Digital twins, the software solution for safer cities

George SUCIU,
Beia Consult International, Bucharest, Romania
george@beia.ro

Cosmina STALIDI,
Beia Consult International, Bucharest, Romania
cosmina.stalidi@beia.ro

Abstract
Objectives: The S4ALLCities project's main goals are to build an open platform for information exchange and management, as well as to provide real-time situational awareness and decision support, thereby increasing the resilience of European cities while respecting citizens' fundamental right to privacy. Prior work: The project seeks to optimize smart cities through modular subsystems known as digital twins, each of which contributes to the overall goal in a unique way. These digital twins excel at real-time digital representation and machine learning of processes and objects encountered in a variety of open public spaces. Approach: These digital twins aid in the detection of potential hazards in urban public spaces. They will be validated for three months in three European cities: Trikala, Bilbao and Pilsen.They will monitor infrastructure in the city, such as traffic and access to restricted areas, as well as detect potential explosions, cyber attacks, and suspicious activity.Results:The demonstration events will demonstrate the effectiveness of the smart monitoring system by taking key measurements of city infrastructure (such as traffic, access to restricted areas, and evacuation routes), detecting explosives, cyber-attacks, and suspicious activity.Implications: S4ALLCities will be validated in three European cities over the course of three months, where it will be installed and tested. Its advantages will be demonstrated to stakeholders through a series of scenarios involving physical and cyber attacks on soft targets in the aforementioned smart cities. Public space, which is currently vulnerable to attacks of all kinds, could be a soft target. Value:By using innovative digital twin technologies, possible dangers to public safety are prevented.

Keywords: S4ALLCITIES; security; smart city.

1. Introduction
The advancements in IoT, big data analytics, and machine learning have made the concept of a smart city a reality. As we all know, the goal of a smart city is to provide efficient answers to its residents by utilizing modern technology and data analytics collected by sensors. The concept of a smart city was something SF for many people in the twentieth century, and it was only portrayed in popular media. Cities are becoming smarter not only in terms of automating routine operations for individual people, buildings, and traffic systems, but also in terms of monitoring, comprehending, analyzing, and designing the city in real-time to increase efficiency, equity, and quality of life for its inhabitants. organizations to keep up with newly emerging vulnerabilities and threats, given the dynamics of the domain. A smart city is more than just using digital technology to increase resource efficiency and reduce pollution. Improved urban transportation networks, updated water and waste disposal facilities, and more energy-efficient lighting and heating systems are all part of the plan. It also includes more involved and responsive local government, safer public spaces, and addressing the needs of the elderly. In this paper, we will look at what a smart city is today, how it has evolved in recent years, the domains where it is used (for example, traffic management, healthcare, and public safety), and the global future of smart cities.

The concept of "smart cities" has received a lot of attention in the context of urban development policy (Schaffers, et al. 2011). Smart cities are technologically advanced metropolitan areas with a high degree of connectivity between people and organizations. All of the components work together to form an integrated system that provides real-time access to high-quality services and goods while remaining economically and socially sustainable. This strategy includes the use of information and communication technologies (ICTs) to boost economic growth and improve quality of life, as well as the integration of all hardware and software technologies to improve urban administration (Kitchin 2015). According to the definition of "smart city," this new city "frequently links together technical informational transformations with economic, political, and socio-cultural development." (2018, Voda and Radu)

Smart cities begin with smart human capital because only smart people can develop ICTs with AI (Figure no. 1).

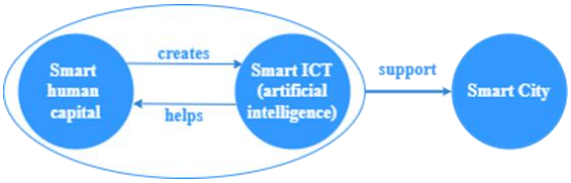

Fig. 1. How are Smart Cities built

Source: Kitchin, Rob. 2015. "Making sense of smart cities: addressing present shortcomings." Cambridge Journal of Regions, Economy and Society 8: 131-136.

A. IoT technology – an important actor in the smart cities development

The majority of cities are looking for intelligent solutions to improve their operations. This term refers to the combination of innovative ideas that include general improvements to existing technologies, all of which typically borrow the same principles from one another. All innovative ideas borrow technologies related to IoT, cybersecurity, and ICT.

ICT advancements must improve management and environmental operations. As a result of the rapid pace of change, smart city problems are becoming increasingly difficult. This results in constantly updated technologies, which cause organizational changes. These can be enhanced by collecting personal information about people through mobile applications and social networks [1].

According to the UK's Department for Business, Innovation, and Skills, the global market for smart city solutions is expected to reach $408 billion in 2020, accounting for approximately 24% of the global market. The actual amount reached in 2020 was $410.8 billion, with a projected increase to $820.7 billion by 2025 [2], [3]. The interest of authorities in platform manufacturers over smart solutions is a significant factor driving the global growth of the smart city market. The platform is used by the vast majority of shareholders.

The Internet of Things is a rapidly evolving paradigm that allows electronic devices to communicate with one another over the internet. The Internet of Things aims to make

people's lives easier by providing innovative solutions to various challenges or problems in government, public, or business situations. In fact, they are a hybrid of various smart devices, sensors, and frameworks, with the added benefit of providing storage space and high processing speed.

The Internet of Things (IoT) is at the heart of the European Spaces Safety and Security for All Cities (S4ALLCities) project, which aims to implement and assess cyber and physical security threat levels in smart cities through digitally augmented situational awareness. It is under constant development and will focus on risk-based systems for security management, detection of suspicious activities, identification of illegal objects, and real-time estimation of physical or cybernetic attacks from multiple locations, as well as crisis management countermeasures. S4ALLCities will also play an important role in promoting European city security.

2. IoT platform State of the Art

This section's goal is to provide preliminary information needed to design an IoT platform. The information on IoT platforms is provided at a higher level of abstraction and from a broader perspective. The information presented here is primarily derived from academic literature. The terms IoT platform, IoT framework, and IoT middleware are used interchangeably in this section. Concerning the architectural specifications, it can be mentioned:

1. Interoperability: A middleware can interact with disparate devices/technologies/applications without requiring additional effort from the application or service developer. Heterogeneous components must be able to exchange data and services. Interoperability in middleware can be viewed from three perspectives: network, syntactic, and semantic, all of which must be provided for IoT.
2. Service-based: A middleware architecture may be service-based to provide greater flexibility when adding new and advanced functions to an IoT's middleware.
3. Context-awareness: Context-awareness is an important requirement for developing adaptive systems and determining value from sensed data. The IoT middleware architecture must be aware of the context of users, devices, and the environment in order to provide effective and essential services to users.
4. Adaptive: Middleware must be adaptable in order to evolve in response to changes in its environment or circumstances. The network and its environment are likely to change frequently in the IoT.
5. Abstraction in Programming: An API for application developers is a necessary functional requirement for any middleware. High-level programming interfaces must be used by the application or service developer to isolate the applications or services from the operations provided by the underlying, heterogeneous IoT infrastructures. When creating an API, the level of abstraction, programming paradigm, and interface type must all be considered. The level of abstraction describes how the application developer sees the system (individual node/device level, system-level). The programming paradigm (for example, Publish/Subscribe) is concerned with the model for creating or programming applications or services. The style of the programming interface is defined by the interface type.

6. Distributed: The applications/devices/users of a large-scale IoT system (e.g., WSNs, VANETs) exchange information and collaborate.
7. Autonomous: To be autonomous means to be self-governing. Devices/technologies/applications are functional participants in IoT processes, and they should be able to interact and communicate with one another without requiring direct human intervention.

3. Architectural requirements - related difficulties

1. Service-based: The majority of middleware is service-based. Each service must include a description of service composition or discovery. To ensure semantic and syntactic interoperability, a standard service description is required.
2. Interoperability: While most existing middleware supports network interoperability, many lack semantic and syntactic interoperability. Because of heterogeneity and a lack of standards in ontologies, semantic interoperability in IoT is extremely difficult. The service-oriented approach provides the best support for semantic interoperability among all middleware categories. Support for syntactic interoperability, on the other hand, is limited.
3. Programming Abstraction: The majority of middleware supports programming abstraction. The new languages and tools that must be adopted, on the other hand, have a steep learning curve for both developers and users.
4. Context-awareness and autonomous behavior: Various types of middleware have taken advantage of some level of context-awareness. For example, MUSIC regulates context for self-adaptation in order to maintain a satisfactory QoS. Popular context applications (for example, context-aware resource)
5. Adaptive: In many approaches, adaptation decision-making is hard coded and must be recompiled and re-deployed. Adaptation is more dynamic; policies, rules, or QoS definitions are used, and these can be changed during runtime to produce new behavior. Despite the fact that most middleware is dynamic, the rules, policies, and QoS definitions are mostly hard-coded and not context-aware. This approach is not scalable in IoT.

A. Fundamental IoT-SYSTEM concepts

Figure 2 depicts the overall system architecture and problem setup for our approach. We concentrate on the analysis of potential technologies and IoT platforms for the realization of an Industrial IoT-platform (IIoT-platform, shown in light green in the above figure), which is a critical component for enabling communication between different subsystems, devices, and machines, as well as inter-communication at various levels.

Additionally, the primary communication technology, i.e., the lower physical communication layer, is considered, which allows the actual physical signal and data transfer between system components.

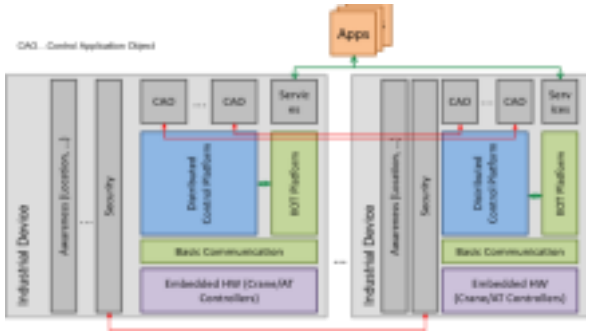

Fig. 2. System architecture and key system components

B. IoT systems and protocols stack

The IoT protocol stack was created to simplify and facilitate the development of complex networked systems, with the goal of achieving widespread adoption of IoT systems. Figure 2 depicts and compares the various layers of the IoT stack to the international standard ISO-OSI-model and the consolidated Internet protocol stack (TCP/IP).

The main feature of this stack, as shown in figure 3, is its simplicity. In contrast to the ISO-OSI-model, it has only four distinct layers.

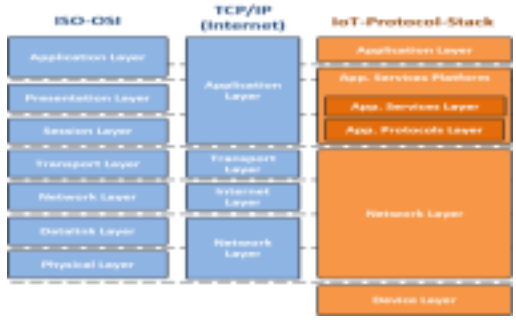

Fig. 3. Representation of the IoT protocol stack and comparison with the ISO-OSI and consolidated TPC/IP (Internet) models.

4. S4ALLCITIES Project

A. The architecture of the system

The S4ALLCities project aims to address smart city optimization through modular subsystems known as digital twins, each of which contributes to the goal in a complementary way. These digital twins are experts in real-time digital representation and machine learning of processes and objects encountered in various open public spaces. (Fig. 2)

The Digital Twins are as follows:

- The Internet of Things (IoT) Distributed Edge Computing (DECIoT) provides intelligent edge processing of measurements and sensor observations.
- MAIDS stands for Malicious Actions Information Detection Systems, and it is in charge of machine detection and intelligent detection of suspicious behavior.

- ACMS (Augmented Context Management System) is in charge of information within a common operational picture and augmented reality.

Thus, when digital twins are used in conjunction, they achieve high levels of awareness of potential risk situations in public spaces.

Fig. 4. Digital twins
Source: https://www.s4allcities.eu/press-release-01

The main goals of the S4ALLCities project are:

- to create an open platform for information exchange and management, as well as to provide real-time situational awareness and decision support, thereby increasing the resilience of European cities while respecting citizens' fundamental right to privacy;
- to design and develop an intelligent architecture for communication and interconnection of smart systems via IoT.
- completing smart city monitoring systems in order to improve preparedness and responsiveness in the event of a physical or cyber attack

S4ALLCities will be validated in three European cities: Trikala (GR), Bilbao (ES), and Pilsen (CZ), where it will be installed and tested for three months. Its benefits will be presented to stakeholders through various scenarios involving physical and cyber attacks on soft targets in the aforementioned smart cities. A soft target could be public space, which is currently vulnerable to attacks of all kinds. The demonstration events will demonstrate the effectiveness of the smart monitoring system by taking key measurements of city infrastructure (such as traffic, access to restricted areas, and evacuation routes), detecting explosives, cyber-attacks, and suspicious activity, and detecting explosives, cyber-attacks, and suspicious activity.

The Trikala pilot scenario will concentrate on two key soft targets: autonomous bus transportation and the park of Trikala municipal buildings.

These two scenarios will show how Digital Twins technology will handle crowd protection in public spaces or autonomous bus transportation infrastructure.

The Bilbao scenario will be based on detecting suspicious behavior, explosives, and directing people to a safe location. This scenario is based on the events of the 2017 Cambrils terrorist attack, in which members of a terrorist organization attacked several pedestrians on the street. On the same day, 100 kilometers away, another member drove a van into a crowd, killing 14 people and injuring many more. These dreadful scenarios can be avoided and avoided if detection systems are put in place.

The Malicious Actions Information Detection Systems will detect anomalies and illicit behaviors of various individuals or groups of people in various crowded places in a high risk area. The Augmented Context Management System will detect explosives and suspected armed attackers using augmented reality technology. Furthermore, the early detection and protection of cyber-attacks will be tested, with the goal of avoiding the loss of control over the scenario's information and systems.

The Pilsen demonstration will call for the evacuation of the football stadium. It can hold up to 15000 people, and with the surrounding area, which includes a pedestrian zone, park, and bus terminal, the number can be much higher.

The scenario focuses on crisis management at the stadium in the event of a terrorist attack or a toxic ammonia gas leak from a nearby brewery. Its main purpose is to safely evacuate people from the stadium and its surrounding areas.

Another data collection method that will be expanded in the S4ALLCities project is the use of fiber optic networks for communications, which are already prevalent in many urban areas.

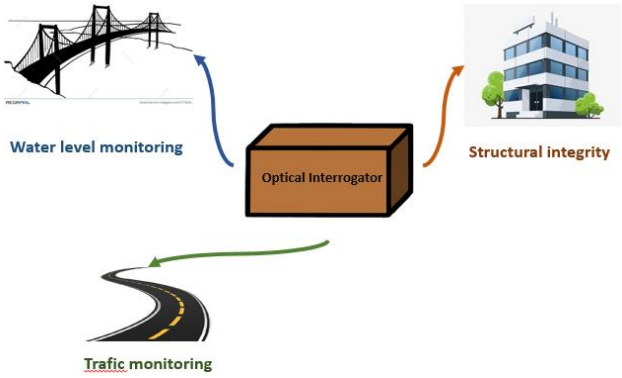

Fig. 5. Data collection using FBG

These can be used to transmit various low-data optical signals from various deployed sensors in critical infrastructure locations. Fibre Bragg Grating (FBG) sensors will be used, which have high accuracy at a low cost. (Fig. 5)

This System of Systems aims to achieve TRL-7 by the end of the project, demonstrating the S4ALLCities functionality to the appropriate end-users and stakeholders.

5. Conclusions

At the end of this paper, Smart Cities face challenges due to far too rapid change. The S4ALLCITIES project's solution optimizes solutions through modular systems, also known as digital twins. These digital twins aid in identifying potential risks in urban public spaces. They will be validated in three European cities for three months: Trikala (GR), Bilbao (ES), and Pilsen (PL) (CZ). They will measure the city's infrastructure, such as traffic and access to restricted areas, as well as detect potential explosions, cyber attacks, and suspicious activity.

Acknowledgements

This paper was partially supported by UEFISCDI Romania and MCI through Eureka ITEA projects PARFAIT and SOLOMON, and funded in part by European Union's Horizon 2020 research and innovation program under grant agreements No. 872698 (HUBCAP) and No. 883522 (S4AllCities).

References

[1] A. Essa et al. (2018), Cyber physical sensors system security: threats, vulnerabilities, and solutions, in IEEE ICSGSC, pp. 62–67

[2] S.A. Timashev (2019), Cyber reliability, resilience, and safety of physical infrastructures, in IOP Conference Series: Materials Science and Engineering, vol. 481, p. 012009

[3] C. Konstantinou et al. (2015), Cyber-physical systems: a security perspective, in IEEE ETS, pp. 1–8

Kirimtat, A., Krejcar, O., Kertesz, A., & Tasgetiren, M. F. (2020), Future trends and current state of smart city concepts: A survey, Pages 1-2 IEEE Access, 8, 86448-86467.

[4] Degree of urbanization (percentage of urban population in total population) by continent in 2020 https://www.statista.com/statistics/270860/urbanization-by-continent/

Andrés Camero, Enrique Alba (2019), Smart City and information technology: A review, Volume 93, , Pages 84-94, ISSN 0264-2751

Kumar, S., Tiwari, P. & Zymbler (2019), M. Internet of Things is a revolutionary approach for future technology enhancement: a review, J Big Data 6, 111. https://doi.org/10.1186/s40537-019-0268-2

A. Essa et al. (2018), Cyber physical sensors system security: threats, vulnerabilities, and solutions, in IEEE ICSGSC, pp. 62–67

S.A. Timashev (2019), Cyber reliability, resilience, and safety of physical infrastructures, in IOP Conference Series: Materials Science and Engineering, vol. 481, p. 012009

C. Konstantinou et al. (2015), Cyber-physical systems: a security perspective, in IEEE ETS, pp. 1–8

Huertas, Assumpció, and Andrea Oliveira (2019), "How tourism deals with terrorism from a public relations perspective: A content analysis of communication by destination management organizations in the aftermath of the 2017 terrorist attacks in Catalonia." Catalan Journal of Communication & Cultural Studies 11.1: 39-58.

Kumar, Sachin & Tiwari, Prayag & Zymbler, Mikhail (2019), Internet of Things is a revolutionary approach for future technology enhancement: a review, Journal of Big Data. 6. 10.1186/s40537-019-0268-2.

M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke (2016), "Middleware for Internet of Things: A survey". IEEE Internet of Things Journal, 3(1), 70-95.

H. Derhamy, J. Eliasson, J. Delsing, and P. Priller, "A survey of commercial frameworks for the internet of things". In IEEE International Conference on Emerging Technologies and Factory Automation: 08/09/2015-11/09/2015.

L. Da Xu, W. He,and S. Li (2014), "Internet of things in industries: A survey", IEEE Transactions on industrial informatics, 10(4), 2233-2243. [4] R. Rouvoy, P. Barone, Y. Ding, F. Eliassen, S. Hallsteinsen,J. Lorenzo, and U. Scholz (2009), "Middleware support for self-adaptation in ubiquitous and service-oriented

environments" In Software engineering for self adaptive systems (pp. 164-182). Springer, Berlin, Heidelberg.
Angelidou, Margarita (2015), "Smart cities: A conjuncture of four forces." (Cities 47): 95-106.
Bhattacharya, Sweta, Siva Rama Krishnan Somayaji, Thippa Reddy Gadekallu, Mamoun Alazab, and Praveen Kumar Reddy Maddikunta (2020), "A review on deep learning for future smart cities." *Internet Technology Letters*,.
Bhushan, Bharat, Aditya Khamparia, K. Martin Sagayam, Sudhir Kumar Sharma, Mohd Abdul Ahad, and Narayan C. Debnath (2020), "Blockchain for smart cities: A review of architectures, integration trends and future research directions." *Sustainable Cities and Society* 61: 102360.