sensing or Mobile Crowd Sensing to cut costs. Participatory Sensing involves collecting data of interest with the help of willing individuals carrying mobile phones, while Mobile Crowd Sensing employs both explicit and implicit user participation and social media data [66,67]. In [21], the authors proposed an SIOC that uses Participatory Sensing, where citizens tag their valuables with Bluetooth beacons. When one of the items is stolen, the SIOC notifies the volunteering participants, who enable their phone's Bluetooth device. The volunteers' phones send sighting information of the item to the SIOC. Then, the SIOC dispatches police to investigate the case further. Unconnected AIOC also finds application in solid waste management: In [62], the authors proposed an AIOC for waste collection in SC. The system consists of smart bins that send their status to an IOC. The IOC uses a hybridized genetic algorithm (GA) to plan a cost-effective schedule containing the route to the full bins for a waste truck. This system is an Unconnected AIOC because it has no actuators that the IOC directly controls; the IOC cannot control either the trucks' or the bins' actions, like moving, locking, or emptying them. Unconnected AIOCs are easiest to maintain because of their low complexity. However, they have the slowest response time because they rely on boots on the ground, which makes it the least accurate system due to human errors.
2. Semi-Connected AIOCs: These AIOCs partly control the ROI directly and are partly controlled manually by boots on the ground. SCs resort to developing semi-connected AIOCs because connecting or automating some controls could be expensive, impossible, or illegal. Some researchers use a Human-in-the-Loop emergency response AIOC [68,69]. The authors used the CitySCAPE framework to develop an agent-based system consisting of sensor agents for monitoring the environment, inference agents that use algorithms to make decisions, and action agents that are a combination of actuators (e.g., alarms, valves, air conditioning, electric gates) and emergency responders. In this system, the IOC monitors the system and controls some parts of the ROI. Traffic management IOCs are also semi-connected AIOCs because the system can control traffic lights, dynamic management signs, and smart gates, but it cannot directly operate the drivers, passengers, and traffic police [70]. Semi-Connected AIOCs integrate existing systems (both connected and unconnected) into a unified system managed by the IOC. The authors in [70] proposed the use of the Integrated Centre of Urban Mobility (CIMU) in São Paulo to optimize the transport system of the city. The authors demonstrate how the CIMU will combine all the existing systems and departments through an IOC. They recommended open protocols to ensure openness and encourage creative solutions from the public. Although the semi-connected AIOC offers some control to the IOC officials, it cannot control the manual part of the system; it can only dispatch the police and advise the drivers and passengers. Thus, for the system's proper functioning, the automated subsystem must account for the errors from the manual part.

3. Fully Connected AIOCs: These AIOCs are connected and can remotely control all parts of the ROI. Some Fully Connected AIOCs find applications in cybersecurity IOCs, where they manage the ROI by determining who receives access to what resources. Xu et al. [71] proposed an example of a cybersecurity Fully Connected AIOC. They used an IOC to develop a Certificateless Designated Verifier Proxy Signature (CLDVPS) scheme, where the IOC has supreme command over the UAV and acts as the original signer; the Ground Control Station (GCS) is entrusted by the IOC to securely send missions to the UAV with the help of a Key Generator Center (KGC). Fully Connected AIOCs also find applications in intrusion detection and prevention systems. In [22], the authors developed a Security Information and Event Management (SIEM) to protect all IoT devices within an SC. The system gathers data from the IoT devices, indexes them, and stores them in an AIOC using Splunk Enterprise [72]. The system analyzes the data using rule-based and machine learning techniques for intrusion detection and prevention. However, privacy is an issue with this technique. They are widely used in Smart Buildings for access controls where all actuators (such as doors, lighting, and ventilation) are remotely accessible. There are some examples of fully connected AIOCs in energy management. Al Kindhi et al. [73] show that an IOC is necessary for the efficient maintenance and monitoring of public lighting. They developed a centralized web-based system for monitoring and controlling solar-powered and IoT-enabled garden streetlights, thus reducing emergency calls and manual patrol. Several papers show that a fully connected Energy Operation Center (EOC) can help public and private buildings save energy by up to 17%. Fully connected AIOCs achieved more efficient service provision since they control the whole system. However, they are expensive to build, especially in large cities.

PIOCs could be the initial development phase of AIOCs. They could also be research facilities for data acquisition. Research shows that PIOC can be converted to AIOC: the Bhopal Integrated Command and Control Center [38], which functions as an environmental monitoring system, was then converted to a COVID-19 emergency response AIOC. Moreover, an AIOC can be an MFIOC; the Tumakuru Command and Control Center consists of an environment-monitoring, solid waste management, emergency response, and traffic management system [37]. AIOCs are more complex than PIOCs. They require more staff to operate.

2.1.3. Classification by Number of Domains

In the context of SCs, a domain refers to a specific area or sector of urban life improvable through technology and data. Neirotti et al. [74] categorized SC domains into hard and soft. The earlier domains include energy, lighting, environment, transportation, buildings, healthcare, and safety, while the latter include education, society, government, and the economy. They propose six application domains for SCs, including natural resources and energy, transport and mobility, buildings, living, government, and economy and people, which address corresponding challenges. Later papers narrow the list to eight domains, as discussed in Section 1 and shown in Figure 5. They are Smart Economy, Smart Environment, Smart Governance, Smart Mobility, Smart Human/Smart People, Smart Living, Smart Healthcare, and Smart Industry and Production [7,8].

An IOC can be domain-specific (DIOC) and cross-domain (CIOC). A DIOC is an IOC that focuses on one domain only. The Smart Environment domain consists of anything within the citizens' surroundings: environment monitoring, surveillance, disaster and emergency response, security, and sanitation. A DIOC for environment monitoring is where sensors in the ROI send measurements like wind, temperature, atmospheric pressure, and humidity to the center where the data are cleaned and stored. The data are also processed to provide government officials the necessary information for decision making. In some countries, the law demands that public data be available to citizens, which encourages disruption in data analytics and the economy of the SC [20]. DIOCs for Smart Buildings also belong to the environment domain. Several companies now have off-the-shelf Smart

Building IOC suites (see Table 2) [43,50]. A DIOC can perform a single function in the case of Bophal IOC [38] or be an MFIOC, like in the case of Tumakuru [37].

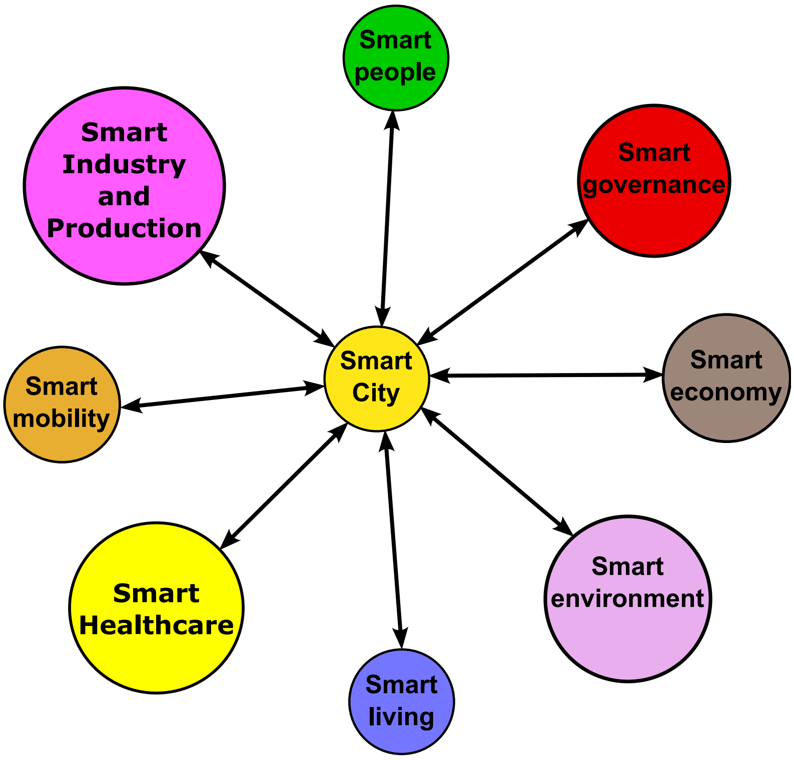


Figure 5. Hard Smart Cities' domains.

CIOCs are those IOCs that combine two or more domains. IBM's InOC is an example of a CIOC, albeit it can serve as a DIOC [17,44]. The system has connection points where new applications can connect to the IOC, providing users the flexibility to expand the IOC's functions. It can manage water management, public safety, transportation, social programs, entertainment venues, buildings, energy, healthcare, and more [17]. A CIOC brings together diverse staff from multiple domains. However, managing such a center can be challenging due to the many employees with different backgrounds. Therefore, the center cannot operate optimally without proper work protocols and staff training on collaboration across the domains. This inter-domain collaboration is crucial for the success of the CIOC. Although DIOCs are cheaper and easier to implement, they leave a communication gap for the decision makers. However, a CIOC can bridge this gap. It also shows the officials new dimensions and challenges that would be invisible otherwise.

2.2. Size

One can measure the size of an IOC by the number of citizens it services, the size of the area it covers, the complexity of operations it can perform, and its computing power (i.e., size, number, and complexity of hardware and software in the system). However, all four criteria are correlated; as the number of citizens or Regions of Interest (ROI) increase, the amount of hardware and software necessary to process the information timely and accurately increases.

Scientists have discussed the layers of IOCs. Prakash and Dattasmita [37] presented street IT infrastructure, Network, Data center, Application, and Integration layers, while India's Ministry of Housing and Urban Affairs (MoHUA) combined the first two layers into one, as shown in Figure 6 [75]. This model considers the network layer as part of the street IT infrastructure. However, Fadli and Sumitra listed only three of the layers (i.e., sensor, network operation center/data center, and COC layer). We adopt the MoHUA because their model has listed all the necessary components in a successful IOC.

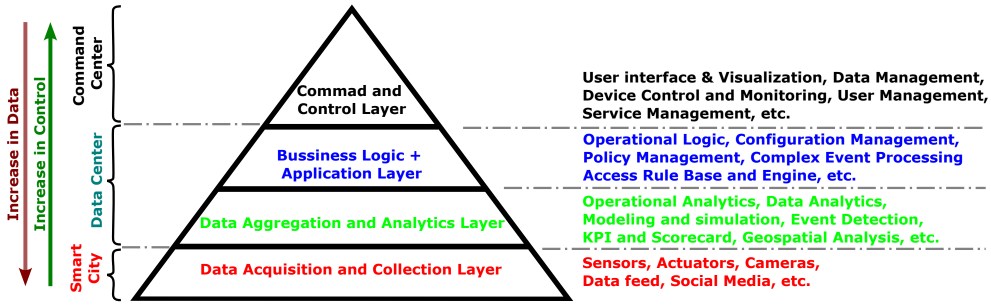


Figure 6. IOC platform architecture.

Figure 6 shows the layers in the architecture of an IOC according to [75]. There are four layers: the data acquisition and collection layer (DACL), the data aggregation and analytics layer (DAAL), the business logic and application layer (BLAL), and the command and control layer (CCL). The DACL is in the ROI. It contains the sensors and actuators that improve citizens' QoL. The DAAL collects, processes, and analyzes the data coming from the DACL. It uses advanced analytics tools and algorithms to identify patterns, trends, and anomalies, which enables informed decision making processes. The authors in [75] combined the Business Logic Layer and an Application Layer to form the BLAL. The Business Logic Layer is a component of software that contains the business logic or rules for how data are processed and managed within an application; the Application Layer is responsible for implementing specific business use cases, such as user authentication or data processing [76]. Both the DAAL and the BLAL are in the data center. The CCL is more like a presentation layer, where users access and visualize the data processed by the immediate BLAL and DAAL.

Moreover, the figure shows that the DACL is in the SC, the DAAL and BLAL are in the data center, and the CCL is in the command center, but this configuration may change. The data center is the heart of the IOC. It ties the DACL and the CCL together by collecting data from DACL, processing them, and sending the information to the CCL. Any change in the DACL's or CCL's size affects the data center's size. When the area or service demand increases, more sensors are necessary for adequate sensing. This sensors increase causes an increase in the data generated, and the additional data require a higher data center. Likewise, an increase in the CCL's functions (see Section 2.1.1) increases the number of requests to the data center, which necessitates a data center upgrade to maintain the IOC's performance. Hence, we classify the sizes of the IOCs according to the size of their data center.

Table 3 shows the four types of data centers. Each type corresponds to a specific size and level of redundancy. Tier 1 has the lowest configuration without redundancy, while Tier 4 has the highest with a fully fault-tolerant redundancy. Therefore, there are four types of IOCs based on their data center. These are micro, small, medium, or large. The Micro-IOC contains a Tier 1 data center or a single workstation. Typically, they manage Smart Buildings, as in [77], where the authors proposed an EOC that consists of a Building Information Modeling (BIM) and a Building Automation System (BAS). It achieved a 17% reduction in energy consumption. A Small IOC requires a Tier 2 data center. It can monitor and control larger environments, like hotels, stadiums, or public buildings. In [78], a small IOC (an EOC) uses Genetic Algorithm to save 9.44–15% of energy consumption of a South Korean City's four public buildings: the office of the community center, the postal office, the police station, and the fire station. A Medium IOC uses a Tier 3 data center. Examples of their application are COC and MOC for small cities or IOC in the early phase of development. The large IOCs are for large cities that use a Tier 4 data center.

Large IOCs store and process more data. Thus, they improve the services of the SC. They also require more staff than their smaller counterparts. However, they are expensive to build and operate. They also have large data centers, typically Tier 3 or 4, consuming enormous amounts of energy, contributing to carbon emissions and climate change [79].

Although smaller IOCs have Tier 1 or 2 data centers or no data centers, their processing power limits their capabilities. Hence, they are only suitable for small areas.

Table 3. Classification of data centers by tiers.

Parameters	Tier 1	Tier 2	Tier 3	Tier 4
Uptime guarantee	99.67%	99.74%	99.98%	100.00%
Downtime per year	<28.8 h	<22 h	<1.6 h	<26.3 min
Component redundancy	None	Partial	Full	Fault-tolerant
Concurrently maintainable	No	No	Partially	Yes
Price	Very Low	Low	High	Very High
Compartmentalization	No	No	No	Yes
Typical customer	Small businesses	Medium businesses	Large businesses	Large enterprises
Build Time	<3 Months	3–6 Months	15–20 Months	16–20 Months
Year first deployed	1965	1970	1985	1995

2.3. Scope

Another way of classifying IOCs is by their scope. In this category, they can be classified into Private and Public IOCs. This classification also indicates the ownership of the center. The proprietary rights of an IOC affect its operations, privacy policy, and how the cities' laws treat them and their data.

2.3.1. Private IOCs

As the name implies, companies or individuals own Private IOCs for their private applications. They monitor and control jurisdictions that are illegal for Public IOCs due to privacy. They find applications in privately owned buildings and industries. Several companies offer IOC suites for Smart Industry and Production applications [41,42,45,46,49]. They typically present a broad view of manufacturing, business processes, and infrastructure operations by combining information from different sources, which helps officials' decision making.

In [78], the authors investigate the performance of EOC in a commercial building. In this case, the IOC and the data belong to the business owner. Shopping malls use IOCs to gain insight into customers' preferences, control crowd distribution, improve customer experience, and increase sales [80]. IBM proposed an Entertainment Venue Operations Center (EVOC) that targets the entertainment industries, like a sports complex or stadium, cruise ship, theater, or concert hall [17]. An EVOC aims to improve the quality of entertainment and enhance the customer experience by improving crowd control, parking, and waiting time.

Private IOCs complement Public IOCs by improving the QoL of workers and customers that constitute the SC. They also improve the SC by collaborating with the government through information sharing or leasing part of their IoT network to the government. Researchers in [81] have demonstrated how smartphones can share livestream data with Public IOCs to improve the community's security. Other benefits of Private IOCs are that they enable businesses to tailor services to customer needs. They also improve manufacturing performance and the coordination of daily activities by increasing collaboration between workers [82]. They also promote greater operational awareness, which in turn helps executives make informed decisions. Their improved crisis response ensures workers' and citizens' safety [82].

2.3.2. Public IOCs

Public IOCs belong to the community. In the case of South Sumatera, Indonesia [25], they are created by the laws or policies of the city's legislature, which means that the city's legislature decides to fund, regulate, or oversee the development and operation of Public IOCs in the SC. However, they are usually developed through special purpose vehicles (SPVs) in India [37,38]. Full-time CEOs head the SPVs, while the board contains nominees of the central government, government, and the Urban Local Bodies (ULBs). In this format, the government lends the SPV financial credibility, and it also helps in building infrastructure that benefits the public [37]. Other ways the government establishes Public IOCs are joint ventures, subsidiaries, public–private partnerships (PPP), or turnkey contracts.

Table 4 shows that COC and MOC are the same. The table shows that neither population nor area determines the center's name. The difference in nomenclature depends on the country's administrative terminology. Fadli and Sumitra [52] surveyed Bandung COC. Bandung is the capital of West Java Province, Indonesia. Bandung COC is for e-government applications. The DACL is a wireless network of audio and visual sensors, while the DAAL is hierarchical: the data center is at the top and the local government areas (SKPD) at the bottom. The SKPDs collect data from their subnet and send it to the data center for backup and processing. The CCL monitors the communities' activities by monitoring the SKPDs' performance reports. Another example of a COC is the Daejeon Smart City Operation Center in Daejeon City, South Korea. It is a security and emergency response IOC. It reduced the response time from 7.5 min to 6.0 min while decreasing the crime rate by 5.0% and increasing the arrest rate by 7.7%. However, COC projects have a history of delays. The Daejeon took 4 years to complete [30]. COC project delays are due to factors such as fundraising, budget constraints, and collaboration between various departments, which can lead to delays due to differences in priorities. Additionally, there are few Public IOC solutions in the market due to the market size and the large number of parameters to consider during development. Thus, tech companies often collaborate with the customer (i.e., the government) to design a system to accommodate their needs, which increases development price.

Table 4. List of COC and MOC in the literature.

Ref.	Country	City	Population	Area (km^2)	Center
[27]	Portugal	Porto	214,349	41.42	MOC
[35,36]	Russia	Novgorod	218,717	229.28	MOC
[37]	India	Tumakuru	302,143	44.47	MOC
[31]	Indonesia	Jambi	702,209	205.38	MOC
[30]	S. Korea	Daejeon	1,475,221	539.80	COC
[29]	Brazil	Porto Alegre	1,483,771	496.00	MOC
[20]	Spain	Barcelona	1,636,762	101.90	COC
[38]	India	Bhopal	1,798,218	286.00	MOC
[29]	Brazil	Belo Horizonte	2,501,576	331.00	MOC
[32]	Indonesia	Bandung	2,575,478	167.70	COC
[26,27]	Brazil	Rio de Janeiro	6,718,903	1221.00	MOC
[20]	United Kingdom	London	9,126,366	1572.00	COC

2.3.3. Collaborations in Public IOCs

Meijer and Bolívar [83], define an SC as a city with smart collaboration, while Chun et al. define collaboration as "a process or set of activities in which two or more agents work together to achieve shared goals" [84]. Hence, although the primary goal of an IOC is to optimize services in an SC to improve QoL, they must also help improve collaboration between the government, citizens, and other stakeholders. Unlike the Private IOC, where the employees share a mission, vision, and culture and work towards the same goals, the Public IOC is more diverse, consisting of various government departments having different priorities, policies, and regulations, which can lead to conflicting interests and goals.

Figure 7 shows the types of collaboration a government can harness for a sustainable SC. The government can collaborate with citizens, organizations, and sectors to maximize the efficiency of the IOC.

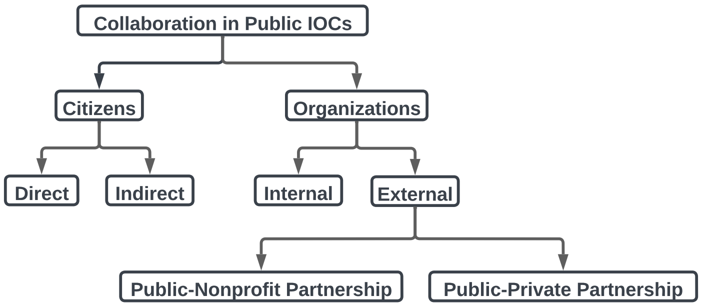


Figure 7. Collaboration in Public IOCs.

Government–Citizen Collaboration (GCC) is when the government engages citizens in governance. This type of collaboration increases citizens' trust and confidence in their government [29]. There are two types of GCCs: direct and indirect. A direct GCC is when citizens directly contribute to the IOC's operations. Participatory sensing is an example of direct GCC, where the citizens use their smartphones to sense the environment and send the information to the IOCs. Papadakis et al. proposed a Bluetooth-based beacon attached to a stolen item that communicates with volunteering participants (i.e., citizens) [21]. The volunteers' phones send sighting information of the item to the IOC, where police further investigate. Another form of direct GCC is Smart Governance: it is the engagement of various stakeholders in decision making and public services [29]. MOCs in Brazil use social media and the internet to communicate with citizens [53], while London uses open data to enable citizens to come up with solutions to the city's pressing problems [20]. Indirect GCC is when citizens contribute to governance through their government representatives, who present those inputs at the IOC war room meetings [29]. Some of the concerns of GCC are [29]: (1) the digital divide excludes a large section of the citizens in the city's development, (2) more demands by the citizens [29], and (3) difficulty in sensitizing the citizen on the role of the IOC, and the hows and why they should contribute.

Government–Organization Collaboration (GOC) is the relationship between the government and other government or non-government organizations to ensure the smooth working of the IOC. There are two main types of GOCs: internal and external collaborations. Internal GOC refers to the joint effort of government organizations to ensure an efficient IOC. It can be inter-agencies, inter-departmental, inter-organizational, or cross-collaboration within the government [29]. Interviews with IOC officials show that they emphasize collaboration in data sharing and decision making [29,53,59]. Internal collaboration can be at the data sharing level or the decision making level. At the data sharing level, the various departments access one another's data. However, difficulty arises in this type of collaboration due to a lack of contextualization of the shared data [29]. Kushnareva et al. [35] cited an example of the lack of context awareness of meteorological (rainfall) data that failed to adjust water release plans, which caused a severe flood event in Brisbane, Australia. At the decision making level, IOCs have war rooms where government representatives deliberate on cases with significant political ramifications [29].

External collaboration refers to the cooperation of the Public IOC with non-governmental entities like civic groups, nonprofit organizations (NPOs), and for-profit organizations [53]. Researchers also refer to it as a cross-sectoral or inter-sectoral collaboration because it is a relationship between the public, private, and nonprofit sectors. Public–private partnership (PPP) allows the government to reach the vulnerable. An example is Daejeon IOC signing an agreement with private communications companies to provide emergency services to vulnerable groups, like children, patients with dementia, and senior citizens living alone [30]. Also, PPP helps the IOC reduce running costs. The authors in [85] cited how Rio de Janeiro IOC uses the Waze application to monitor the city's traffic. However, due to the large number of cameras deployed in the city, the IOC collaborates with laboratories from the engineering school at the Federal University of Rio de Janeiro, which use AI algorithms to select the co-located cameras based on data from platforms like Waze [85].

This collaboration indicates the existence of a public–private-university relationship. Public–nonprofit partnership (PNP) is widely observed between EOCs and NPOs [86,87]. It allows them to contribute their quota to the city's success by helping the IOC solve complex societal problems or overcoming socio-technical hurdles [88]. However, they have some challenges, such as privacy and other legal issues, lack of trust, conflicting interests, and coordination difficulties.

3. Humanitarian Engineering in IOCs

In this section, we investigate the impact of IOC on SC from a humanitarian engineering perspective. Humanitarian engineering is a field of engineering that focuses on using engineering principles to address social issues and improve the QoL for underserved communities. It includes designing and implementing solutions for clean water, sanitation, healthcare, energy, and transportation. Humanitarian engineers work collaboratively with community members to identify needs and develop sustainable solutions that are culturally appropriate and environmentally responsible. The ultimate goal of humanitarian engineering is to create a positive social impact and promote equity and justice in society.

The primary aim of an SC IOC is to improve QoL. In the transportation sector, IOCs ensure the safety of passengers and pedestrians. In [23], the authors use Vehicular Ad Hoc Networks (VANETs) and machine learning to improve traffic efficiency and safety. The system implements driver maneuver prediction to prevent collisions, especially at intersections. However, the system's scalability largely depends on the Traffic Command Center (TCC) to dynamically plan traffic while anticipating the drivers' intentions. Additionally, the system must be real-time-based because a collision prevention system is a safety-critical system. Thus, it will require deploying real-time middleware systems, which increases the system's cost.

Security and emergency response are the primary concerns of cities. MoHUA included it in the "Extent of crimes recorded against women, children and elderly per year" as one of the indicators of a successful SOC [75]. Daejeon City IOC signed an agreement with the private communication companies in the city to protect children, dementia patients, senior citizens, and people with disabilities as one of the primary functions of its MFIOC [30]. The government prioritized aiding these groups because they often cannot communicate their location or needs during emergencies. Thus, the IOC uses the data from private companies, including photos and location information, to determine a citizen's whereabouts and situation. Based on this information, the center could take appropriate action, such as alerting law enforcement or other emergency responders. Although the process saves lives, it has some serious privacy issues.

Furthermore, IOCs help underserved communities by mining information from social media. Social media applications are platforms for minorities and the underserved to air their grievances and highlight issues they face. Through IOCs, these concerns and requests can be directly linked to the mayor's office [29,53,75], allowing for prompt action. This integration between social media and IOCs has given a voice to the underserved and allowed them to participate in society in ways that were not possible before. It is a powerful tool for promoting inclusivity and ensuring that everyone's concerns are heard and addressed. However, the veil of anonymity on social media can also make it conducive to bullying and harassment. Therefore, the government needs to address these issues to encourage the participation of minorities and underserved communities in public discourse.

4. Challenges

IOCs are central hubs in SCs that collect and analyze data from various sources. IOCs can aid in emergency response, public safety, and transportation management. IOCs can quickly identify and respond to incidents such as traffic accidents, natural disasters, and crime by gathering real-time data from sensors, cameras, and other devices. Furthermore, IOCs can improve city planning and resource allocation by providing insights into patterns of urban life, such as foot traffic, energy consumption, and air quality. Overall, IOCs can assist cities in becoming more efficient, sustainable, and resilient. However, SC IOCs are difficult to develop because the government (1) requires legislative approval for the project, (2) has to determine the departments and agencies to involve in the IOC, (3) must outline how the IOC will collaborate with the citizens, (4) must also ensure transparency, and (5) must protect citizens' privacy according to the law. Other challenges of IOCs are as follows:

1. Privacy Issues: The IOC is the navel of the SC, where all data are accessible. Thus, information misuse, information inequity, and privacy violations could occur from both external and internal perpetrators. Unfortunately, many IOCs do not have clear procedures for treating users' data [27]. Therefore, the government must consider privacy per the city's laws at all phases of the IOC's development [75]. It must also have a privacy protection framework that detects violations and violators. In the event of privacy violation, the framework should also have event mitigation and recovery processes. However, privacy often becomes a barrier to cross-sectorial collaboration, causing delays or hindering access to some services. Thus, many cities' privacy acts contain clauses that enable law enforcement officers and emergency responders limited access to private citizens' information in danger. The South Korea Information Protection Act allows third parties to access personal data when there is a threat to life or physical property or during a criminal investigation [30]. However, the implementation of privacy policies is not the only problem; Bernardes et al. [27] argue that there are also academic gaps for legal/normative production.
2. Public–Nonprofit Collaboration Issues: Collaboration is an essential management skill for the unprecedented demand for quick disaster response [87]. Often, during a disaster, the first responders are the citizens in the area. However, public managers hesitate to rely on volunteers and NPOs during extreme events due to concerns over their intentions, skills, resources, safety, and legal liability [33,89]. This reluctance results in IOCs that lack the mechanisms for absorbing volunteers. Meanwhile, the NPOs' challenge is finding the right place and time to help [87]; this information is readily available to the government through its IOC. They also face difficulty managing unsolicited donations and unaffiliated volunteers [87], which the IOC can easily redistribute since it has a bird's eye view of the situation. They also struggle to organize pre-disaster training for their staff, while the government has professionals on standby that can help provide such training. Therefore, SC IOCs must have a database of NPOs to ensure collaboration. Also, IOCs can use machine learning to reallocate unsolicited donations and unaffiliated volunteers to NPOs or locations where they are much needed. Thus, the government can use IOCs to streamline philanthropic decisions, especially during emergencies. Also, there is a need for emergent human resources models that incorporate emergent volunteers into an organized emergency response [33].
3. Intra-governmental Collaboration Issues: Effective coordination in an IOC partnership between government departments and agencies ensures that timing, quality, and resources are on schedule. Therefore, there is a need to investigate institutional arrangements that affect IOCs, especially disaster recovery. This issue has two faces: on the one hand are government agencies that are reluctant to participate in IOC partnership agreements [53]. A long-standing reason is that they see this type of collaboration as an additional function to their original function [90]. Other reasons are limited resources, budgets, and staffing may constrain departments' collaboration. On the other hand, government entities that are willing to collaborate face challenges during the agreement phase and running of the IOC. During the agreement phase, the common challenges are bureaucracy, institutional barriers, and coordination issues [30]. In the running phase, the partners encounter conflicting interests and objectives, which may arise due to varying priorities, policies, and regulations. Secondly, distinct organizational structures, cultures, and communication channels may impede effective collaboration. Lastly, varying autonomy, accountability, and authority levels may impact the willingness to share information and cooperate.

4. Security Issues: There are incentives for attackers to target SC IOCs: (1) they are the central hub for managing critical infrastructure and services, such as transportation, utilities, and emergency response; Roy et al. [91] show that smart traffic systems can be victims of stealth attack and an IOC can be an intrusion detection and prevention system for such attacks; (2) they collect large amounts of data, which makes them prime targets for cybercriminals seeking to steal personal information; (3) attacking them causes widespread chaos and harm to citizens and businesses with little effort; (4) the IOCs rely on IoT devices that may have vulnerabilities that attackers can exploit [92]. The literature proposes several solutions: Sophisticated decentralized password authentication systems can protect IOCs' assets [93]. Some researchers advocate using a Cybersecurity Operation Center (COC) to protect the IOC and its sensors [92,94]. In [94], the authors proposed a three-tier security system for SCs. The first tier involves component-level security using authentication and encryption. The second tier uses independent defense mechanisms, such as anti-malware software and firewalls, while the third tier is an SOC that collects real-time activity data from all devices. Then, the SOC team uses advanced data analytics, machine learning, and visualization techniques to identify and respond to attacks. However, this Human-in-the-Loop technique has a slow response. The government may hesitate the automating cyberattack mitigation for legal and political reasons. Additionally, building a separate IOC for security alone is expensive. To cut costs, the SOC can be a subsystem or a department of the IOC.
5. IOC Performance Issues: Concerning performance, we focus on energy consumption and latency. Energy consumption is a vital factor because of its financial and environmental implications. The energy consumption of IOCs is proportional to their size (see Section 2.2). Thus, Large and Medium IOCs, commonly used for Public IOCs, consume the most energy because the quantity of data they process makes it necessary to use higher-tier data centers. A possible solution is Nano Data Centers (NaDa) [95]. They save up to 30% of the energy of traditional data centers because they reuse already committed baseline power, avoid cooling costs, and reduce network energy consumption. Alternatively, the IOCs can switch to renewable energy or develop systems with lower computational overhead [96]. Another issue with IOCs' performance is latency. We define IOC latency as the time from when the IOC receives a service request to when it responds with a solution. The IOC latency is affected by two factors: the time it takes the IOC to process the data and the time it takes the IOC to make a decision. Increasing the computation power of the IOC can reduce the earlier factor, but it increases its energy consumption. It can reduce its workload with Fog Computing to filter or process data at the network's edge [80,97]. The latter factor depends on the officials' latency to make a decision. Artificial intelligence can automate non-critical decisions [29]. In [98], the authors used two AI paradigms: Action Languages and Answer Set Programming to allow an agent to plan delivery like a multiple Travelling Salesperson Problem. For critical decisions, the IOC can use technologies like virtual reality to simplify information to enable officials to make informed decisions in real time [64].
6. Compatibility Issues: Interviews with practitioners show that systems' interoperability is a barrier even in more advanced technological-maturity-level IOCs [29]. The IOCs are inherently heterogeneous at all layers of the IOC platform architecture (see Figure 6): In the Smart City layer, designing the connection between sensors can be challenging due to the diverse range of sensors available. As most companies specialize in a specific type of sensor, the IOC must obtain sensors from multiple companies that use varying technologies. This diversity means careful design is necessary to ensure successful sensor networks. At the data center, heterogeneity is often inevitable because different applications have different requirements and characteristics. For example, some applications may require high computational resources, while others require large storage capacity. Thus, incorporating a mix of hardware and

software technologies can optimize data centers to meet the needs of their users. Also, heterogeneous systems can lead to better fault tolerance, energy efficiency, and cost-effectiveness. However, managing and integrating these systems can be challenging and requires careful planning and execution. It also affects the security considerations of the IOC [92]. At the command center layer, the incompatibility between the IOC's systems and the legacy systems of the agencies and departments increases the IOC's complexity and errors in center management, leading to decreased efficiency and effectiveness [29]. Also, data heterogeneity from several departments makes it necessary to develop data mining solutions [99]. Therefore, researchers must investigate the use and performance of middleware technologies on the IOC and all of its layers. Additionally, practitioners should adhere to standards. Although applying standards is optional, using them makes the design process easier, ensures compatibility with application standards, and can solve unexpected issues [100].

7. Financial Issues: Financial issues in an IOC are complex because they affect both the human resource and the technological dimensions [29]. Surveys of some IOCs in Brazil show that budget constraints lead to a lack of human resources [29]. From the technological perspective, both the IOC's initial and running costs are high. Building the Rio de Janeiro IOC cost approximately BRL 68.9 million (USD 29.3 million) [28], while Daejeon IOC deployed 4288 public security CCTVs at the cost of USD 17,000 per CCTV, without the installation, support, and control systems costs [30]. Some IOCs deploy cheap sensors in non-critical sensing like pollution and noise [59]. Akbar et al. [81] developed an IOC that uses inexpensive smartphones to replace CCTV cameras. However, smartphones are not durable enough to withstand outdoor conditions, and they do not have surveillance-specific features like night vision and motion tracking. Another cheap option for environmental sensing is participatory sensing, where citizens volunteer to sense the environment for the IOC [21,66]. However, participatory sensing is unreliable because volunteers may be unavailable when needed. It also puts the volunteers in harm's way, especially in SOCs and EOCs. Some researchers argue that PPP is a possible solution to budget constraints challenges [29]. Financial contributions of players and the role of the government in providing subsidies help reduce the initial and running costs of IOCs [28,30]; the state Ministry of Justice and the federal-level Extraordinary Secretary for Mega-Event Security jointly financed the Rio de Janeiro IOC [28].
8. Environmental Issues: IOCs have a significant environmental impact. Although some IOCs incorporate some environment-aware components in their decision making [37,62,68], many do not [99]. The data center and command center levels (see Figure 6) contribute the most impact [67,101–103]: They consume large amounts of electricity, which contributes to carbon emissions and global warming; the data centers in the US (accounting for one quarter of global data centers) are responsible for 1.8% and 0.5% of energy consumption and greenhouse gas emissions in the country [104]. They also require vast amounts of water for cooling, straining the local water resources. Additionally, they generate copious amounts of heat and can contribute to urban heat islands. Also, their construction and maintenance can lead to deforestation and habitat destruction. Therefore, more research on sustainable IOC solutions is necessary. However, at the city level, the environment impacts sensors. For example, extreme temperatures can cause hardware failure or reduce battery life. High humidity can cause corrosion and damage to components, while excessive sunlight can cause overheating and degradation of plastic casing and parts. Bad weather can also affect sensing; dust, debris, and other particulate matter render CCTV data useless. Nikolic et al. [105], proposed weather-resistant surveillance systems consisting of a Remotely Piloted Aircraft System (RPAS) with a Multi-Functional Radar System (MFRS). However, this approach is not scalable as it will be too expensive to deploy on a large scale. Therefore, there is a need for affordable weather-resistant sensors or sensing techniques that are deployable at a large scale.

9. Social Issues: The development of IOCs benefits cities, but it only makes them “smart” if it empowers citizens and enhances democratic debates about the kind of city people want to live in. However, research shows that SC IOCs do not help to solve problems of inequality, poor governance, or compromised urban planning agendas [28]. At the citizens’ level, the IOCs’ use of machine learning and other forms of automation are responsible for workforce displacement. Social inequalities are another issue affecting IOCs. Many IOCs use social media and mobile applications to aid decision making, which automatically alienates people with little or no access to the internet and those without technology experience [29,53,75]. IOCs also worsen the consequences of the digital divide, such as in the case of Daejon IOC [30], where children, seniors, and dementia patients with access to telecommunication services receive immediate help. SC technologies such as IOCs lead to technology dependencies, which may have unforeseen consequences. At the administrative level, the integration of municipal operations centers faces cultural barriers and resistance to change at both individual and organizational levels. Individual resistance comes when there is a shift from a hierarchical to a collaborative structure, leading to pride becoming a barrier to collaborative governance [29]. Also, representatives often prioritize individualism and their agency [29]. Therefore, there should be sensitization to show staff the benefits of non-hierarchical collaboration. The IOC should also have clear goals, a mission, and a vision. At the citizen level, policies should balance service provision against a reduced public budget to avoid unfair monopoly and politicizing IOCs by active stakeholders in an SC [106].

5. Conclusions

An IOC is a centralized facility that provides a comprehensive view of an organization’s or SC’s operations by integrating data from multiple sources. Cities and other organizations typically use it to monitor and manage real-time systems, such as transportation, public safety, and utilities. An IOC uses advanced analytics and visualization tools to process large amounts of data and provide actionable insights. By providing a centralized view of operations, the IOC enables organizations to make informed decisions, improve efficiency, and respond more quickly to emergencies and other events.

This paper surveyed 45 papers. It classifies IOCs into three main classes based on their function, size, or scope. This survey showed that an IOC’s function has three subclasses depending on how one looks at it. Looking at the number of functions: an IOC can be a single-function or a multi-function IOC; the function’s nature classifies the IOC into active—an IOC that can directly change its environment—or passive; the diversity of domains the IOC targets classifies it as either domain-specific or cross-domain. According to the size category, the IOC can be micro, small, medium, or large, while, in the scope category, IOCs are either private or public. Private IOCs are individual-owned or company-owned, while Public IOCs are community-owned. We found that Public IOCs have more challenges than Private IOCs because of the diversity among the collaborators, who may have different goals, the availability of funds, and legal constraints.

We also investigated how IOCs help underserved citizens. We found a few cases of humanitarian engineering in IOCs, outside emergency response and security IOCs. Therefore, Public IOC design should include the physically challenged, the poor, and citizens with limited access to technology. Finally, the research has uncovered nine challenges that fall into three groups: social, financial, and performance. The social issues include environmental, privacy, and collaboration challenges. Finance-related problems are common in Public IOCs where their monetary gains are not immediately conspicuous. The performance issues refer to energy consumption and service delays. Energy consumption by IOCs exacerbates the financial and environmental impacts, while service delays defeat one of the main objectives of the SC concept. Therefore, research on optimizing IOCs’ energy consumption while reducing service delays is necessary.

Author Contributions: Conceptualization, B.A.; methodology, F.A.; validation, B.A., F.A. and A.A.; formal analysis, B.A., F.A. and A.A.; investigation, B.A., F.A. and A.A.; resources, F.A.; data curation, F.A. and A.A.; writing—original draft preparation, F.A.; writing—review and editing, B.A., F.A. and A.A.; visualization, F.A.; supervision, B.A.; project administration, B.A. All authors have read and agreed to the published version of the manuscript.

Funding: The APC was funded by the Deanship of Research Oversight and Coordination (DROC), King Fahd University of Petroleum and Minerals (KFUPM).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to acknowledge all support provided by Alfozan Academy, the Center for Excellence in Development of Nonprofit Organizations (CEDNPO), Applied Research Center for Metrology, Standards, and Testing, and King Fahd University of Petroleum and Minerals (KFUPM).

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

SC	Smart Cities
IOC	Integrated Operations Center
SFIOC	Single-function Integrated Operation Center
MFIOC	Multi-function Integrated Operation Center
DIOC	Domain-specific
CIOC	Cross-domain
DACL	Data Acquisition and Collection Layer
DAAL	Data Aggregation and Analytics Layer
BLAL	Business Logic and Application Layer
CCL	Command and Control Layer
EOC	Energy Operation Center
PIOC	Passive IOC
AIOC	Active IOC
QoL	Quality of Life
GCC	Government–Citizen Collaboration
GOC	Government–Organization Collaboration
GSC	Government–Sector Collaboration
PPP	Public–Private Partnership
PNP	Public–Nonprofit Partnership
NPO	Nonprofit Organization
IoT	Internet of Things

References

1. UN. *68% of the World Population Projected to Live in Urban Areas by 2050, Says UN*; UN Desa Department of Economic and Social Affairs: New York, NY, USA, 2018.
2. WB. *Urban Development Overview*; World Bank (WB): Washington, DC, USA, 2022. Available online: https://www.worldbank.org/en/topic/urbandevelopment/overview (accessed on 8 June 2023).
3. Yin, C.; Xiong, Z.; Chen, H.; Wang, J.; Cooper, D.; David, B. A literature survey on smart cities. *Sci. China Inf. Sci.* **2015**, *58*, 1–18. [CrossRef]
4. Silva, B.N.; Khan, M.; Han, K. Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities. *Sustain. Cities Soc.* **2018**, *38*, 697–713. [CrossRef]
5. Wu, J.; Guo, S.; Huang, H.; Liu, W.; Xiang, Y. Information and Communications Technologies for Sustainable Development Goals: State-of-the-Art, Needs and Perspectives. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 2389–2406. [CrossRef]
6. Lai, C.S.; Jia, Y.; Dong, Z.; Wang, D.; Tao, Y.; Lai, Q.H.; Wong, R.T.K.; Zobaa, A.F.; Wu, R.; Lai, L.L. A Review of Technical Standards for Smart Cities. *Clean Technol.* **2020**, *2*, 290–310. [CrossRef]

7. Arroub, A.; Zahi, B.; Sabir, E.; Sadik, M. A literature review on Smart Cities: Paradigms, opportunities and open problems. In Proceedings of the 2016 International Conference on Wireless Networks and Mobile Communications (WINCOM), Fez, Morocco, 26–29 October 2016; pp. 180–186. [CrossRef]
8. Bellini, P.; Nesi, P.; Pantaleo, G. IoT-Enabled Smart Cities: A Review of Concepts, Frameworks and Key Technologies. *Appl. Sci.* **2022**, *12*, 1607. [CrossRef]
9. Kézai, P.K.; Fischer, S.; Lados, M. Smart economy and startup enterprises in the Visegrád Countries—A comparative analysis based on the Crunchbase Database. *Smart Cities* **2020**, *3*, 1477–1494. [CrossRef]
10. Sarker, I.H. Smart City Data Science: Towards data-driven smart cities with open research issues. *Internet Things* **2022**, *19*, 100528. [CrossRef]
11. Nazim, S.F.; Danish, M.S.S.; Senjyu, T. A brief review of the future of smart mobility using 5G and IoT. *J. Sustain. Outreach* **2022**, *3*, 19–30. [CrossRef]
12. Mun Chye, C.; Fahmy-Abdullah, M.; Sufahani, S.F.; Bin Ali, M.K. A Study of Smart People Toward Smart Cities Development. In Proceedings of the Third International Conference on Trends in Computational and Cognitive Engineering, Virtual, UTHM, Malaysia, 21–22 October 2021; Kaiser, M.S., Ray, K., Bandyopadhyay, A., Jacob, K., Long, K.S., Eds.; Springer Nature: Singapore, 2022; pp. 257–271. [CrossRef]
13. Gaur, B.; Shukla, V.K.; Verma, A. Strengthening People Analytics through Wearable IOT Device for Real-Time Data Collection. In Proceedings of the 2019 International Conference on Automation, Computational and Technology Management (ICACTM), London, UK, 24–26 April 2019; pp. 555–560. [CrossRef]
14. Laurent, P.; Erica, M.; Laurent, F.; Daniela, C.; PwC Luxembourg. Understanding the Smart Living trend—Smart Construction Products and Processes. In *Smart Living: Smart Construction Products and Processes*; European Union: Brussels, Belgium, 2014; pp. 3–4.
15. Nasr, M.; Islam, M.M.; Shehata, S.; Karray, F.; Quintana, Y. Smart Healthcare in the Age of AI: Recent Advances, Challenges, and Future Prospects. *IEEE Access* **2021**, *9*, 145248–145270. [CrossRef]
16. Lopes, N.V.M.; Farooq, S. Smart City Governance Model for Pakistan. In *Smart Governance for Cities: Perspectives and Experiences*; Springer International Publishing: Cham, Switzerland, 2020; pp. 17–28. [CrossRef]
17. Arundhati, B.; Eduardo, F.; Luis, G.; Robert, L.; Pam, N.; Shi, W.Y. IBM Intelligent Operations Center for Smarter Cities Administration Guide. *IBM* **2012**, *1*, 4–5.
18. Huawei. *Intelligent Operation Center Solution*; Huawei Enterprise: Singapore, 2022.
19. Yong, P. *Intelligent Operations Center: A Smart Brain for City Management*; Huawei Enterprise: Singapore, 2022.
20. Bibri, S.E. The Leading Data-Driven Smart Cities in Europe: Their Applied Solutions and Best Practices for Sustainable Development. In *Advances in the Leading Paradigms of Urbanism and Their Amalgamation: Compact Cities, Eco–Cities, and Data–Driven Smart Cities*; Springer International Publishing: Cham, Switzerland, 2020; pp. 227–258. [CrossRef]
21. Papadakis, N.; Koukoulas, N.; Christakis, I.; Stavrakas, I.; Kandris, D. An IoT-Based Participatory Antitheft System for Public Safety Enhancement in Smart Cities. *Smart Cities* **2021**, *4*, 919–937. [CrossRef]
22. Hwoij, A.; Khamaiseh, A.; Ababneh, M. SIEM Architecture for the Internet of Things and Smart City. In Proceedings of the International Conference on Data Science, E-Learning and Information Systems 2021, DATA'21, Petra, Jordan, 5–7 April 2021; Association for Computing Machinery: New York, NY, USA, 2021; pp. 147–152.
23. Zhang, H.; Fu, R.; Wang, C.; Guo, Y.; Yuan, W. Turning Maneuver Prediction of Connected Vehicles at Signalized Intersections: A Dictionary Learning-Based Approach. *IEEE Internet Things J.* **2022**, *9*, 23142–23159. [CrossRef]
24. Nokia. *Integrated Operations Center for Smart Cities*; Nokia: Espoo, Finland, 2021.
25. Hasmawaty.; Utami, Y.T.; Antoni, D. Building Green Smart City Capabilities in South Sumatra, Indonesia. *Sustainability* **2022**, *14*, 7695. [CrossRef]
26. Muse, L.P.; Martins, P.R.; Hojda, A.; Abreu, P.A.d.; de Almeida, P.C. The role of Urban Control and Command Centers in the face of COVID-19: The case of COR in Rio de Janeiro, Brazil. In Proceedings of the 2020 IEEE International Smart Cities Conference (ISC2), Virtual, 28 September–1 October 2020; pp. 1–8. [CrossRef]
27. Bernardes, M.B.; de Andrade, F.P.; Novais, P. Smart cities, data and right to privacy: A look from the Portuguese and Brazilian experience. In Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance, Galway, Ireland, 4–6 April 2018; pp. 328–337.
28. Gaffney, C.; Robertson, C. Smarter than Smart: Rio de Janeiro's Flawed Emergence as a Smart City. *J. Urban Technol.* **2018**, *25*, 47–64. [CrossRef]
29. Pereira, G.V.; Cunha, M.A.; Lampoltshammer, T.J.; Parycek, P.; Testa, M.G. Increasing collaboration and participation in smart city governance: A cross-case analysis of smart city initiatives. *Inf. Technol. Dev.* **2017**, *23*, 526–553. [CrossRef]
30. Kim, H.; Choi, D.; Lee, Y. *Improving Interagency Collaboration for an Innovative Emergency Response System: The Daejeon Smart City Operation Center, 2010–2017*; Global Delivery Initiative: San Jose, Costa Rica, 2021; pp. 1–13.
31. Pratama, I.; Suswanta, S. Artificial Intelligence in Realizing Smart City through City Operation Center. In Proceedings of the International Conference on Public Organization (ICONPO 2021), Yogyakarta, Indonesia, 13–14 August 2021; Atlantis Press: Amsterdam, The Netherlands, 2022; pp. 53–60.
32. BAP. *Bandung Command Center—Bagian Administrasi Pembangunan*; Bagain Administrasi Pembangunan: Bandung, West Java, Indonesia, 2021.

33. Lutz, L.D.; Lindell, M.K. Incident Command System as a Response Model Within Emergency Operation Centers during Hurricane Rita. *J. Contingencies Crisis Manag.* **2008**, *16*, 122–134. [CrossRef]
34. Zhuhadar, L.; Thrasher, E.; Marklin, S.; nez de Pablos, P.O. The next wave of innovation—Review of smart cities intelligent operation systems. *Comput. Hum. Behav.* **2017**, *66*, 273–281. [CrossRef]
35. Kushnareva, E.; Rychkova, I.; Le Grand, B. Modeling business processes for automated crisis management support: Lessons learned. In Proceedings of the 2015 IEEE 9th International Conference on Research Challenges in Information Science (RCIS), Athens, Greece, 13–15 May 2015; pp. 388–399. [CrossRef]
36. Kushnareva, E.; Rychkova, I.; Le Grand, B. Modeling and Animation of Crisis Management Process with Statecharts. In Proceedings of the Perspectives in Business Informatics Research, Tartu, Estonia, 26–28 August 2015; Matulevičius, R., Dumas, M., Eds.; Springer International Publishing: Cham, Switzerland, 2015; pp. 145–160.
37. Prakash, B.; Dattasmita, H. A Case Study of Command-and-Control Center—A DSS Perspective. In *Decision Support Systems for Smart City Applications*; John Wiley & Sons, Ltd.: Hoboken, NJ, USA, 2022; Chapter 2, pp. 17–33. [CrossRef]
38. Bagdi, S.S.; Mondal, M.; Chatterjee, A. Gas Tragedy and COVID-19 Vulnerabilities: An Analysis of Health Infrastructure in Bhopal, India. In *COVID 19, Containment, Life, Work and Restart: Urban Studies*; Springer Nature: Singapore, 2022; pp. 99–114. [CrossRef]
39. Megan, M. *Honeywell and Accelerator for America Collaborate to Promote Smart City Growth in Five U.S. Cities*; Hoenywell International Ress & Media: Charlotte, NC, USA, 2022.
40. Ashley, L.; Tyler, S. *Siemens Advanta Joins Colorado Smart Cities Alliance*; Siemens USA Press Release: Munich, Germany, 2021.
41. Cisco. *Cisco Smart+Connected City Operations Center: Unified Management for City Infrastructure*; Cisco System: San Jose, CA, USA, 2014.
42. Honeywell. *Honeywell Building Technologies; Smart Cities; Honeywell City Suite*; Honeywell: Charlotte, NC, USA, 2022.
43. Siemens. *Building X Cloud-Based Smart Building Software Platform*; Siemens: Munchen, Germany, 2023.
44. IBM. *Intelligent Operations Center 5.2.0*; IBM: Armonk, NY, USA, 2021.
45. GE. *Remote Operations—Command Center*; General Electric Company (GE): Boston, MA, USA, 2021.
46. AVEVA. *AVEVA Unified Operations Center*; Schneider Electric: Andover, MA, USA, 2023.
47. Hitachi. *Smart Spaces—Improve Safety and Efficiency*; Hitachi Vantara: Santa Clara, CA, USA, 2023.
48. Motorola. *Network & Security Operations Center*; Motorola Solutions: Chicago, IL, USA, 2021.
49. Emerson. *iOps Workspace Solution*; Emerson Electric: Saint Louis, MO, USA, 2023.
50. JC. *OpenBlue*; Johnson Controls: Milwaukee, WI, USA, 2023.
51. Musulin, K. *Cisco Explains Its Smart City Software Exit*; Smart Cities Dive: Washington, DC, USA, 2021.
52. Fadli, M.; Sumitra, I.D. A Study of Application and Framework Smart City in Bandung: A Survey. *Iop Conf. Ser. Mater. Sci. Eng.* **2019**, *662*, 022083. [CrossRef]
53. Pereira, G.V.; Testa, M.G.; Macadar, M.A.; Parycek, P.; de Azambuja, L.S. Building Understanding of Municipal Operations Centers as Smart City' Initiatives: Insights from a Cross-Case Analysis. In Proceedings of the International Conference on Electronic Governance and Open Society: Challenges in Eurasia, EGOSE '16, St. Petersburg, Russia, 4–6 September 2017; Association for Computing Machinery: New York, NY, USA, 2016; pp. 19–30. [CrossRef]
54. Pashchenko, A.F. Smart Management for Smart Cities—Synchronized Solutions. *IFAC-PapersOnLine* **2021**, *54*, 732–737. [CrossRef]
55. Selçuk, A.A. A guide for systematic reviews: PRISMA. *Turk. Arch. Otorhinolaryngol.* **2019**, *57*, 57. [CrossRef]
56. Ballew, B.S. Elsevier's Scopus® database. *J. Electron. Resour. Med. Libr.* **2009**, *6*, 245–252. [CrossRef]
57. Van Eck, N.; Waltman, L. Software survey: VOSviewer, a computer program for bibliometric mapping. *Scientometrics* **2010**, *84*, 523–538. [CrossRef] [PubMed]
58. van Eck, N.J.; Waltman, L. Text mining and visualization using VOSviewer. *arXiv* **2011**, arXiv:cs.DL/1109.2058.
59. Bibri, S.E.; Krogstie, J. The emerging data–driven Smart City and its innovative applied solutions for sustainability: The cases of London and Barcelona . *Energy Inform.* **2020**, *3*, 5. [CrossRef]
60. Bernardes, M.B.; de Souza, R.M.S.; de Andrade, F.P.; Novais, P. The Rio de Janeiro, Brazil, Experience Using Digital Initiatives for the Co-production of the Public Good: The Case of the Operations Centre. In *Recent Advances in Information Systems and Technologies*; Rocha, Á., Correia, A.M., Adeli, H., Reis, L.P., Costanzo, S., Eds.; Springer International Publishing: Cham, Switzerland, 2017; pp. 18–27.
61. Jacobs, P.; Arnab, A.; Irwin, B. Classification of security operation centers. In Proceedings of the 2013 Information Security for South Africa, Washington, DC, USA, 14–16 October 2013; pp. 1–7.
62. Bouleft, Y.; Elhilali Alaoui, A. Dynamic Multi-Compartment Vehicle Routing Problem for Smart Waste Collection. *Appl. Syst. Innov.* **2023**, *6*, 30. [CrossRef]
63. Beg, A.; Qureshi, A.R.; Sheltami, T.; Yasar, A. UAV-enabled intelligent traffic policing and emergency response handling system for the smart city. *Pers. Ubiquitous Comput.* **2021**, *25*, 33–50. [CrossRef]
64. Bellini, E.; Bellini, A.; Pirri, F.; Coconea, L. Towards a Trusted Virtual Smart Cities Operation Center Using the Blockchain Mirror Model. In Proceedings of the Internet Science, Perpignan, France, 2–5 December 2019; El Yacoubi, S., Bagnoli, F., Pacini, G., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 283–291.
65. Baliga, A.; Solanki, N.; Verekar, S.; Pednekar, A.; Kamat, P.; Chatterjee, S. Performance Characterization of Hyperledger Fabric. In Proceedings of the 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), Zug, Switzerland, 20–22 June 2018; pp. 65–74. [CrossRef]

66. Guo, B.; Yu, Z.; Zhou, X.; Zhang, D. From participatory sensing to Mobile Crowd Sensing. In Proceedings of the 2014 IEEE International Conference on Pervasive Computing and Communication Workshops (PERCOM WORKSHOPS), Budapest, Hungary, 24–28 March 2014; pp. 593–598. [CrossRef]
67. Atat, R.; Liu, L.; Wu, J.; Li, G.; Ye, C.; Yang, Y. Big Data Meet Cyber-Physical Systems: A Panoramic Survey. *IEEE Access* **2018**, *6*, 73603–73636. [CrossRef]
68. Dragoicea, M.; Patrascu, M.; Serea, G.A. Real time agent based simulation for smart city emergency protocols. In Proceedings of the 2014 18th International Conference on System Theory, Control and Computing (ICSTCC), Sinaia, Romania, 17–19 October 2014; pp. 187–192. [CrossRef]
69. Pătraşcu, M.; Drăgoicea, M. Integrating Agents and Services for Control and Monitoring: Managing Emergencies in Smart Buildings. In *Service Orientation in Holonic and Multi-Agent Manufacturing and Robotics*; Springer International Publishing: Cham, Switzerland, 2014; pp. 209–224. [CrossRef]
70. Swiatek, D.; Pokorny, M.S.; Tatto, J.A.; Melo, V.; Dias, E. Traffic management solutions in large cities-the integrated centre of urban mobility (CIMU) in São Paulo. In Proceedings of the 18th International Conference on Systems, London, UK, 13–14 May 2014.
71. Xu, Z.; Luo, M.; Vijayakumar, P.; Peng, C.; Wang, L. Efficient certificateless designated verifier proxy signature scheme using UAV network for sustainable smart city. *Sustain. Cities Soc.* **2022**, *80*, 103771. [CrossRef]
72. Subramanian, K. Introducing the Splunk Platform. In *Practical Splunk Search Processing Language: A Guide for Mastering SPL Commands for Maximum Efficiency and Outcome*; Apress: Berkeley, CA, USA, 2020; pp. 1–38.
73. Al Kindhi, B.; Pramudijanto, J.; Pratama, I.S.; Rahayu, L.P.; Adhim, F.I.; Susila, J. Solar Cell Based Integrated Sensor System Monitoring on Smart IoT. In Proceedings of the 2021 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT), Virtual, 17–18 July 2021; pp. 213–218. [CrossRef]
74. Neirotti, P.; De Marco, A.; Cagliano, A.C.; Mangano, G.; Scorrano, F. Current trends in Smart City initiatives: Some stylised facts. *Cities* **2014**, *38*, 25–36. [CrossRef]
75. MoHUA. Maturity Assessment Framework and Toolkit to unlock the potential of Integrated Command and Control Centers (ICCCs). *Minist. Hous. Urban Aff.* **2018**, *1*, 25–36.
76. Khan, N. *The 5 Layers of Software—What You Need to Know*; Arden: New York, NY, USA, 2022. Available online: https://www.ardentisys.com/the-5-layers-of-software-what-you-need-to-know/ (accessed on 8 July 2023).
77. Lee, D.; Cha, G.; Park, S. A study on data visualization of embedded sensors for building energy monitoring using BIM. *Int. J. Precis. Eng. Manuf.* **2016**, *17*, 807–814. [CrossRef]
78. Jung, D.k.; Lee, D.; Park, S. Energy operation management for Smart city using 3D building energy information modeling. *Int. J. Precis. Eng. Manuf.* **2014**, *15*, 1717–1724. [CrossRef]
79. Gelenbe, E.; Caseau, Y. The Impact of Information Technology on Energy Consumption and Carbon Emissions. *Ubiquity* **2015**, *2015*, 2755977. [CrossRef]
80. Aliyu, F.; Abdeen, M.A.; Sheltami, T.; Alfraidi, T.; Ahmed, M.H. Fog computing-assisted path planning for smart shopping. *Multimed. Tools Appl.* **2023**, 1–26. [CrossRef] [PubMed]
81. Akbar, M.A.; Azhar, T.N. Concept of Cost Efficient Smart CCTV Network for Cities in Developing Country. In Proceedings of the 2018 International Conference on ICT for Smart Society (ICISS), Semarang, Indonesia, 10–11 October 2018; pp. 1–4. [CrossRef]
82. AVEVA. *Unified Operations Center*; AVEVA: Cambridge, UK, 2023. Available online: https://www.aveva.com/en/solutions/operations/unified-operations-center/ (accessed on 8 June 2023).
83. Meijer, A.; Bolívar, M.P.R. Governing the smart city: A review of the literature on smart urban governance. *Int. Rev. Adm. Sci.* **2016**, *82*, 392–408. [CrossRef]
84. Ae Chun, S.; Luna-Reyes, L.F.; Sandoval-Almazán, R. Collaborative e-government. *Transform. Gov. People Process. Policy* **2012**, *6*, 5–12. [CrossRef]
85. Pereira, G.V.; Macadar, M.A.; Luciano, E.M.; Testa, M.G. Delivering public value through open government data initiatives in a Smart City context. *Inf. Syst. Front.* **2017**, *19*, 213–229. [CrossRef]
86. Kendra, J.M.; Wachtendorf, T. Elements of Resilience After the World Trade Center Disaster: Reconstituting New York City's Emergency Operations Centre. *Disasters* **2003**, *27*, 37–53. [CrossRef]
87. Kapucu, N.; Yuldashev, F.; Feldheim, M.A. Nonprofit Organizations in Disaster Response and Management: A Network Analysis. *J. Econ. Financ. Anal.* **2018**, *2*, 69–98.
88. Clement, J.; Manjon, M.; Crutzen, N. Factors for collaboration amongst smart city stakeholders: A local government perspective. *Gov. Inf. Q.* **2022**, *39*, 101746. [CrossRef]
89. Kapucu, N. Public-Nonprofit Partnerships for Collective Action in Dynamic Contexts of Emergencies. *Public Adm.* **2006**, *84*, 205–220. [CrossRef]
90. Raju, E.; Van Niekerk, D. Intra-governmental coordination for sustainable disaster recovery: A case-study of the Eden District Municipality, South Africa. *Int. J. Disaster Risk Reduct.* **2013**, *4*, 92–99. [CrossRef]
91. Roy, T.; Dey, S. Secure Traffic Networks in Smart Cities: Analysis and Design of Cyber-Attack Detection Algorithms. In Proceedings of the 2020 American Control Conference (ACC), Denver, CO, USA, 1–3 July 2020; pp. 4102–4107. [CrossRef]
92. Knerler, K.; Parker, I.; Zimmerman, C. *11 Strategies of a World-Class Cybersecurity Operations Center*; MITRE: McLean, VA, USA, 2022.

93. Li, W.; Fan, L.; Lei, W.; Li, D. Dynamic Password Authentication Method Based on Vehicle Command and Dispatch System. In Proceedings of the 2020 International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS), Vientiane, Laos, 11–12 January 2020; pp. 28–32. [CrossRef]
94. Mohammad, N. A Multi-Tiered Defense Model for the Security Analysis of Critical Facilities in Smart Cities. *IEEE Access* **2019**, *7*, 152585–152598. [CrossRef]
95. Valancius, V.; Laoutaris, N.; Massoulié, L.; Diot, C.; Rodriguez, P. Greening the Internet with Nano Data Centers. In Proceedings of the 5th International Conference on Emerging Networking Experiments and Technologies, CoNEXT '09, Rome, Italy, 1–4 December 2009; Association for Computing Machinery: New York, NY, USA, 2009; pp. 37–48. [CrossRef]
96. Peng, X.; Bhattacharya, T.; Cao, T.; Mao, J.; Tekreeti, T.; Qin, X. Exploiting Renewable Energy and UPS Systems to Reduce Power Consumption in Data Centers. *Big Data Res.* **2022**, *27*, 100306. [CrossRef]
97. Javed, M.A.; Nafi, N.S.; Basheer, S.; Aysha Bivi, M.; Bashir, A.K. Fog-Assisted Cooperative Protocol for Traffic Message Transmission in Vehicular Networks. *IEEE Access* **2019**, *7*, 166148–166156. [CrossRef]
98. Gouidis, F.; Flouris, G.; Plexousakis, D. A Demo for Smart City Operation Center. In Proceedings of the Challenge+ DC@ RuleML, Prague, Czech Republic, 18–20 August 2014. Available online: https://ceur-ws.org/Vol-1211/paper13.pdf (accessed on 8 July 2023).
99. Li, D.; Cao, J.; Yao, Y. Big data in smart cities. *Sci. China Inf. Sci.* **2015**, *58*, 1–12. [CrossRef]
100. Jew, A. Data Center Telecommunications Cabling. In *Data Center Handbook*; John Wiley & Sons, Ltd.: Hoboken, NJ, USA, 2014; Chapter 14, pp. 257–258. [CrossRef]
101. Shao, X.; Zhang, Z.; Song, P.; Feng, Y.; Wang, X. A review of energy efficiency evaluation metrics for data centers. *Energy Build.* **2022**, *271*, 112308. [CrossRef]
102. Sovacool, B.K.; Upham, P.; Monyei, C.G. The "whole systems" energy sustainability of digitalization: Humanizing the community risks and benefits of Nordic datacenter development. *Energy Res. Soc. Sci.* **2022**, *88*, 102493. [CrossRef]
103. Wu, J.; Guo, S.; Li, J.; Zeng, D. Big data meet green challenges: Big data toward green applications. *IEEE Syst. J.* **2016**, *10*, 888–900. [CrossRef]
104. Siddik, M.A.B.; Shehabi, A.; Marston, L. The environmental footprint of data centers in the United States. *Environ. Res. Lett.* **2021**, *16*, 064017. [CrossRef]
105. Nikolić, D.; Drajić, D.; Čiča, Z. Multifunctional Radars as Primary Sensors in IoT Based Safe City Solutions. In Proceedings of the 2021 15th International Conference on Advanced Technologies, Systems and Services in Telecommunications (TELSIKS), Nis, Serbia, 20–22 October 2021; pp. 273–278.
106. Wiig, A.; Wyly, E. Introduction: Thinking through the politics of the smart city. *Urban Geogr.* **2016**, *37*, 485–493. [CrossRef]