International Journal of Architectural, Civil and Construction Sciences
ISSN: 2415-1734
Vol:15, No:8, 2021

Cybersecurity for Digital Twins in the Built Environment: Research Landscape, Industry Attitudes and Future Direction

Kaznah Alshammari, Thomas Beach, Yacine Rezgui

***Abstract*—**Technological advances in the construction sector are helping to make smart cities a reality by means of Cyber-Physical Systems (CPS). CPS integrate information and the physical world through the use of Information Communication Technologies (ICT). An increasingly common goal in the built environment is to integrate Building Information Models (BIM) with Internet of Things (IoT) and sensor technologies using CPS. Future advances could see the adoption of digital twins, creating new opportunities for CPS using monitoring, simulation and optimisation technologies. However, researchers often fail to fully consider the security implications. To date, it is not widely possible to assimilate BIM data and cybersecurity concepts and, therefore, security has thus far been overlooked. This paper reviews the empirical literature concerning IoT applications in the built environment and discusses real-world applications of the IoT intended to enhance construction practices, people's lives and bolster cybersecurity. Specifically, this research addresses two research questions: (a) How suitable are the current IoT and CPS security stacks to address the cybersecurity threats facing digital twins in the context of smart buildings and districts? and (b) What are the current obstacles to tackling cybersecurity threats to the built environment CPS? To answer these questions, this paper reviews the current state-of-the-art research concerning digital twins in the built environment, the IoT, BIM, urban cities and cybersecurity. The results of the findings of this study confirmed the importance of using digital twins in both IoT and BIM. Also, eight reference zones across Europe have gained special recognition for their contributions to the advancement of IoT science. Therefore, this paper evaluates the use of digital twins in CPS to arrive at recommendations for expanding BIM specifications to facilitate IoT compliance, bolster cybersecurity and integrate digital twin and city standards in the smart cities of the future.

***Keywords*—**BIM, cybersecurity, digital twins, IoT, urban cities

I. Introduction

THE construction sector is striving to produce buildings and cities that are smarter but this is only possible if advances in ICT continue to be made so that information can be exchanged ever-more seamlessly.

Examples of recent technological advances include wireless communications, continual connectivity, faster communication speeds and lower cost sensors. Technology is becoming omnipresent at a time when cyber systems are increasingly being incorporated into physical objects [1], widely referred to as the IoT. Use of this technology is accelerating due to a combination of better communication networks and cheaper technology [2], thereby enabling value to be derived from knowledge of the built environment. BIM is an information model used in architecture, engineering, construction and facilities management (AECFM) to enable information about the built environment to be digitalised.

Unfortunately, BIM relies on legacy formats and complex modelling paradigms which makes it unsuitable for application in the IoT. Therefore, little use of BIM has been made because alternative systems make use of extensible, lightweight data schemas in web-native languages. The need for building plans to meet various environmental, financial and societal needs has resulted in them becoming increasingly complicated [3]. Therefore, BIM offers the ability for a layered model to illustrate and methodically classify various aspects, focusing on how business services can be enhanced using ICT and knowledge [4] using a sensing layer, a means of communication and the capacity to store data. In addition, business, governance, application and innovation layers are incorporated.

Sensor networks are used to design CPS communication infrastructure [5] and digital twin technology offers CPSs alternative outcomes in terms of simulating, forecasting, monitoring and optimising the condition. Therefore, benefits can be derived from a virtual representation of a CPS to secure a system using continual feedback [6].

The potential benefits that can be derived from deploying digital twin and IoT technologies in the built environment are starting to be recognised and the result could be smart cities whereby ICT is used to enable information to be shared with the public. The benefits are apparent but there is a need to address the associated security threat [7] because it is not currently possible to assimilate BIM data and cyber security concepts and, therefore, security has thus far been overlooked. Thus, this paper aims to map the future development of the cybersecurity landscape of the built environment by generating a series of future research recommendations. This entails reviewing the latest technology in the fields of BIM, IoT, digital twins, smart cities and cybersecurity as well as surveying industry attitudes to cybersecurity in the built environment and the obstacles to the further development of this area.

In the remainder of this paper, Section II presents our methodology, Section III presents a review of the research concerning digital twins in the built environment and the IoT in information models through a previous literature review and, additionally, eight reference zones across Europe that

Kaznah Alshammari, Thomas Beach, and Yacine Rezgui are with School of Engineering, Cardiff University, Cardiff, UK (e-mail: Alshammarik1@cardiff.ac.uk, beachth@cardiff.ac.uk, rezguiy@cardiff.ac.uk).

have been influential in progressing research into the IoT are studied. Section IV presents our recommendations. Finally, Section V concludes the paper.

II. Methodology

To achieve the aim of this paper as described in Section I, two research questions will be answered:

- RQ1: How suitable are the current IoT and CPS security stacks to address the cybersecurity threats facing digital twins in the context of smart buildings and districts?
- RQ2: What are the current obstacles and blockers to tackling cybersecurity threats to the built environment CPSs?

To answer these research questions, the following methodology will be applied:

A detailed literature review of a CPS and the built environment developments will be conducted using a systematic search of academic databases (Google Scholar, Scopus, IEEE Xplore, ScienceDirect and Elsevier). Moreover, the literature review will consider the following topics: (a) BIM, (b) CPS, specifically focusing on the IoT related to built environment assets, (c) digital twins, (d) smart cities and (e) cybersecurity.

The previous two elements will be analysed to determine the obstacles encountered in providing increased cybersecurity for digital twins in the built environment. From these obstacles, a series of recommendations will be elicited for future research that will be required to provide the required cybersecurity levels for the evolving field of research into digital twins.

III. Literature Review

This section summarises the empirical research in the BIM, urban cities, IOT, digital twin and cybersecurity domains. This includes research of cybersecurity for digital twins in the built environment and improvements in the built environment.

A. Building Information Modelling

Those engaged in the architecture, engineering and construction (AEC) sector are required to collaborate closely and, consequently, there is a need for communication channels to be made more secure. The AEC sector uses exchange files to convey information [8]. The use of BIM data in the construction industry is well-established because it enables users to update when exchanging the files [9]. Use of BIM in the AECFM sector has effectively transformed step digitisation. Using Industry Foundation Classes (IFC), it is possible to create and manage BIM in the design and construction processes, thereby conferring benefits [3].

BIM utilises commercial software and the AEC sector uses BIM to produce 3D models and facilitate communication between contributors. BIM also offers data-containing tools [10] such as Microstation (Bentley), Revit (Autodesk) and Constructor (Vicosoft) [11]. Even when the construction process is complete, BIM can be used to continue sharing information over the lifetime of a building through to demolition. BIM offers an interface for operational execution data that present the fundamental role in facilitating operations and maintenance [12]. Crucially, however, security features are not supported by BIM and this prevents its application in smart build environments that require security from the outset. Rather, it can only be incorporated at a later date using a Building Automation System (BAS) [13].

The information that BIM makes available makes a valuable contribution to the commissioning process such as the timing of building performance evaluations of the adjusting of energy systems. The operation stage entails stakeholders engaging with the built environment with resulting economic activity [14]. The building process comprises four roles: strategy making, deal-making, controlling and task management. The 3D or 4D BIM models are employed in the operation stage for recovery purposes. The 4D BIM requires a construction schedule project and a 3D BIM [15] but BIM is not well suited for the operation stage; for instance, there are limitations with IFC in terms of recycling knowledge from other domains to bring about advanced reasoning [3].

B. CPS in the Built Environment

One way in which a CPS can be realised is to utilise the IoT. The IoT links the various elements of a building's construction lifecycle, amassing data along the way [16]. By incorporating BIM into the IoT, real-time construction data can be combined with the building design model so that designers can engage in real-time to address any issues that arise. Combining the IoT with mobile devices, sensors and software provides remote insight into smart construction sites. As such, it is the effective combination of the digital and physical worlds that gives building sites interoperability and interconnectivity [17].

It is the combination of BIM and the IoT that yields a 'digital twin' of a building based on the BIM platform. This twin can then be used to simulate the construction process, enhance performance and recognise the most influential factors. Synchronous simulations are possible by correlating the IoT data with the BIM model and using analytical tools. It is the combination of the BIM with real-time IoT data that represents the core of the enabling technology system and facilitates the production of smart construction processes [18]. Therefore, the IoT is fundamental to efforts associated with lean construction strategies. More specifically, the IoT helps determine the number of specialists needed, measure the data controlled, and identify the areas to be considered [19].

C. Urban Cities

Urban cities are a collection of buildings that utilise ICT to arrive at intelligent solutions that enhance the performance and quality of urban services such as energy and transportation [20]. Therefore, the current section provides details for eight innovative urban cities across Europe: Antwerp, Carouge, Eindhoven, Helsinki, Manchester, Milan, Porto and Santander. Each of these cities are utilising IoT ecosystems and open standards in accordance with the Open & Agile Smart Cities (OASC) standards. Moreover, each city has its own ideas for

developing the IoT with distinct technologies and functionalities that contribute to the smart city [20].

Antwerp's IoT innovations are channelled through its City of Things (CoT) [21] and the Antwerp City Platform as a Service Platform (ACPaaS) [22]. Meanwhile, Carouge intends to utilise the IoT in three architectures: monitoring street noise, facilitating smart parking [23], and a proprietary tourism application. Eindhoven's efforts entail supporting the organic development and interoperability of IoT stages and vertical systems using various sensors such as actuators and wireless communication. Helsinki operates Digitransit architecture with Helsinki CKAN and an O-MI (Open Message Interface) node [24]. Manchester has adopted a wider perspective regarding what is possible and the current projects include Triangulum H2020 and CityVerve [25]. Furthermore, Milan is pursuing three custom-developed main architectures: building/energy; parking; and weather/noise/pollution. Porto is also developing custom-made apps and services including a citizen platform, a water management platform, an environmental monitoring platform, and a mobility management platform [20]. Finally, Santander is pursuing numerous IoT projects such as CKAN Data Persistence, FIWARE Short Term Historic (Comet), FIWARE Context Broker (Orion), and FIWARE persistence connector (Cygnus).

Reference Zones are intended to improve privacy and security based on the FIWARE cloud platform and FIWARE secure. FIWARE offers innovative programming components via APIs that offer developers access to useful cloud platforms [26]. Antwerp has not incorporated a security privacy layer, albeit that the city's platforms contain tools with authorisation and authentication functions. Meanwhile, Carouge is currently in the process of exploring options for authorisation, authentication and accounting and it weighing up the merits of both FIWARE Secure Catalogue and FIWARE AAA. Mandat International and ODG have been charged with incorporating FIWARE into the IoT for Carouge [27]. Similarly, Eindhoven is exploring the possibility of using FIWARE for security purposes. Meanwhile, Helsinki is seemingly opting for open message interface (O-MI) security models based on the O-MI RESTful API and Manchester is using a combination of private sector companies and public sector IG specialists to provide privacy software tools. The CityVerve project has appointed British Telecommunications (BT) to implement Privacy Policy Manager (PPM). Milan uses OAuth2 protocol for its API Management System as well as an authorisation element. The possibility of incorporating FIWARE is also being evaluated to bolster security. Porto's approach is to rely on personal login details based on https and is considering using OAuth/OAuth2 for authentication and accounting. The Santander Reference Zone does not have an official layer usage for security but incorporates elements of Wilma PEP and FIWARE Keyrock IDM [20]. Therefore, whilst these cities are making progress with combining the IoT with sensors, there is still no effective, seamless cybersecurity model [20].

Industry 4.0 is the term for combining ICT and industrial technologies to process and communicate data to produce digital twins [29]. Originally developed by the aerospace sector [30], digital twins facilitate the continuity of information throughout the product lifecycle [31].

Digital technologies are now being incorporated into the built environment in ways that were previously unimaginable, thereby helping the management of facilities become 'smart'. For such purposes, BIM presents a value proposition provided it can be applied in conjunction with internet-based systems and learning capabilities [32]. Further innovations related to artificial intelligence (AI) and the IoT are producing new products that can be utilised in various real-world settings [33], [34].

Using BIM to process data using the IoT presents a cybersecurity threat [39]. A recent development is smart grid cybersecurity, offering the potential for secure communication, secure authentication and information security [40]. There are numerous standards associated with cybersecurity including Federal Information Processing Standard (FIPS) 201 and ISO 27002:2013, and Advanced Encryption Standard (AES) [41] but a need exists for appropriate hazard evaluations [40]. Utilising BIM for asset management purposes will further complicate security efforts. Asset management processes start from the moment that responsibility for the underlying assets is handed over by the project team to the owner. Crucially, the data in the BIM model are also transferred and it is envisaged that the model will evolve over time as the asset is used with data for maintenance being added to the existing design and construction data [38].

Standard specification IFC, COBie and BIM Level 2 models are unable to support the IoT's security features. Therefore, it is not possible to use these standard specification models during the building design process for smart environments if they need the IoT and suitable cybersecurity. Instead, this must be added at a later stage using a BAS. Any built environment utilising BIM will be devoid of the IoT and cybersecurity features [28]. This approach results in a technological base. BIM PAS 1192-5 of Level 2 Standard underlines that publishing building properties on a large-scale is an independent process and this is especially the case when coordinated with data distribution [42]. Reference [28] utilises a proof of concept (PoC) based on a smart building environment where there are two secure rooms but the details about how to access them must be kept secure from hackers. It may be best to retain any sensitive information and details of how to access it in an inaccessible place. As such, the technology base helps mitigate threats but these perils are not adequately addressed.

Efforts to enable BIM Level 2 to support the IoT and security overlooked the need to operate secure servers which are another element of the PAS 1192-5 of Level 2 Standard. The Handle System's global decentralised servers only provide access to the local system but any security vulnerabilities in application-specific servers could result in the BIM data being compromised. Moreover, the system could be susceptible to malware if it relies on external templates operating on systems with known security issues.

Consequently, it is necessary to protect these against infection but such steps are only required for BIM data and not for EBIS [28].

It is imperative that those charged with managing smart building projects and the utilisation of BIM have a thorough understanding of the current cybersecurity threats so that any risk to the underlying data is nullified. Otherwise, the security of the asset could be compromised through the loss of intellectual property or a breach of the systems related to the asset. To help address this issue, the UK government is developing a Publicly Available Specification (PAS) specifying the optimal approach to managing security for those engaged in BIM, developing built environments or managing smart assets [42].

D. Digital Twins

Digital twins afford promising opportunities in terms of simulating, monitoring, optimising and forecasting the condition of CPSs. In addition, they provide continual feedback to facilitate improvements [6]. Moreover, a replica of a CPS can help improve the system's security [43].

CPS issues require the ability to examine the relationship between physical and cyber elements [44]. It is the sensor network security that governs a CPS's security [45]. Most attempts to make sensor networks secure have focused on developing a secure communication infrastructure [5] with the results being algorithms for bootstrapping security associations and key management [46], secure routing protocols [47], and secure communication [48]. Meanwhile, the replication function represents data about physical objects. Possible sources of information regarding virtual objects could be sensor estimations, network communications and logs. The CPS twinning structure can be used to achieve a direct connection for sensors [43].

Many of the applications are critical to the system remaining safe and their failure could compromise the system but also adversely affect those who rely on it. For example, SCAD systems are used in various national infrastructures such as the supply of natural gas, wastewater treatment, and electricity grids and any issues in their control systems could jeopardise public safety and incur significant financial costs. In the past, efforts to improve CPS systems have overwhelmingly sought to enhance their reliability but now it is recognised that it is necessary to actively prevent cyberattacks [49]. Therefore, a role exists for digital twins to conduct determination utilising IDS. IDS has the potential to serve not only as a primary input for the purposes of analysis (host-based) but also for auditing traffic on the network (network-based) [50].

The potential for power application security to be used in conjunction with cyber infrastructure security to prevent cyberattacks has been explored by [44]. More specifically, they considered cybersecurity for smart grids which involves acquiring operational control functions needed to ensure stability beyond the physical power framework. Their work helped classify the power system's control loops which recognise control actions, communication signals, protocols, computations and devices. It is the sensors located in the field that feedback estimations to control centres. Algorithms in the control centre receive measurements and compute these to arrive at suitable decisions. Having made a decision, a command is issued to an actuator so that the devices in the field can be manipulated accordingly. Consequently, if a third party were to exploit a vulnerability in the system, attack templates could be made to cause delays, deny access or interfere with the content [51]. Therefore, continual monitoring of the power system is required to maintain its integrity. The related consequences could entail load being lost, the operating frequency of the system being violated, alterations to the voltage or various secondary effects. Undertaking attack studies offers one way in which countermeasures can be readied to help lessen any disruption or prevent an attack from being initiated. Such countermeasures could include the identification of bad data or the use of attach resistant control algorithms.

IV. Recommendations

Based on the literature and survey results, there are several key points that must be considered in the future when designing an information security layer for digital twins/CPSs in the built environment.

Extend the specifications of BIM to enable compliance with the IoT: Effectively combining BIM with the IoT would afford unparalleled operational and structural competences with data being streamed in real time from IoT sensors to facilitate various BIM-based applications [52], as described in Section III *A*.

Extend the standards for BIM to enable the necessary cybersecurity features: The shortcomings in terms of making BIM resilient to cyberattacks are evident. The main concepts are as follows:

PAS 1192-5 offers a security framework that enables a proportionate approach to tackling the known security vulnerabilities regarding asset data. The procedures set out by PAS 1192-5 help avoid the possibility of data divergence which could compromise a built asset's users, benefits or security [42]. By incorporating effective cybersecurity, it is possible to ensure that the measures taken are of a suitable standard [9], as described in Section III A.

Digital twin and future city confirm that the important make provision for cybersecurity and IoT considerations are as follows:

Integrating a security layer to devise a smart application architecture that affords security for HyperCat with traversal links for data open sources; certain systems will only provide access to authenticated users [3]. As a result, if resources can be discovered but are only available with authentication, users can be provided with authentication data where appropriate [35].

Smart grid security is of great importance owing to the industry's reliance on ICT that communicates information using the IoT [36]-[44]. In addition, digital twins offer potential CPS outcomes [43]. Given that a network of sensors is needed for the CPS, there is a clear need to ensure the

security of these sensors supported by encrypted algorithms such as 3DES and AES to guarantee that actors have the appropriate permissions and there is adequate security throughout the built environment [40], as described in Section III *D*.

Incorporating established standards for built environment data into cybersecurity concepts by means of a standardised cybersecurity layer for the built environment:

Incorporating the IoT with data for the built environment produces a digital twin of a building asset that can then be utilised for the purposes of simulating construction methods to enhance performance and recognise important factors including possible cybersecurity threats. The security of an asset could be compromised in the event that intellectual property is intercepted, or the asset's systems are penetrated [18], as described in Section III *C*.

Incorporating the IoT, digital twins and information models such as BIM in a cybersecurity layer designed specifically for built environment data requires a reference architecture to be devised. It should be possible for digital twins to identify and effectively protect their true twin. More specifically, the survey has determined specific requirements for this cybersecurity layer:

1. The cyber security layer must be configurable for the scenario in which it is deployed.
2. The built environment cyber security layer should be based, where possible, upon established standard APIs.
3. It must be able to deal with layered data with responsibilities split across multiple stakeholders.
4. Access must be definable across multiple organisations.

V. Conclusion

This paper has aimed to plan the future development of the cybersecurity landscape of the built environment by generating a series of future research recommendations. The current study has undertaken a systematic review of the research concerning digital twins in the built environment and the IoT in information models so as to confirm a suitable definition and the practical applications in real-world settings. The research has confirmed the value of using digital twins in physical objects such as the IoT as well as in information models such as BIM. Specific attention has been devoted to eight reference zones across Europe that have been influential in progressing research into the IoT. The empirical literature in combination with the underlying analysis helped to identify the knowledge gaps concerning the IoT, presenting several associated challenges.

Specifically, this research sought to address two research questions (defined in Section II). RQ1 and RQ2 have been answered (in Section III). The most pressing problem concerns the possibility of cyberattacks given the rapid expansion of the use of CPS in the built environment and this study has made a number of recommendations to further the advancement of cybersecurity in the built environment.

Acknowledgment

K.A. acknowledges the Northern Border University, Saudi Arabia for the assistance offered. However, the opinions and statements presented in this paper are purely those of the author and are not necessarily endorsed by the University.

References

[1] D. Miorandi, S. Sicari, F. De. Pellegrini, and I. Chlamtac, Ad Hoc Networks Internet of things: Vision, applications and research challenges, *Ad Hoc Networks*. Elsevier B.V., 10(7), pp. 1497–1516. doi: 10.1016/j.adhoc, Sep. 2012.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, Internet of Things (IoT): A vision, architectural elements, and future directions, *Future Generation Computer Systems*. Elsevier B.V., 29(7), pp. 1645–1660. doi: 10.1016/j.future, Sep. 2013.

[3] S. Howell, Y.Rezgui, Beyond BIM, 2018.

[4] D. H. Shin, Ubiquitous city: Urban technologies, urban infrastructure and urban informatics, 35(5), pp. 515–526. doi: 10.1177/0165551509100832, Oct 2009.

[5] A. A. Cardenas, S. Amin, and S. Sastry, 'Secure Control: Towards Survivable Cyber-Physical Systems ∗', pp. 495–500. doi: 10.1109/ICDCS.Workshops.2008.40, Jun. 2008

[6] S. C. Steinmetz, A. Rettberg, and F.G. Ribeiro, Internet of Things Ontology for Digital Twin in Cyber Physical Systems. doi:10.1109/SBESC.2018.00030, Nov.2018.

[7] A. El. Saddik, 'The Convergence of Multimedia Technologies', *IEEE MultiMedia*. IEEE, 25(June), pp. 87–92. doi: 10.1109/MMUL.2018.023121167, Aug. 2018.

[8] M. Das, J.C. Cheng, and S.S. Kumar, BIMCloud: A Distributed Cloud-based Scoial BIM Framework for Project Collaboration, *The 6th International ASCE Conference on Computing in Civil and Building Engineering*, pp. 41–48. doi: 10.1061/9780784413616.006, Dec. 2015.

[9] H. Boyes, Building Information Modelling (BIM): Addressing the Cyber Security Issues, *Iet*, pp. 1–12. doi: 10.1049/etr, Sep. 2014.

[10] Autodesk, Building Information Modeling for Sustainable Design, *Autodesk White Paper*, pp. 1–13, 2003.

[11] H.S. Cha, DG. Lee, A case study of time/cost analysis for aged-housing renovation using a pre-made BIM database structure, *KSCE Journal of Civil Engineering*, 19(4), pp. 841–852. doi: 10.1007/s12205-013-0617-1, May. 2015.

[12] A. GhaffarianHoseini, T. Zhang, O. Nwadigo, A. H. GhaffarianHoseini, N. Naismith, J. Tookey, and K. Raahemifar, Application of nD BIM Integrated Knowledge-based Building Management System (BIM-IKBMS) for inspecting post-construction energy efficiency, 72(February), pp. 935–949. doi: 10.1016/j.rser.2016.12.061, May. 2017.

[13] M. Jung, C. Reinisch, and W. Kastner, Integrating Building Automation Systems and IPv6 in the Internet of Things, *2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*. IEEE, pp. 683–688. doi: 10.1109/IMIS.2012.134, Jul. 2012.

[14] A. Bosch, L. Volker, and A. Koutamanis, A. 2015. BIM in the operations stage: bottlenecks and implications for owners, 5(3), pp. 331–343. doi: 10.1108/BEPAM-03-2014-0017, Jul. 2015.

[15] A. Romigh, J. Kim, and A. Sattineni, 4D Scheduling: A Visualization Tool for Construction Field Operations, pp. 395–404, 2017

[16] F. Tao, Y. Zuo, L. Da. Xu, and L. Zhang, IoT-Based Intelligent Perception and Access of Manufacturing Resource Toward Cloud, 10(2), pp. 1547–1557, Feb. 2014.

[17] K. Ding, H. Shi, J. Hui, Y. Liu, B. Zhu, F. Zhang, and W. Cao, Smart steel bridge construction enabled by BIM and Internet of Things in industry 4.0: A framework, *2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC)*. IEEE, pp. 1–5. doi: 10.1109/ICNSC.2018.8361339, Mar. 2018.

[18] F. Tao, Q. Qi, New IT Driven Service-Oriented Smart Manufacturing: Framework and Characteristics, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*. IEEE, 49(1), pp. 81–91. doi: 10.1109/TSMC.2017.2723764, Jul. 2017.

[19] A. Guerriero, S. Kubicki, F. Berroir, and C. Lemaire, BIM-enhanced Collaborative Smart Technologies for LEAN Construction Processes, pp. 1023–1030, Jun.2017.

[20] Synchronicity-iot.eu. Synchronicity, 2019. (Online) Available at: https://synchronicity-iot.eu/ (Accessed 6 Sep. 2019).

[21] Imec-int.com. imec - city of things, 2019. (Online) Available at:

https://www.imec-int.com/en/cityofthings (Accessed 6 Aug. 2019).
[22] Antwerpen.digipolis.be.Digipolis Antwerpen, 2019. (Online) Available at: https://antwerpen.digipolis.be/en/blog/2fac1bf7-eeee-432b-9a93-dad32bbb2002 (Accessed 6 Aug. 2019).
[23] IEM. IEM - Innovative parking solutions for smart cities: Parking meters, 2019. (Online) Available at: http://www.iemgroup.com/ (Accessed 16 Aug. 2019).
[24] Digitransit. Digitransit, 2019. (Online) Available at: https://digitransit.fi/en (Accessed 6 Aug. 2019).
[25] CityVerve. CityVerve Manchester | Manchester's Smart City Demonstrator, 2019. (Online) Available at: http://www.cityverve.org.uk (Accessed 6 Aug. 2019).
[26] M. Fazio, A. Celesti, F.G. Marquez,A. Glikson, M. Villari, Exploiting the FIWARE Cloud Platform to Develop a Remote Patient Monitoring System, pp. 264–270. doi: 10.1109/ISCC.2015.7405526, Jul. 2015.
[27] International, M. Mandat International, welcome centre NGO UN international conference information Geneva, 2019. (Online) Mandint.org. Available at: https://www.mandint.org/ (Accessed 6 Aug. 2019).
[28] P.T. Kirstein, A. Ruiz-Zafra, Use of Templates and The Handle for Large-Scale Provision of Security and IoT in the Built Environment, pp. 1–10, 2018.
[29] S. Haag, R. Anderl, Digital twin – Proof of concept. Society of Manufacturing Engineers (SME), 15, pp. 64–66. doi: 10.1016/j.mfglet.2018.02.006, Jan. 2018.
[30] E. Negri, L. Fumagalli, M. Macchi, A review of the roles of Digital Twin in CPS-based production systems. The Author(s), 11(June), pp. 939–948. doi: 10.1016/j.promfg.2017.07.198, Jan. 2017.
[31] M. Abramovici, J.C. Göbel, H.B. Dang, CIRP Annals - Manufacturing Technology Semantic data management for the development and continuous reconfiguration of smart products and systems, 65, pp. 185–188, Jan.2016.
[32] J. Green, Cisco, The internet of things reference model, In *Internet of Things World Forum, Cisco White Paper*, pp. 1–12, June. 2014.
[33] F.H. Abanda, J.H.M. Tah, R. Keivani, Expert Systems with Applications Trends in built environment semantic Web applications: Where are we today?, *Expert Systems With Applications*. Elsevier Ltd, 40(14), pp. 5563–5577. doi: 10.1016/j.eswa.2013.04.027, Oct.2013.
[34] F. Ameri, L. Patil, Digital manufacturing market: a semantic web-based framework for agile supply chain deployment, *Journal of Intelligent Manufacturing*, pp. 1817–1832. doi: 10.1007/s10845-010-0495-z, Oct.2012.
[35] Z. Wang, J. Sun, and D. Hutchison, *Semantic Technology*, 2016.
[36] O. Bodenreider, R. Stevens, Bio-ontologies: current trends and future directions, 7(3), pp. 256–274. doi: 10.1093/bib/bbl027, Sep.2006.
[37] Q. Rajput, S. Haider, Procedia Computer A comparison of ontology-based and reference-set-based semantic annotation frameworks, *Procedia Computer Science*. Elsevier, 3, pp. 1535–1540. doi: 10.1016/j.procs.2011.01.045, Jan.2011.
[38] H. Boyes, and the Built Environment, *IT Professional*. IEEE, 17, pp. 25–31. doi: 10.1109/MITP.2015.49, Jan.2015.
[39] D.G. Photovoltaics, E.Storage, *Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads IEEE Standards Coordinating Committee 21 Sponsored by the*, 2011.
[40] S. Howell, Y. Rezgui, JL. Hippolyte, B. Jayan, B. Jayan, and H. Li, Towards the next generation of smart grids: Semantic and holonic multi-agent management of distributed energy resources, *Renewable and Sustainable Energy Reviews*. Elsevier Ltd, 77(March), pp. 193–214. doi: 10.1016/j.rser.2017.03.107, Sep.2017.
[41] M. Hogan, B. Piccarreta, and Interagency International Cybersecurity Standardization Working Group. *Interagency report on status of international cybersecurity standardization for the Internet of Things (IoT)* (No. NIST Internal or Interagency Report (NISTIR) 8200 (Draft)). National Institute of Standards and Technology, Feb. 2018.
[42] S.C. BSI, PAS 1192-5: 2015 A specification for security-minded building information modelling, digital built environments and smart asset management, 2015.
[43] M. Eckhart, A. Ekelhart, Towards Security-Aware Virtual Environments for Digital Twins, pp. 61–72, May.2018.
[44] S. Sridhar, A. Hahn, and M. Govindarasu, Cyber – Physical System Security for the Electric Power Grid, *Proceedings of the IEEE*. IEEE, 100(1), pp. 210–224. doi: 10.1109/JPROC.2011.2165269, Oct.2011.
[45] A. Perrig, J. Stankovic, and D. Wagner, Security in wireless sensor networks, Jan.2004.
[46] A. Perrig, R. Szewczyk, J.D. Tygar, V. Wen, and D.E. Culler, SPINS : Security Protocols for Sensor Networks, pp. 521–534, Sep. 2002.
[47] B. Parno, M. Luk, E. Gaustad, A. Perrig, Secure Sensor Network Routing: A Clean-Slate Approach, Dec. 2006.
[48] M. Luk, G. Mezzour, A. Perrig, and V. Gligor, MiniSec : A Secure Sensor Network Communication Architecture CBC-enCrypton , eq andly, pp. 479–488, Apr. 2007.
[49] R.J. Turk, Cyber Incidents Involving Control Systems, (No. INL/EXT-05-00671). *Idaho National Laboratory* (INL), Oct.2005.
[50] R. Mitchell, I.R. Chen, A Survey of Intrusion Detection Techniques for Cyber-Physical Systems, 46(4), Mar.2014.
[51] YL. Huang, A.A. Cárdenas, S. Amin, ZS. Lin, H-Y. Tsai, and S. Sastry, Understanding the physical and economic consequences of attacks on control systems, *International Journal of Critical Infrastructure Protection*. Elsevier B.V., 2(3), pp. 73–83. doi: 10.1016/j.ijcip.2009.06.001, Oct. 2009.
[52] S. Tang, D.R. Shelden, C.M. Eastman, P. Pishdad-Bozorgi, and X. Gao, Automation in Construction A review of building information modeling (BIM) and the internet of things (IoT) devices integration: Present status and future trends, *Automation in Construction*. Elsevier, 101(January), pp. 127–139. doi: 10.1016/j.autcon.2019.01.020, May. 2019.