www.itcon.org - Journal of Information Technology in Construction - ISSN 1874-4753

CYBERSECURITY FOR DIGITAL TWINS IN THE BUILT ENVIRONMENT: CURRENT RESEARCH AND FUTURE DIRECTIONS

SUBMITTED: May 2020
REVISED: March 2021
PUBLISHED: April 2021
EDITOR: Bimal Kumar
DOI: 10.36680/j.itcon.2021.010

Kaznah Alshammari,
Cardiff University;
alshammarik1@cardiff.ac.uk

Thomas Beach, Dr.,
Cardiff University;
beachth@cardiff.ac.uk

Yacine Rezgui, Professor,
Cardiff University;
rezguiy@cardiff.ac.uk

SUMMARY: *Recent technological developments in the construction industry are seeking to create smart cities by using Cyber-Physical Systems (CPSs) to enhance information models such as BIM. Currently, BIM models are commonly adopted to work with IoT-based systems and embrace smart technologies that offer interoperability in the communication layer. In future, it is envisioned that digital twins will provide new possibilities for cyber-physical systems via monitoring and simulation. However, rarely in this rapidly developing field is security fully considered. This paper reviews the relevant literature regarding the use of the IoT in the built environment and analyses current practices. It also presents examples of cities that use the IoT to improve construction and the lived experience. Finally, it reviews how digital twins factor in multiple layers defined in CPSs, from physical objects to information models. Based on this review, recommendations are provided documenting how BIM specifications can be expanded to become IoT compliant, enhancing standards to support cybersecurity, and ensuring digital twin and city standards can be fully integrated in future secure smart cities.*

KEYWORDS: *BIM, IoT, digital twins, cybersecurity*

REFERENCE: *Kaznah Alshammari, Thomas Beach, Yacine Rezgui (2021). Cybersecurity for digital twins in the built environment: current research and future directions. Journal of Information Technology in Construction (ITcon), Vol. 26, pg. 159-173, DOI: 10.36680/j.itcon.2021.010*

1. INTRODUCTION

Currently, the construction industry is seeking to create ever-smarter buildings, cities and districts. Such a trajectory relies on continuous advances in information and communication technologies (ICT) to create and exchange information.

Technological developments in recent times have delivered advances in terms of wireless and mobile communications, ever-present connectivity, improved communication speeds and cheaper sensors. Not only has technology become increasingly pervasive but there has also been closer integration between cyber systems and physical infrastructure (Miorandi et al., 2012), more commonly referred to as the Internet of Things (IoT). Falling costs and advances in communication networks have resulted in the rapid uptake of this technology in recent years (Gubbi et al., 2013). Consequently, this presents numerous opportunities for knowledge of the built environment to yield considerable value. Building Information Modelling (BIM) is an example of an information model in the built environment and has appeared in the architecture, engineering, construction and facilities management (AECFM) industry as a new step in the enhanced digitisation of built environment data.

However, the legacy formats of BIM and its convoluted modelling paradigms make it ill-suited for use in an IoT setting. As such, adoption of BIM remains distant at a time when other systems are increasingly utilising lightweight and extensible data schemas in web-native languages. Building designs are increasingly required to satisfy a combination of environmental, societal and economic requirements and, consequently, they are becoming more complex. This is apparent from the need to include the latest construction technologies, procurement paths, construction methods and materials. As such, rather than relying solely on the traditional disciplines such as knowledge of mechanics, architecture, electrics and structures, professional insight must also be sought in areas such as waste, the environment, energy and the IoT (Howell and Rezgui, 2018).

One way in which BIM can be used in this evolving environment is in a layered model to help visualise and systematically categorise the different elements, paying particular attention to how best to enable knowledge and ICT to improve business services (Shin, 2009). In essence, this involves the use of a sensing layer, a form of communication, as well as facilities to process and store information. Finally, the application, business, innovation and governance layers are included.

Sensor networks have concentrated on planning cyber-physical systems (CPSs) communication infrastructure. Therefore, digital twin technology provides for the CPSs a new potential outcome as far as monitoring, simulating, optimising and predicting the condition. Therefore, a virtual replica of a CPS is useful and can assume a significant role in securing a system with ceaseless feedback to improve personal satisfaction and prosperity (Steinmetz and Rettberg, 2018; Eckhart and Ekelhart, 2018).

There is growing recognition of the opportunities presented by digital twins and the IoT in the built environment. This contributes to the creation of smart cities which use ICT to facilitate information sharing with the public. However, while they offer numerous benefits, there are also a number of associated challenges and chief among these is the security threat (Demkovich and Yablochnikov, 2018). At present, there are distinct challenges when attempting to install cybersecurity into digital twins that will be utilised in applications designed for the built environment. Moreover, this is an area that has been woefully under-researched. As such, a need exists for digital twins that can protect and identify true twins. The aim of this paper is to review the current cybersecurity landscape of the built environment focusing on the current state-of-the-art in the fields of BIM, IoT, digital twins and cybersecurity. This paper then analyses the current state-of-the-art to present a series of recommendations for future research in order to provide an appropriate cybersecurity framework for the emerging field of research into digital twins.

In the remainder of this paper, Section 2 presents the methodology of the review, Section 3 defines the concept of a building information model, and Section 4 discusses the use of cyber-physical systems in the construction industry by defining the concepts of a smart built environment and also presenting eight smart cities in Europe that have been at the forefront of IoT advances. In addition, a definition is provided for digital twins. Then Section 5 presents a number of recommendations to realise the goal of developing smart buildings in a safe environment. Finally, Section 6 concludes the paper.

2. METHODOLOGY

This section describes the methodology of the review. The aim of this research is to review current work in digital twins in the context of a web-based IoT in the built environment, focusing on the current cybersecurity landscape and the need for digital twins protection to ensure the identity of their true twin by using a systematic search of academic databases (Google Scholar, Scopus, IEEE Xplore, ScienceDirect and Elsevier).

A combination of BIM, IoT, smart built environment, digital twins and cybersecurity were used when searching and the total of number of publications was 124. The number of publications in each category is detailed in Table 1. When reading this table, it should be noted that each paper only appears once in the row that best defines its contents. However, some publications were omitted from further study because they were deemed to be obsolete (pre-2002) or featured only a brief discussion of the selected topic and did not advance the state-of-the-art in the built environment domain. As a result, the current paper analysed a total of 58 articles. More specifically, the following criteria were applied for the purpose of filtering:

- Paper published since 2002.
- The paper must include an advancement in the state-of-the-art in its subject area relevant to the built environment domain.
- Finally, they must clearly discuss a problem and present a scientifically developed solution that is evaluated based on clear evidence.

Table 1: Article distribution

Keywords	**Number of articles in this category**
BIM	30
Digital twins	3
IOT	13
Security	26
BIM, DT	0
BIM, IOT	2
BIM, Security	12
DT, IOT	2
DT, Security	3
IOT, Security	14
BIM, DT, IOT	3
BIM, DT, Security	1
BIM, IOT, Security	5
DT, IOT, Security	3
BIM, DT, IOT, Security	1
Random	6

Cybersecurity is the main issue in all of these research papers which cover a variety of topics from digital twins to physical objects (i.e. IoT) and information models (including BIM).

BIM is discussed in Section 3, the IOT is discussed in Section 4 and Section 4.1, DTs in Section 4.2, while cybersecurity is discussed in all of the sections because it is an essential element in this paper.

3. BUILDING INFORMATION MODELLING (BIM)

The architecture, engineering and construction (AEC) industry demands a great deal of collaboration between project users which can only be improved by making the means of communication more secure. Because the AEC industry depends on the exchange of information, the data files connect by means of exchange files (Das, Cheng and Kumar, 2014). BIM data is well-suited for the design, planning and monitoring of progress in the construction of a building because it is updated when users exchange BIM data files (Boyes, 2014). BIM has developed within the architecture, engineering, construction and facilities management (AECFM) industry, causing a marked change in step digitisation. Through Industry Foundation Classes (IFC), BIM can be created and managed in the design and construction stages, thereby resulting in notable industrial advances (Howell and Rezgui, 2018).

BIM uses commercial software and the AEC industry creates and designs 3D modelling with BIM software which is a platform that makes the communication of project ideas and designs easier. It also provides tools for buildings and infrastructure which contain data (Autodesk, 2003) such as Revit (Autodesk), Constructor (Vicosoft) and Microstation (Bentley) (Cha and Lee, 2015). Many empirical studies have presented opportunities that support software development and implementation but stressed that an iterative, collaborative and modular approach is required (Dave et al., 2016).

BIM concerns the generation and management of information relating to a building over the course of its usable life from the drawing board to its ultimate demolition. BIM provides a basic role in supporting building operation and maintenance by offering an incorporated interface to building operational execution data in all aspects (Gha et al., 2017).

One of the most widely applied approaches to BIM is IFC. IFC are open data model specifications for the geometry of building components and the related properties used so that people can transfer data from one software program to another when using CAD (Howard, 2008). The idea is that they afford a comprehensive definition of the various building components as well as their qualities and inter-relationships. The data used in relation to IFC includes illustrations, numerical models, textual data, structured documents, and the annotations of project managers. IFC often appear in ISO standards and are maintained using buildingSMART. The IFC method arguably offers a highly-suitable framework for handling data relating to building management because it has established rules governing areas such as the storage and exchange of data as well as protocols (Howell and Rezgui, 2018).

However, it must be noted that neither BIM Level 2 which focuses on the collaboration between teams and the BIM process and sharing the data collected about a built asset nor BIM models are able to support security features (Kirstein and Ruiz-Zafra, 2016). At present, security concepts do not feature in the BIM standards and the standards are solely concerned with design. As such, it is not possible for them to be translated into the operational phase. Rather, it is necessary to utilise a Building Automation System (BAS) to enable it to be incorporated at a later time. Doing so enables incorporation into building data and the IoT, possibly by means of proprietary data models to produce a smart building as well as access to physical building objects (Jung, Reinisch and Kastner, 2012).

BIM lays down an array of information to help steer the commissioning process such as when to adjust energy systems and when to undertake an initial evaluation of building performance. The operation stage includes stakeholders who interact with the built environment and perform certain activity (insert, extract, update or modify) information from the BIM (Bosch, Volker and Koutamanis, 2015). It involves four roles for a building process: strategy making, controlling, decision-making, and task managing. The operation stage uses 3D or 4D BIM models that afford additional insight in terms of information for a project information model. Such information is incorporated to elements as progress is made with the project. 4D BIM is set from a 3D BIM model and a construction schedule project. However, in the operation stage, BIM remains ill-suited for a number of duties; for example, the limitations of IFC with regards to re-using the knowledge of other domains to achieve advanced reasoning (Rezgui, Beach and Rana, 2013).

BIM is used to model built assets and these assets are at the core of a variety of systems that the IoT serves. Therefore, the knowledge at the heart of information models at the design and construction stages sets the background for the data that IoT sensors amass in real time (Cisco, 2014).

One of the primary ways in which BIM technology is advancing is through the use of Semantic Web Technologies. The Semantic Web enables the possibility of extending BIM to provide users of building data with richer and better specified datasets critical to support effective decision-making for planning, designing, constructing and operating built assets (Boje et al., 2020).

The Semantic Web (Ameri and Patil, 2012) represents the semantics of Web content in a machine-readable structure that enables the application of intelligent techniques to automate tasks that are, at present, dealt with manually by users. Adding Semantic Web layers above present Web technologies enables machines to comprehend the meaning of content and data over open standards and enables further advanced applications by separating data gathering.

Machine-readable semantics of ideas in an application area can be characterised utilising Semantic Web standards. These standards include following core concepts and the main standards in Semantic Web are the *"resource*

description framework (RDF) and SPARQL Protocol and RDF Query Language (SPARQL). RDF is a standard model for data interchange on the Web. SPARQL is a W3C specification and a query language for RDF" (Abanda, Tah and Keivani, 2013).

Ontologies are a key factor in the Semantic Web that are used to display and exchange knowledge. Ontologies should be defined using standard languages to enhance interoperability, information retrieval and natural language processing (Rajput and Haider, 2011). There are several ontology languages such as the Web Ontology Language (WOL) which refers to the determination of classes, properties and related limitations. WOL is intended for use by applications that need to process the substance of information (Abanda, Tah and Keivani, 2013). Semantic Web Rule Language (SWRL) and Semantic Query-Enhanced Web Rule Language (SQWRL) are propositions for a Semantic Web rule language joining the sub-languages of the WOL (WOL DL and Lite) with the Rule Mark-up Language (RML). It uses SQL-like tasks to recover information from WOL (Abanda, Tah and Keivani, 2013). Semantic Web Services (SWS), according to the W3C, is a software system with the purpose of facilitating machine-to-machine engagement across a network. The interface used is referred to as a machine-processible format, otherwise termed the Web Services Description Language (WSDL) (Abanda, Tah and Keivani, 2013). Linked data is a style for distributing and connecting organised data on the Web. The value and convenience of information are enhanced when interlinked or compounded with different datasets (Bizer and Berlin, 2008). Furthermore, there are linked and domain dictionaries and specialised taxonomies: "bcXML is an XML vocabulary developed by the eConstruct Information Society Technologies (IST) project for the construction industry. Industry Foundation Classes (IFC) were developed by buildingSMART; OmniClass. In the empirical literature there are diverse opinions regarding which of these are real ontologies. Both IFC and bcXML are considered to be implicit ontologies (Yang and Zhang, 2006).

The type of file used is ifcOWL and this offers a number of benefits. For instance, it links building data to material data, integrates manufacturing data and processes, links to GIS data, provides context to sensor data, and links to social data. IfcOWL is based on 'ontologies' that are Web empowered, a development of legacy element relationship models that are all the more likely to suit the versatile and distributed nature of the Web. Also, the speed of collaborative IoT innovation and facilitating application layer interoperability are aims that achieve the HyperCat Standard that proposes a REST pattern API, a key-based verification strategy that should be incorporated. The standard also offers further benefits such as *"subscription, more security options, various search methods, and a means for further integrating HyperCat into the linked data and Semantic Web ecosystem"* (Howell and Rezgui, 2018).

Automating tasks is increasingly significant today for the multiplication of linked devices that constitute the IoT (Gubbi et al., 2013). By employing computers and ICT in Semantic Web technology, BIM information becomes exchangeable and provides insight into different fields. However, knowledge about trends in the applicability of the Semantic Web is limited and not many empirical studies have been conducted into how existing Semantic Web technologies are applied (Howell and Rezgui, 2018).

4. CYBER-PHYSICAL SYSTEMS IN THE BUILT ENVIRONMENT

One way to achieve a cyber-physical system is to use the IoT concept. The IoT interconnects each physical entity in a building's construction lifecycle and collects data from the processes of a project (Tao et al., 2014). The building design information model is connected with real-time construction data via integration BIM with the IoT that enables designers to interact in real-time and resolve construction progress uncontrollability problems and costs during the execution phase. The IoT, sensors, mobile devices and software applications are resources that can be used to better understand the smart construction site. Thus, the interconnectivity and interoperability of the building site are understood from the perspective of both digital world and physical world reconciliation (Ding et al., 2018).

The integration of BIM with the IoT produces a 'digital twin' of a real building in a BIM platform and can be used to simulate the construction process, thereby enabling performance to be assessed and the key influential factors to be identified. IoT data is correlated with the BIM model and analytical tools are utilised to simulate the construction process in a synchronous manner. As such, the combination of real-time IoT data with the BIM model comprises the main element of the enabling technology system. The data made available from the IoT-enabled lifecycle model and the BIM-enabled lifecycle model effectively forms the core of efforts to produce 'smart' construction processes (Tao and Qi, 2019).

In light of these outcomes and considering the effect of the IoT on building sites for improving construction strategies, the IoT can offer both effective and necessary support. In particular, the measure of data controlled, the quantity of specialists included, and the variety of areas to be considered require a lot of IoT-empowering highlights (Guerriero et al., 2017).

4.1 Smart built environment

Construction projects benefit from BIM, especially in terms of how information is delivered across supply chains during procurement and when agreeing a design. By making a distinctive value proposition, BIM is able to effectively stimulate and re-energise how the construction sector operates by reducing costs and waste while simultaneously making the delivery process more efficient. Moreover, automation and control systems help to make buildings smarter as a result of innovations in the areas of HVAC, telecommunications, building management systems, utilities, and health and safety. It is possible to categorise these as smart building components, pervasive sensing nodes, and intelligent control and actuation devices (Howell and Rezgui, 2018).

Industry 4.0 refers to the integration of industrial technologies with ICT that are able to process data and communicate it to create digital twins (Haag and Anderl, 2018). Digital twins were first used in the aerospace industry (Negri, Fumagalli and Macchi, 2017), paying particular attention to material science, structural mechanics and predictions of performance for aircraft and spacecraft (Tuegel et al., 2011). The digital twin can support information to confirm its continuity during the complete product lifecycle (Dang, Abramovici and Go, 2016).

Digital technologies are now being incorporated into the built environment in ways that had not previously been considered and this is giving rise to smart approaches to building and infrastructure management. In this domain, BIM is well-suited to offer a particular value proposition if it can be adapted to work alongside internet-based systems and embrace smart technologies. This is because built environment stakeholders are already familiar with the concepts and standards involved and existing built environment software tools are already compatible. Continual innovation in the realms of the IoT and artificial intelligence (AI) are resulting in more mature products and services that can be applied in an ever-wider range of fields (Howell and Rezgui, 2018).

The technological elements are concerned with the cybersecurity set-up regarding how data is formed and applied in information exchanges, the supply chain and shared repositories, and common data environments. Construction and asset management supply chains are unaccustomed to accommodating cybersecurity considerations and, as a result, wide-ranging changes will need to be made to security policies if BIM is to be implemented. Cybersecurity is based on many standards such as ISO 27002:2013, Federal Information Processing Standard (FIPS) 201, Advanced Encryption Standard (AES) (Technology, 2017), and Triple Data Encryption Algorithm (3DES) that provide lower costs while ensuring high levels of security and performance. However, there is a need to apply suitable hazard evaluations and in appropriate scenarios rely on the communication asset (Howell et al., 2017). Indeed, the UK government has taken a proactive stance on this matter by encouraging relevant parties to take cybersecurity into consideration, including certification by contractors of ISO 27001 (Boyes, 2015).

As BIM is rolled out in the asset management domain, this will result in security matters becoming considerably more complicated. It is when responsibility for assets is formally transferred to the owner from the project team that asset management processes are initiated. This transfer also extends to responsibility for the data incorporated into the BIM model in the common data environment. The intention is for the model to evolve throughout the working life of the asset, combining data relating to the design and construction stages with that concerning the use of the asset and its maintenance (Boyes, 2015).

The future of BIM that is able to communicate with IoT devices presents key cybersecurity concerns (Generation and Storage, 2011). Moreover, the implementation of cybersecurity in smart grids which are used in energy systems has emerged as a significant subject lately because of the security problems that face these energy systems. Howell et al. (2017) discussed three avenues to improve security and performance: *"Firstly, research must identify and quantify the risk of a breach of privacy and security to the systemic reliability and quality of service (QoS) caused by insecure authentication occurring in a heterogeneous environment, where legacy standards and applications need to remain in operation alongside advanced standards. Secondly, research must identify and quantify loss of data, breach of privacy and vulnerability due to the heterogeneous communication infrastructure (wireless, wired, PLC) and the impact on grid reliability and QoS. Finally, research must develop guidelines for information security management and inform related legislation and standardisation."* The energy systems are

based on the smart grid to improve performance, so three fundamental elements of smart grid security are discussed here: secure authentication, secure communication, and information security management (Howell et al., 2017).

The standard specifications of BIM Level 2, IFC and COBie models cannot support the security features of the IoT. Consequently, these standard specifications cannot be applied to assist with the early stage building design process for smart built environments that require security and the deployment of the IoT. Rather, it has been possible to subsequently incorporate this by means of a Building Automation System (BAS). If a built environment has relied upon BIM, it will be deficient in security and IoT services. While BIM is able to accommodate conventional aspects of buildings including the likes of doors, ceilings and electrical sockets, it is ill-suited to accommodate security features or IoT devices. For instance, it could not incorporate IoT devices that require a particular security token to operate or determine which people are permitted to gain entry to certain rooms (Kirstein and Ruiz-Zafra, 2016).

BS EN ISO 19650-5:2020 specifies the principles and standards for security-minded information management of sensitive information collected as part of a relationship with a project, an asset and a service (CPNI, 2020).

The global decentralized servers for the Handle System's security only permits access to the local system. Be that as it may, it is necessary to be aware that the BIM data could be compromised as a result of security weaknesses in the application-specific servers. In addition, relying on external templates running on systems with known security frailties could be a source of malware and, therefore, efforts must be made to ensure they are free from infection. Such an approach to security is necessary for BIM data but not for EBIS (Kirstein and Ruiz-Zafra, 2016). Those responsible for overseeing investment in smart buildings and the application of BIM when designing and managing assets must have a grasp of the latest cybersecurity threats and mitigate any risk to the common data environment. If this is not the case, the asset's security could be placed at risk because intellectual property could be lost or the systems associated with the asset could be breached. Recognising the seriousness of this issue, the UK government published BS EN ISO 19650-5:2020 concerning the principles and criteria for information security management setting out how best to manage security issues while applying BIM, managing smart assets or developing digital built environments (CPNI, 2020; Dasgupta, Gill and Hussain, 2019).

An integrated solution capable of accommodating security and IoT features was proposed by Kirstein and Ruiz-Zafra (2016). This approach offers the potential for built structures to incorporate dynamic asset data structures. This forms part of current efforts to extend BIM Level 2 to support the IoT and security (EBIS) initiative which developed a framework for built environments to incorporate IoT scenarios, including details of the procedures to be adhered to and the necessary software. This study sets out to assign a hierarchical identity to the various physical elements through the Handle System. The Handle System involves Digital Objects (DOs) with each physical asset being assigned a digital representation so that the attribute data can be stored in a protected repository, and security features and the IoT can be incorporated in the digital representation. The Handle System supports the DOs and this is a Secure Identity Data Management System (SIDMS).

Furthermore, Kirstein and Ruiz-Zafra (2016) addressed the *"Use of templates and the Handle for the large-scale provision of security and IoT in the built environment"* using HyperCat which is a "a standard for driving secure and interoperable IoT for industry." It provides an extensive selection of algorithms and mechanisms.

More specifically, HyperCat is a lightweight JSON-based hypermedia catalogue. HyperCat manages various data sources amassed into data hubs via connected data and web methods. It involves a lightweight JSON application based on a technology stack utilised by a large populace of Web developers. HyperCat gives a standard machine-process capable method for resource revelation that empowers an interoperable environment. HyperCat provides open source devices (Wang, Sun and Hutchison, 2016). According to the paper, by utilising HyperCat as well as the Handle System, it should have the potential to distribute every one of the assets of a structure with Handle identifiers so as to be utilised by third-party programming or users.

However, Kirstein and Ruiz-Zafra's method merely provides a technology base. Kirstein and Ruiz-Zafra (2016) validate their work with a proof of concept (PoC) in a smart building environment which contains two secure rooms to publish the location of these rooms without uncovering details of how they may be accessed and giving undesirable information to potential attackers. It might be significantly more desirable to put all sensitive information and how to find it into areas that are inaccessible to unauthorised entities. Therefore, the technology base provides some tools for mitigating threats but it does not address them.

So, smart grid security is important to secure the sensor of a network and the encryption algorithms are a standard of cybersecurity (e.g. AES and 3DES) that ensure correct permissions for actors and security across the different scales of the built environment (Howell et al., 2017).

Overall, apart from these, there are few papers that propose methods for enhancing IoT security in the built environment. However, in addition to pure academic work, there are currently eight cities engaged in projects to improve their infrastructure using an intelligent solution that includes ICT to improve the quality and performance of urban services such as transportation, energy and water (Synchronicity, 2019). This paper will now briefly review these cities to determine how they are solving the problem of security in the smart city domain. These cities are Antwerp, Carouge, Eindhoven, Helsinki, Manchester, Milan, Porto and Santander. These cities are all on a path towards developing a smart city condition based on existing IoT ecosystems and frameworks utilising open standards and being consistent with Open & Agile Smart Cities (OASC) standards. These cities have ideas for IoT development and contain the different functionalities and technologies that support the smart city environment (Synchronicity, 2019).

The cities have different architectural approaches. These commonly include (a) Southbound interfaces which refer to APIs that support both IoT data collection and command addressing; (b) Data management which refers to data storage and management; (c) Northbound interfaces which provide data access and data management that is provided by context management APIs; and (d) Security and privacy components which refer to security and privacy concepts including authentication, authorisation and accounting arrangements (Synchronicity, 2019).

Antwerp channels its IoT advancement through two fundamental activities: the Antwerp City Platform as a Service Platform (ACPaaS) and City of Things (CoT). Carouge looks to use IoT advancement activities in three core architectures: smart parking, street noise monitoring, and an app for tourism that is proprietarily developed and not open. Eindhoven centres around supporting organic development of and interoperability between the arrangement of IoT stages and vertical systems effectively present in the city. Eindhoven depends on a wide arrangement of sensors including actuators and wireless communication technologies. Eindhoven has four core architectures but only integrated data management (CKAN) is currently available, while FIWARE Orion Context Broker, FIWARE Complex Processing (Proton) and FIWARE Big Data (Cosmos) are currently being evaluated for the next platform evolution. Helsinki, as of now, is represented by Digitransit architecture (Digitransit, 2019) that implements an Open Message Interface (O-MI) node (Opengroup.org, 2019) and Helsinki CKAN. Manchester is looking more broadly at executing smart city projects, while the current arrangement of smart city projects comprises CityVerve (CityVerve, 2019) and Triangulum H2020. Milan has three core architectures (parking, building/energy, and weather/noise/pollution) that contain several projects in different domains which are specifically developed and not open. Porto is involved with different apps and services which are specifically developed and not open which are: a water management platform, a mobility management platform (Synchronicity, 2019), an environmental monitoring platform, and a citizen platform. The Municipality of Santander provides a large number of projects and IoT initiatives: FIWARE Context Broker (Orion), FIWARE Short Term Historic (Comet), FIWARE persistence connector (Cygnus) and CKAN Data Persistence.

Regarding these cities, Eindhoven, Porto and Santander are the most developed urban cities and utilise the IoT to make them smart cities. Carouge and Milan each contain three architectures that operate several projects. Antwerp and Manchester are less-developed urban cities with each containing two core architectures (see Fig. 1).

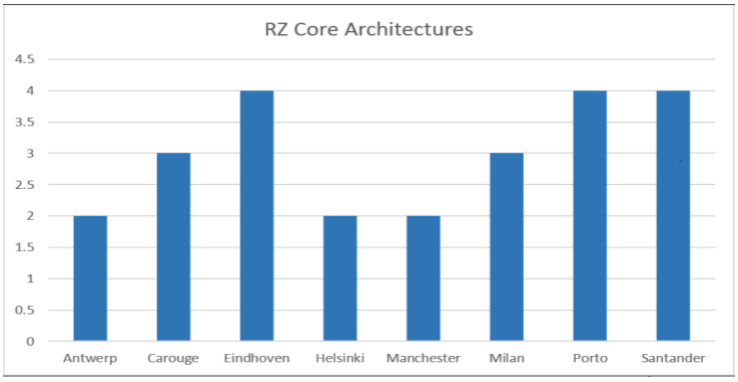

FIG. 1: Reference Zone Core Architectures

Reference Zones are intended to support various security and privacy levels in future by using FIWARE on FIWARE secure. FIWARE is a cloud platform that gives new novel programming components accessible through APIs to give developers new significant cloud platform operations (Fazio and Celesti, 2015). For smart cities, it offers elements that facilitate data collection from numerous remote systems and IoT devices across the city. In addition, FIWARE offers the means to link conventional open data with real-time data. However, the security component used by FIWARE is a standard off-the-shelf tool and possesses no specific built environment security concepts (Synchronicity, 2019). The Reference Zones are suggesting the creation of a security layer as follows:

Table 2: Reference Zone Cybersecurity (Synchronicity, 2019)

Reference Zones	**Cybersecurity layer**
Antwerp	Does not have an official security layer but Antwerp's platforms have been given certain tools to execute authentication and authorisation functionalities.
Carouge	Currently undertaking an investigation into selecting a solution for authentication, authorization and accounting and is considering employing FIWARE AAA with the FIWARE Secure Catalogue as a conceivable solution. The integration of the Carouge IoT with FIWARE will be overseen by Mandat International (International, 2019) and UDG.
Eindhoven	Considering the utilisation of FIWARE in order to improve security and privacy.
Helsinki	Suggests potential support for O-MI security models that execute authentication and authorisation mechanisms operated with the O-MI RESTful API.
Manchester	Manchester public sector IG specialists and private sector partners are looking to implement a privacy management software tool. Privacy Policy Manager (PPM) is being implemented by British Telecommunications (BT) as part of the CityVerve project. Manchester has an API management system that uses an OAuth2 protocol to manage Identity Management (IDM) and an authorisation component.
Milan	Will assess the adoption of FIWARE to enhance certain security and privacy aspects.
Porto	Porto's app is based on login/password through https and is looking for authentication, authorisation and accounting using OAuth/OAuth2. However, no security layer is currently specified.
Santander	There is no official layer specific for security and privacy functionalities in the Santander Reference Zone but it executes some solutions founded on FIWARE Keyrock IDM and Wilma PEP that supports OAuth mechanisms to manage access to resources.

Therefore, the cities look forward to optimising their infrastructure to become smart cities through IOT compliance with sensors. However, they still lack a cybersecurity model to be able to work perfectly and safely (Synchronicity, 2019).

4.2 Digital twins

Digital twins enable new potential outcomes as far as monitoring, simulating, optimising and predicting the condition of cyber-physical systems (CPSs) is concerned. They also provide humans with continual feedback to improve personal satisfaction and prosperity (Steinmetz and Rettberg, 2018). Furthermore, a virtual replica of a CPS is useful and can assume a significant role in securing a system (Eckhart and Ekelhart, 2018).

Cyber-physical system issues require the capacity to analyse the connection between physical and cyber components (Sridhar, Hahn and Govindarasu, 2012). The security of a CPS relies on sensor network security (Perrig, Stankovic and Wagner, 2004). The majority of efforts expended on the security of sensor networks has concentrated on planning a secure communication infrastructure. The fundamental outcomes contain effective algorithms for: (1) bootstrapping security associations and key management (Eschenauer and Gligor, 2002; Perrig et al., 2002) to create a secure infrastructure; (2) secure communication (Luk et al., 2007); and (3) secure routing protocols (Karlof, 2003; Parno et al., 2006).

Moreover, the replication mode mirrors information from physical objects. Potential information sources to reflect virtual objects include log documents, network communication and sensor estimations from physical objects. Sensors can be connected directly with the CPS twinning structure (Eckhart and Ekelhart, 2018).

A large proportion of the applications are safety critical and if they were to fail, this would have severe consequences, not only for the system but also the people who rely on it. For instance, SCAD systems play a central role in various national critical infrastructures including electricity grids, natural gas supplies, transport systems and wastewater treatment systems. If these control systems were to be compromised, there would be serious adverse implications in terms of safety, public health and/or the associated financial cost. To date, efforts to preserve CPS systems have largely focused on improving reliability there is now growing appreciation of the need to protect against deliberately initiated cyber-attacks (Directorate et al., 2006; Turk, 2005). With a spotlight on security, digital twins can serve as an establishment for conduct determination based on IDS. It is possible that IDS may become a primary input for analysis (host-based) but also be responsible for auditing the network traffic (network-based) (Mitchell, Chen and Tech, 2014).

Sridhar, Hahn and Govindarasu (2012) discussed the importance of cyber infrastructure security with power application security to block cyber-attacks. They addressed smart grid cybersecurity: a power application that refers to the gathering of operational control functions that are important to maintain stability inside the physical power framework, supporting infrastructure that refers to the infrastructure components (software, hardware and communication networks). They classified the control loops of the power system that recognise protocols and communication signals, computations, devices and control actions related to select control loops in the various functional classifications. Control centres receive estimations from sensors that engage with devices in the field. The control centre's algorithms compute the measurements received and take appropriate decisions accordingly. Once a decision has been made, it is conveyed to an actuator so that appropriate changes can be made to the devices in the field. As such, there is an opportunity for a third party to identify a vulnerability in the communication system to create attack templates in order to either deny access, cause an extended delay or corrupt the content (e.g. denial of service (DoS), timing attacks and desynchronisation) (Huang et al., 2009). The potential for such attacks to the power system must be monitored continually to preserve its integrity. The associated effects could include violations of the system operating frequency, a loss of load, changes in voltage, as well as a range of secondary effects. By conducting attack studies, it is possible to prepare countermeasures to either minimise the disruption caused by such attacks or stop them from taking place. Examples of countermeasures include attack resilient control algorithms and efforts to detect bad data. Providing a cybersecurity layer within DTs for the built environment presents a key challenge. DTs should be able to secure the identity and protection of their genuine twin and this would require the utilisation of cryptography algorithms.

5. RECOMMENDATIONS

Based on Sections 3 and 4, the IoT presents a significant portion of developing BIM to support smart buildings. Whilst the researchers have developed numerous IoT platforms, none of these are yet able to achieve close integration with BIM data models. Extending BIM to support the IoT and security concerns would ignored a vital aspect: the requirement to run secure servers.

Also, DTs enable new potential outcomes as far as monitoring, simulating, optimising and predicting the condition of cyber-physical systems (CPSs) is concerned. Efforts to preserve CPS systems have largely focused on improving reliability but there is now growing appreciation of the need to protect against deliberately initiated cyber-attacks. Providing a cybersecurity layer within DTs for the built environment presents a key challenge. DTs should be able to secure the identity and protection of their genuine twin.

Therefore, the industry looks to develop buildings to become smart buildings through IoT-based adoption of sensors. However, it still lacks a cybersecurity model for digital twins to be able to work perfectly and safely. Those responsible for overseeing investment in smart buildings and the application of BIM when designing and managing assets must have a grasp of the latest cybersecurity threats and mitigate any risk to the common data environment. If this is not the case, the asset's security could be placed at risk because intellectual property could be lost or the systems associated with the asset could be breached.

Furthermore, the basis of smart building technologies would be drawn from BIM specifications. However, BIM specifications have not been developed to support smart buildings. BIM has been developed to prompt data exchange between different applications. Thus, there is a need to enhance BIM to become IoT compliant to support sensors/controllers. As such, the new thread that appears is one that is linked to cybersecurity. The technological elements are concerned with the cybersecurity setup concerning how data is formed and applied in information exchanges. Thus, according to the literature review above, there is currently no cybersecurity model for digital twins or smart cities. Consequently, there are a number of recommendations for future research into a cybersecurity model for digital twins in the built environment:

Recommendation 1: Expand BIM specifications to become IoT compliant.

An integration of BIM with the IoT develops structure and operational competences and provides real-time data streams of IoT sensor networks to the BIM models giving several applications (Tang et al., 2019) (see Section 3).

Recommendation 2: Enhance BIM standards to support the required cybersecurity concepts. The key concept is ISO 19650-5:2020 which gives a security framework to apply a suitable and proportionate way to deal with the security risk that influences asset information and data. ISO 19650-5:2020 determines the procedures that will help to reduce the danger of divergence which could affect the security of the built asset, the users of the built asset, and the benefits of the built asset (CPNI, 2020). By applying proper cybersecurity efforts, organisations look to guarantee that they accomplish and maintain the security targets of their own organisation (Boyes, 2014). Kim and Solomon (2018) classified the security concepts as:

Confidentiality: Refers to who authorised a person's access to information.

Integrity: Refers to ensuring the procedures about modifying and deleting information as well as authentication.

Availability: Refers to ensuring that the use of and access to information is only granted to authorised persons (see Section 3).

Recommendation 3: Ensure evolving digital twin and future city standards fully integrate support for IoT and cybersecurity considerations. The key considerations are:

Developing a smart application architecture by incorporating a new layer called a security layer that secures HyperCat which gives data open sources with traversal links at whatever potential; numerous systems will possibly give resources or catalogues only to authenticated users (Howell and Rezgui, 2018). Consequently, where resources are discoverable yet unavailable without authentication, authentication data can be given to users (Wang, Sun and Hutchison, 2016).

The importance of smart grid security (Sridhar, Hahn, and Govindarasu, 2012); the industry supports ICT that is able to communicate data via the IoT which presents key cybersecurity concerns. Also, DTs provide potential outcomes of cyber-physical systems (CPSs) (Eckhart and Ekelhart 2018). The CPS relies on a sensor network. Therefore, the security of a sensor network is an urgent necessity and the encryption algorithms are a standard of cybersecurity, e.g. AES and 3DES that ensure correct permissions for actors and security across the different scales of the built environment (Howell et al., 2017) (see Section 4.2).

Recommendation 4: Integration of existing built environment data standards with cybersecurity concepts.

Integration of built environment data with the IoT produces a digital twin of a real building in a built environment and can be used to simulate the construction process, thereby enabling performance to be assessed and the key influence factors to be identified such as cybersecurity threats. The asset's security could be placed at risk because intellectual property could be lost or the systems associated with the asset could be breached (Tao and Qi, 2019; Kirstein and Ruiz-Zafra, 2016) (see Section 4.1).

Providing a cybersecurity layer with built environment data that covers DTs, IoT and information models (including BIM) for the built environment presents a requirement to develop a reference architecture for a cybersecurity layer. DTs should be able to secure the identity and protection of their genuine twin. This would require the utilisation of cryptography algorithms (see Section 4.1).

6. CONCLUSION

This paper conducted a systematic review of digital twin research in the building environment and enhanced IoT in information models in order to clarify its definition and use in manufacturing applications. In this paper, the scientific literature clarified how digital twins for Industry 4.0 could be useful in the manufacturing field, ranging from physical objects (i.e. IoT) to information models (including BIM). Also, this paper analysed eight Reference Zones in Europe that have been on the front line of IoT advancement. Based on the analysis and the scientific literature, research gaps were specified regarding the IoT, identifying a number of associated challenges and topmost among these being the security threat. In this paper, several solutions have been recommended to secure the building environment to enhance IoT and digital twins to realise the goal of developing smart buildings in a safe environment.

The primary limitation of this paper is that the recommendations have been derived solely based on academic literature which does not give the full picture of a rapidly evolving field of security, digital twins and cyber-physical systems, missing industrial practice and innovation that may not appear in academic literature. To overcome this limitation in future work, this study could be expanded to consider the following recommendations:

- Case studies should be gathered from industry to further understand the current use of CPS, IoT and digital twins in industry. Future research may empirically explore more complex capabilities enabled by digital twins and their effects on the performance of the built environment by comparing multiple smart cities and benchmarking cybersecurity risks and public policies caused by digital twins to understand the realisation or underperformance of smart cities.
- Industry should be involved by conducting a survey to fill in the knowledge gaps regarding the barriers faced in industrial organisations that depend on CPSs. The survey should focus on the use of cyber-physical/IoT systems that are in use in industry in the built environment. It should be targeted at participants working in industrial organisations to gather full knowledge of the security threats faced by CPSs in both the IoT and digital twins and the extent to which organisations require specialised tools to address security vulnerabilities.

REFERENCES

Abanda, F. H., Tah, J. H. M. and Keivani, R. (2013) 'Expert Systems with Applications Trends in built environment semantic Web applications: Where are we today?' *Expert Systems With Applications*, 40(14), pp. 5563–5577. doi: 10.1016/j.eswa.2013.04.027.

Ameri, F. and Patil, L. (2012) 'Digital manufacturing market: a semantic web-based framework for agile supply chain deployment', pp. 1817–1832. doi: 10.1007/s10845-010-0495-z.

Autodesk (2003) 'Building Information Modeling for Sustainable Design', *Autodesk White Paper*, pp. 1–13.

Bizer, C. and Berlin, F. U. (2008) 'Linked Data: Principles and State of the Art', (April).

Boje, C. *et al.* (2020) 'Towards a semantic Construction Digital Twin: Directions for future research', *Automation in Construction*, 114(November 2019), p. 103179. doi: 10.1016/j.autcon.2020.103179.

Bosch, A., Volker, L. and 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.

Boyes, H. (2014) 'Building Information Modelling (BIM): Addressing the Cyber Security Issues', *Iet*, pp. 1–12. doi: 10.1049/etr.2014.9001.

Boyes, H. (2015) 'and the Built Environment', *IT Professional*, 17, pp. 25–31. doi: 10.1109/MITP.2015.49.

Cha, H. S. and Lee, D. G. (2015) '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.

Cisco (2014) 'The Internet of Things Reference Model', *white paper*, pp. 1–12.

CityVerve. (2019). *CityVerve Manchester | Manchester's Smart City Demonstrator*. [online] Available at: http://www.cityverve.org.uk [Accessed 6 Aug. 2019].

CPNI (2020) 'Introduction 19650-5:2020 To BS EN ISO', *Center for the Protection of National Infrastrutcure*.

Dang, H. B., Abramovici, M. and Go, J. C. (2016) 'CIRP Annals - Manufacturing Technology Semantic data management for the development and continuous reconfiguration of smart products and systems', 65, pp. 185–188.

Das, M., Cheng, J. C. P. and Kumar, S. S. (2014) '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.

Dasgupta, A., Gill, A. and Hussain, F. (2019) 'A conceptual framework for data governance in IoT-enabled digital IS ecosystems', *DATA 2019 - Proceedings of the 8th International Conference on Data Science, Technology and Applications*, (Data), pp. 209–216. doi: 10.5220/0007924302090216.

Dave, B. *et al.* (2016) 'Automation in Construction Opportunities for enhanced lean construction management using Internet of Things standards', *Automation in Construction*, 61, pp. 86–97. doi: 10.1016/j.autcon.2015.10.009.

Demkovich, N. and Yablochnikov, E. (2018) 'Multiscale Modeling and Simulation for Industrial Cyber-Physical Systems', *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*. IEEE, pp. 291–296. doi: 10.1109/ICPHYS.2018.8387674.

Digitransit. (2019). *Digitransit*. [online] Available at: https://digitransit.fi/en [Accessed 6 Aug. 2019].

Ding, K. *et al.* (2018) '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)*, pp. 1–5. doi: 10.1109/ICNSC.2018.8361339.

Directorate, T. *et al.* (2006) 'No Title Roadmap to Secure Control Systems in the Energy Sector'.

Eckhart, M. and Ekelhart, A. (2018) 'Towards Security-Aware Virtual Environments for Digital Twins', pp. 61–72.

Eschenauer, L. and Gligor, V. D. (2002) 'A Key-Management Scheme for Distributed Sensor Networks', pp. 41–47.

Fazio, M. and Celesti, A. (2015) 'Exploiting the FIWARE Cloud Platform to Develop a Remote Patient Monitoring System', pp. 264–270. doi: 10.1109/ISCC.2015.7405526.

Generation, D. and Storage, E. (2011) *IEEE 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*.

Gha, A. *et al.* (2017) '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.

Gubbi, J. *et al.* (2013) 'Internet of Things (IoT): A vision, architectural elements, and future directions', *Future Generation Computer Systems*, 29(7), pp. 1645–1660. doi: 10.1016/j.future.2013.01.010.

Guerriero, A. *et al.* (2017) 'BIM-enhanced Collaborative Smart Technologies for LEAN Construction Processes', pp. 1023–1030.

Haag, S. and Anderl, R. (2018) 'Digital twin – Proof of concept', 15, pp. 64–66. doi: 10.1016/j.mfglet.2018.02.006.

Howard, R. (2008) 'Building information modelling – Experts' views on standardisation and industry deployment', 22, pp. 271–280. doi: 10.1016/j.aei.2007.03.001.

Howell, S. and Rezgui, Y. (2018) 'Beyond BIM'.

Howell, S. *et al.* (2017) '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.

Huang, Y. *et al.* (2009) 'Understanding the physical and economic consequences of attacks on control systems', *International Journal of Critical Infrastructure Protection*, 2(3), pp. 73–83. doi: 10.1016/j.ijcip.2009.06.001.

Jung, M., Reinisch, C. and Kastner, W. (2012) '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.

Karlof, C. (2003) 'Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures'.

Kim, D. and Solomon, M.G. (2018) *Fundamentals of Information Systems Security: Print Bundle*. Jones & Bartlett Learning.

Kirstein, P. T. and Ruiz-zafra, A. (2016) 'Use of Templates and The Handle for Large-Scale Provision of Security and IoT in the Built Environment', pp. 1–10.

Luk, M. *et al.* (2007) 'MiniSec: A Secure Sensor Network Communication Architecture CBC-enCrypton, eq andly', pp. 479–488.

Miorandi, D. *et al.* (2012) 'Ad Hoc Networks Internet of things: Vision, applications and research challenges,' *Ad Hoc Networks*, 10(7), pp. 1497–1516. doi: 10.1016/j.adhoc.2012.02.016.

Mitchell, R., Chen, I. and Tech, V. (2014) 'A Survey of Intrusion Detection Techniques for Cyber-Physical Systems', 46(4).

Negri, E., Fumagalli, L. and Macchi, M. (2017) 'A review of the roles of Digital Twin in CPS-based production systems', 11(June), pp. 939–948. doi: 10.1016/j.promfg.2017.07.198.

Opengroup.org. (2019) *Open Messaging Interface (O-MI), an Open Group Internet of Things (IoT) Standard*. [online] Available at: http://www.opengroup.org/iot/omi/index.htm [Accessed 16 Aug. 2019].

Parno, B. *et al.* (2006) 'Secure Sensor Network Routing: A Clean-Slate Approach'.

Perrig, A. *et al.* (2002) 'SPINS: Security Protocols for Sensor Networks', pp. 521–534.

Perrig, A., Stankovic, J. and Wagner, D. (2004) 'Security in wireless sensor networks.'

Rajput, Q. and Haider, S. (2011) 'Procedia Computer A comparison of ontology-based and reference-set-based semantic annotation frameworks', *Procedia Computer Science*, 3, pp. 1535–1540. doi: 10.1016/j.procs.2011.01.045.

Rezgui, Y., Beach, T. and Rana, O. (2013) 'A governance approach for BIM management across lifecycle and supply chains using mixed-modes of information delivery', *Journal of Civil Engineering and Management*, 19(2), pp. 239–258. doi: 10.3846/13923730.2012.760480.

Shin, D. (2009) 'Ubiquitous city: Urban technologies, urban infrastructure and urban informatics', 35(5), pp. 515–

526. doi: 10.1177/0165551509100832.

Sridhar, S., Hahn, A. and Govindarasu, M. (2012) 'Cyber – Physical System Security for the Electric Power Grid', *Proceedings of the IEEE*, 100(1), pp. 210–224. doi: 10.1109/JPROC.2011.2165269.

Steinmetz, C. and Rettberg, A. (2018) 'Internet of Things Ontology for Digital Twin in Cyber Physical Systems'. doi: 10.1109/SBESC.2018.00030.

Synchronicity-iot.eu. (2019) *Synchronicity* |. [online] Available at: https://synchronicity-iot.eu/ [Accessed 6 Sep. 2019].

Tang, S. *et al.* (2019) '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*, 101(January), pp. 127–139. doi: 10.1016/j.autcon.2019.01.020.

Tao, F. *et al.* (2014) 'IoT-Based Intelligent Perception and Access of Manufacturing Resource Toward Cloud', 10(2), pp. 1547–1557. doi: 10.1109/TII.2014.2306397.

Tao, F. and Qi, Q. (2019) 'New IT Driven Service-Oriented Smart Manufacturing: Framework and Characteristics', *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 49(1), pp. 81–91. doi: 10.1109/TSMC.2017.2723764.

Technology, N. I. of S. (2017) 'FIPS PUB 201-1 Personal Identity Verification (PIV) of Federal Employees and Contractors', 2.

Tuegel, E. J. *et al.* (2011) 'Reengineering Aircraft Structural Life Prediction Using a Digital Twin', 2011. doi: 10.1155/2011/154798.

Turk, R. J. (2005) 'Cyber Incidents Involving Control Systems', (October).

Wang, Z., Sun, J. and Hutchison, D. (2016) *Semantic Technology*.

Yang, Q. Z. and Zhang, Y. (2006) 'Semantic interoperability in building design: Methods and tools', 38, pp. 1099–1112. doi: 10.1016/j.cad.2006.06.003.