 doi:10.20944/preprints202005.0213.v1

Construction Cybersecurity and Critical Infrastructure Protection: Significance, Overlaps, and Proposed Action Plan

[Position Paper]

Borja Garcia de Soto[1], Alexandru Georgescu[2], Bharadwaj Mantha[1], Žiga Turk[3], and Abel Maciel[4]

[1]New York University Abu Dhabi, United Arab Emirates
[2]National Institute for Research and Development in Informatics, Romania
[3]University of Ljubljana, Slovenia
[4]University College of London, UK

garcia.de.soto@nyu.edu; alexandru.georgescu@ici.ro; bmantha@nyu.edu; ziga.turk@fgg.uni-lj.si; a.maciel@ucl.ac.uk

Abstract

The umbrella concept for the current efforts to digitize construction is known as Construction 4.0. One of its key concepts is cyber-physical systems. The construction industry is not only creating increasingly valuable digital assets (in addition to physical ones) but also the buildings and built infrastructures are increasingly monitored and controlled using digital technology. Both make construction a vulnerable target of cyber-attacks. While the damage to digital assets, such as designs and cost calculations, may result in economic damage, attacks on digitally-controlled physical assets may damage the well-being of occupants and, in worst-case scenarios, even damage (or death) to the users. The problem is amplified by the emerging cyber-physical nature of the systems, where the human checks may be left out. We propose that construction learns from the work done in the context of critical infrastructures (CI). First, a lot of CI is construction-related, and the process of designing and building it must be secured accordingly. Second, while most assets may not be critical in the CI sense, they are critical to the operations of a business and the lives of citizens. In the end, we recommend some steps so that well-established processes of critical infrastructure protection trickle down to make Construction 4.0 and the built environment more cyber-secure. With that in mind, we describe the possible inclusion of Construction 4.0 considerations into existing critical infrastructure protection (CIP) frameworks with minimum frictions. We also propose some suggestions regarding possible future courses of action to improve the increasingly vulnerable cyber-security environment of the built environment across all life cycle phases - design, construction, operation, maintenance, and end of life.

Keywords: BIM; construction; critical infrastructure; cybersecurity; cyber-physical systems; digital twin; EPCIP; Industry 4.0

1. Introduction and motivation

Construction is increasingly digital. Designs and plans are created using digital tools; they are stored on digital media (such as Clouds and Common Data Environments) and exchanged over the internet. The products of the information-intensive phases of construction are increasingly valuable. They contain intellectual property (IP) much more valuable outside of the project context in which they were created, and they contain information that can be reused, not to mention commercial and trade secrets. With this

 doi:10.20944/preprints202005.0213.v1

trend, construction is catching up with other industries that have already recognized the value of their digital assets.

Recently, digitalization is moving beyond the information processes. Construction 4.0 is an umbrella concept for the current efforts to digitize construction, and its key concept is cyber-physical systems (Klinc and Turk, 2019). Essentially, these are systems where material assets are monitored and controlled using digital technology with little or no human intervention. For example, ground motion in an earthquake area is monitored, and the structural systems and counterweights in the building respond to the ground acceleration; or water quality is monitored, and automatically chlorine disinfectant is added into the system; or a robotic excavator is doing its job with no humans present. While some such systems existed in the past, they are getting ubiquitous (e.g., Kanan et al., 2018), are connected to the internet (e.g., Tang et al., 2019), and are autonomous (e.g., Mantha et al., 2018). As such, they are much more vulnerable to cyber-attacks (Mantha et al., 2020; Mantha and Garcia de Soto, 2019).

Cyber-attacks on purely digital assets of other industries can lead to damage in the digital world and economic damages. However, due to the essential material nature of construction and its essential role in vital infrastructure, cyber-attacks in construction may potentially lead to physical property damage and even loss of human life. What is known as critical infrastructure is largely a product of the construction industry (i.e., the result of a construction project), or an asset that is, technically, managed by construction asset management firms.

Beginning in 2004, the European Union has pursued Critical Infrastructure Protection (CIP) as a framework for managing the risks of complex and interdependent socio-technical systems. With the release of Directive 114/2008 (Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection), the European Programme for Critical Infrastructure Protection (EPCIP) assumed an important role in managing the systemic energy, cyber, transport and space vulnerabilities of an “ever-closer Union.” With specific projects, such as the integrated European electricity and gas network, or the development of European transport corridors, the European Union is generating a new security environment, in which risks, vulnerabilities, and threats gain trans-border valences and become increasingly hard to understand, manage and mitigate by jurisdictionally limited national authorities. EPCIP must become not only deeper but also wider, designating European Critical Infrastructures (ECI) in health, finance, and other areas hitherto managed exclusively at National levels.

Given the continuing improvement of EPCIP and the anticipated overhaul of the system, this position paper advances a perspective on the importance of National and European action to mitigate the evolving security situation caused by the Construction 4.0 paradigm. Like the Industry 4.0 paradigm, Construction 4.0 is transforming this vital sector through digitization, automation, and other cyber-mediated processes in all aspects, from design to construction and operation (Mantha et al., 2020; Garcia de Soto et al., 2019; Klinc and Turk, 2019). The position presented in this paper is that the CIP frameworks at the levels of the EU and the Member States are a useful tool for addressing the impact of systemic changes in the construction sector caused by the shift towards digitalization and automation. This position was forged during the 1st Workshop on Cybersecurity in Construction 4.0 that took place on 2-3 February 2020 in New York University Abu Dhabi (NYUAD).

In this position paper, we describe the possible inclusion of Construction 4.0 considerations in the CIP framework with minimum frictions and sketch some suggestions regarding possible future courses of

 doi:10.20944/preprints202005.0213.v1

actions to ameliorate the increasingly vulnerable cyber-security environment of the built environment across all life cycle stages - design, construction, operation, maintenance, and end of life.

2. Significance and relevance of the construction sector

The construction industry is an essential driver for the economy of a country and accounts for a considerable amount of its GDP (World Economic Forum, 2016). According to the Global Construction 2030 report, the volume of construction output will grow to $15.5 trillion worldwide by 2030 (85% increase from 2014), with China, India and the US accounting for a significant part of that growth, and will account for about 14.7% of the global GDP[1,2]. Although these projections will be affected by the impacts caused by COVID-19, the contributions of the Architecture, Engineering, Construction, and Operations (AECO) industry to the economy of a country will continue to be essential and hover at about 10% of the GDP of developed nations. It should be pointed out, however, that most of the remaining 90% of the GDP is created in buildings and/or using other assets of the built environment. Any disruption of those assets would likely have an economic impact that would be orders of magnitude greater than the value of the assets.

Although it is expected that new technologies will have a profound change to the industry, the implications and potential benefits of Construction 4.0 are still difficult to assess, and its repercussions to the different stakeholders, critical components of the supply chain, and the different phases of the lifecycle of construction projects are not yet fully understood. Of particular concern is the general lack of awareness of understanding related to the cybersecurity implications when switching to a connected and digital environment. To address that, the authors have prepared a questionnaire[3] to gauge the awareness and concerns in the industry. This position paper aims to layout key cybersecurity elements to enable the full potential of Construction 4.0 and define research areas needed to pave the roadmap for the future of the construction industry and successful development of a secured and trusted Construction 4.0.

The introduction of the General Data Protection Regulation (GDPR) in Europe in May 2018[4] requires improved cyber-security for the operators of essential services, which includes construction projects using digitally built environments, including digital infrastructure (i.e., smart cities) and intelligent buildings. In the UK, the Publicly Available Specification (PAS) 1192-5 (BSI, 2015) provides a framework to ensure that information is shared in a security-minded way and to enable the reliability and security of digitally built assets, keeping in mind that the data stored about built assets could be used by those with malicious intent (IET, 2013). The Institute of Engineering and Technology report titled 'Resilience and Cyber Security of Technology in the Built Environment,' states that: *"Unauthorised access to BIM [Building Information Modeling] data could jeopardise security of sensitive facilities, such as banks, courts, prisons and defence establishments, and in fact most of the Critical National Infrastructure."* (Boyes, 2013). The 'Code of Practice for Cyber Security in the Built Environment' (IET, 2014) addresses how cybersecurity should be considered throughout a building's life cycle with a focus on building-related systems and all connections to the wider cyber environment. The National Institute of Standards and Technology (NIST) developed a cybersecurity framework for assessing and managing critical infrastructure. Though the framework emphasizes Identification and Detection as primary steps of cyber risk management, which are critical

[1] https://www.ice.org.uk/ICEDevelopmentWebPortal/media/Documents/News/ICE%20News/Global-Construction-press-release.pdf

[2] https://policy.ciob.org/wp-content/uploads/2016/06/GlobalConstruction2030_ExecutiveSummary_CIOB.pdf

[3] The questionnaire can here: https://nyu.qualtrics.com/jfe/form/SV_ellAtgTZTMIC0cJ

[4] https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 May 2020 doi:10.20944/preprints202005.0213.v1

components of threat modeling, it does not detail cyber threats and vulnerabilities in construction (NIST, 2018). However, these guidelines have limitations. They a) focus only on building systems and data exchange security in the built environment, b) neglect bidding, planning, design, and construction phases, and c) do not investigate potential risks and impacts during the operation and maintenance phase by activities/actions performed during early stages of construction.

2.1 Why is construction different?

The construction sector possesses large amounts of data that are created in dynamic, multi-stakeholder settings in a cooperation of several businesses. Some examples include the information generated during the bidding process, engineering designs, calculations and specifications, pricing, profit/loss data, employee information (including intellectual property), and banking records, to name a few. In most cases, this data contains highly confidential or proprietary information; yet, construction companies are significantly vulnerable (Mantha and Garcia de Soto, 2019) and should be proactive in implementing strategies, and educate employees to secure data. However, the reality is that awareness and investment in high-level security in the industry are still very low, making this industry susceptible and particularly attractive to hackers. Therefore, a key element for the successful transition into digitalization of the industry is the consideration of cybersecurity.

In some aspects, the challenges construction companies are encountering are not significantly different from those faced by other industries that have already adopted new technologies and are at a more advanced level of digitalization. However, some cyber risks are specific to the built environment, due to the peculiarities of the different phases of construction projects (with a significant amount of data being generated), the number and dynamism of stakeholders, the long supply chains, and, last but not least, the importance of the built environment for health and lives of the citizens.

Pre-design/bidding phase

During the tendering phase, or the bidding process, electronic tendering is becoming the standard, as digital procurement platforms save time and money; however, highly confidential or proprietary information such as project specifications, pricing, profit/loss data, employee information, and banking records could be exposed.

Planning and design phase

During the planning and design phases, an attack on the Building Information Model (BIM) could compromise essential project information, including personal data. It could also prevent access to the model or corrupt the project information, which might lead to construction issues in subsequent project phases (e.g., construction, operation and maintenance). It may steal valuable intellectual property. Contrary to on-paper designs and 2D digital designs, pieces of building information models are useful and reusable outside of the context of the project in which they were developed.

Construction/execution phase

New technology is also allowing the creation of smart and automated construction sites. They might include sensors equipped on the construction equipment or materials, a network of cameras to monitor construction progress in real-time, wearable technology to minimize safety hazards or robotic systems (connected to sensors to capture information that is fed to a control system) to assist workers or conduct construction activities autonomously. Hijacked heavy autonomous construction equipment could pose

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 May 2020 doi:10.20944/preprints202005.0213.v1

dangers to lives (Andersson et al., 2019). Also, to promote transparency and improve communication, digital platforms are used to allow different project participants to access project data at the same time from different locations (currently using the combination of BIM and common data environment (CDE)) leading to similar issues as discussed in the previous subsection

Operation and Maintenance (O&M) phase

This phase accounts for a significant portion of the cost of a built asset/infrastructure, and critical data is needed during this phase to ensure that the facility is operated and maintained correctly. During the operation and maintenance phase, new technology allows the possibility to move from rigid building management systems (BMSs) to more flexible ones using sensors that interconnect different elements through the IoT. BMSs are particularly vulnerable and can compromise not only the performance of the building or infrastructure being managed, but also the corporation or owner, as in the case of Target back in 2013 when hackers gained entry through a vendor-access HVAC (heating, ventilation, and air conditioning) building control system (Shu et al., 2017).

Stakeholders and supply chain

The exposure to cyberattacks in the construction industry is exacerbated by the number of participating stakeholders and long supply chains, of which 95% are small and medium-sized enterprises (SMEs) with limited resources devoted to IT. While most general contractors and large subcontractors have cyber-security policies, many smaller subcontractors that participate in projects do not (Garcia de Soto, 2019); nevertheless, they may have access to the information assets of other partners. The risks of cyber-attacks thus extend to the different project phases, as previously discussed.

These challenges are particularly unique to construction when compared to the other industries, such as healthcare, electronics, and aerospace because of the following reasons:

- Dynamic workplace and workforce: Unlike other industries, construction is very dynamic with an ever-evolving pace of work, workplace, and workforce. That is, the workplace evolves with the progress of the project, along with the personnel working on the project. For example, before the project begins, the project personnel's workplace is an offsite office, as the project starts, part of the personnel is moved to a temporary onsite office (trailer) and eventually, they will be part of the project workspace. In addition, the ever-changing workforce makes it difficult to educate and train employees of the best cybersecurity practices. This change in the workforce is due to the highly fragmented nature of construction employees, which are sub-contracted workforce for the most part.
- Interoperability issues: Due to the complex nature of the projects, information needs to be shared among different multidisciplinary teams across various platforms. Subsequently, it does not usually exist a common platform that can be used to access information regarding different trades such as civil, mechanical, and electrical. Thus, each of these models cannot be accessed through a central secure server but needs to be individually shared as separate native files using different software. Some of these problems are addressed when using open BIM and CDE, but in practice, each party has its own software applications used for design.
- File sharing: Due to the interdependencies and involvement of multiple sub-contracted parties, information exchange, which in many cases includes confidential and sensitive data, occurs even

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 May 2020 doi:10.20944/preprints202005.0213.v1

outside the company's network (e.g., using personal computers). Besides, most of the devices used on construction sites are personal and are not validated or monitored by the company.

- Socio-economic diversity: Construction workforce includes people belonging to different socio-economic classes, education levels, cultural backgrounds, and geographic locations, which causes varying levels of cybersecurity knowledge, awareness, and understanding. In addition, identifying each employee into distinct categories in order to restrict access to project data is not always a trivial task.

2.2 Overlap with CIP

Most of the existing Critical Infrastructure Protection (CIP) framework focuses on the O&M phase, which involves operation, retrofitting, and decommissioning. For the most part, CIP neglects the earlier phases discussed in the previous subsection. In the recent past, there has been an increased focus in resilience by design as a principle of CI, where the future infrastructure needs to be designed and built in the idea of:

- minimizing vulnerabilities,
- mitigating damage from the materialization of a negative event,
- ensuring graceful decline in infrastructure operation,
- ensuring reduced coupling between CI components and subsystems or between the particular CI and others,
- having failsafe, redundancies, flexibility and adaptability in operation,
- promoting the rapid resumption of normal levels of activity or an acceptable percentage of normal functioning, and
- preventing the alignment of breakages, which lead to cascading disruptions in a critical infrastructure system-of-systems, among others.

Nonetheless, most of the CIP still does not consider the different life cycle of a construction project as a whole. One exception is the heavily regulated sector of nuclear power plants, where there is already a focus on the security consequences of all the phases of the plant's life cycle – from site selection to design, construction, operation, maintenance, upgrading and decommissioning to the sourcing of fuel and the disposal of waste. The present position paper argues that the changes in the security environment generated by the Construction 4.0 paradigm warrants a similar approach to the protection of other types of infrastructure in general and most importantly the critical infrastructure across all the phase of its life cycle.

3. Construction 4.0 and its transformations

After a long history of under-digitization, the construction industry is making a shift towards digitization and automation due to rapidly growing information and communication technologies (ICT) such as 3D printing, blockchain, robotics, machine learning, drones, big data, the Internet of Things (IoT), artificial intelligence, predictive analytics, augmented reality, and gaming engines, to name a few. This is referred to as Construction 4.0, which is the construction industry's surrogate of Industry 4.0. The aim thus is to have connected cyber-physical systems at every stage in the life cycle of a construction project starting from the bidding phase, the operation and maintenance, to the end of life. If achieved, this will have the capability to transform the design, planning, construction, operation, and maintenance of the civil infrastructure systems, and have a positive impact on the overall project time, cost, and resources used.

For example, the adoption of digital twin technology assists in the creation of a digitally built environment, which can integrate the currently fragmented sector by having a digital replica with which all project participants can collaborate. This industry 4.0 concept has been known as BIM/CDE in construction. This also promotes transparency among the different phases of the lifecycle of construction projects. However, as the industry becomes more connected and digitized, the importance of cybersecurity becomes significant and should be considered by all the stakeholders and project participants.

3.1 Threats affecting Construction 4.0

The digitization inherent in the Construction 4.0 phenomenon has led to a transformation in the security environment of the AECO sector, which has become more challenging and more dynamic. The challenges associated with Construction 4.0 and cybersecurity have been described throughout this position paper, but we may say, in general, that the AECO sector has become exposed to the security dynamics of the cyber environment, with specific risks, vulnerabilities, and threats. There is a rich literature in the field; however, we will note that the AECO sector is almost never distinguished from other domains as an object of study to highlight the specifics of cybersecurity threats in the sector. This will have to change in the future.

In 2009, the European Security Research and Innovation Forum (ESRIF, 2009) produced a list of threats, many of them interconnected, that a European security agenda, both internal and external, would have to address. Among these, we find organized crime, cyber-attacks, terrorism, natural disasters, man-made disasters, and the unintended consequences of the introduction of new technologies. All of these are reflected in the cyber domain as a cross-cutting issue.

The threat environment of Construction 4.0 is complex, and its vulnerability to external threats and fragility to internal weaknesses is heightened by the relative opacity of the sector from a cybersecurity perspective in the existing literature, both academic and industry oriented. With this in mind, we will describe the security and threat environment with reference to the general cybersecurity issues.

The 2019 Internet Security Threat Report (O'Gorman et al., 2019), based on Symantec's Global Intelligence Network, a civilian threat collection network, notes the extraordinary dynamics of the threat environment. Even as ransomware was down 20%, enterprise ransomware grew by 12% year on year, and mobile ransomware grew by 33%. Supply chain attacks grew 78% from 2017 to 2018. Hinting at the growing financial dimension of cyber-attacks (even for state-sponsored actors), 48% of malicious attachments were office files, up from 5% in 2017, and a 1000% increase in malicious PowerShell scripts was also noted. At the same time, this report and others have noted a growing incidence of attackers "living off the land," exploiting vulnerabilities and systemic weaknesses rather than using malware to achieve their goals. This is of interest since Construction 4.0 presupposes an automatic increase in the exposure to such vulnerabilities, in addition to a larger surface of contact with the cyber domain for generalized exposure to cyber risks.

The 2019 Cyber Risk Outlook (Coburn et al., 2019) identifies key AECO-relevant trends such as Increasing *Exposure to Digital Attack and Disruption, Increasing Propensity for Cyber-Induced Business Interruption, Attacks on Digital Supply Chains, Growing Potential for Cyber-Physical Loss Events, Cyber Attacks Becoming Increasingly Political, and Changing Motivations of Threat Actors*. Not all of the developments are grim since companies are improving security standards, regulators are adapting, and law enforcement is also improving. It is important to acknowledge that Construction 4.0 organizations and processes will

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 May 2020 doi:10.20944/preprints202005.0213.v1

automatically be exposed to the negative trends, but will require targeted efforts to also experience the positive ones. The report does not include AECO in its taxonomy of economic domains affected by cyber, though elements of AECO can be found bundled in multiple areas. It does note that Construction is currently one of the least digitized sectors in terms of business processes, however the Construction 4.0 paradigm points towards rapid change in this regard. It also cites the following threats:

- Data exfiltration, whose impact is almost certainly underestimated in the AECO sector according to current methodologies which rely on counting mega-breaches of individual user data;
- Contagious malware, with ransomware replacing trojans as preferred attack vectors and increasing vulnerability through mobile devices and Internet-of-Things devices. In previous years, trends such as the commoditization of malware, accessible even to attackers without specialized knowledge, were noted;
- Financial theft, through fraud, transaction frauds and so on;
- Cloud outages stemming from concentration risks in the big four service providers. We would also note that concentration risks may also stem from manufacturers of automated and networked equipment, devices and software for the AECO industry;
- Distributed Denial of Service attacks. Given the profile of the most affected organizations, further research is required in the AECO industry, especially outside of the facilities management sector.

Lastly, the report notes that, despite improvements in the reporting of incidents and the capability to ensure rapid recovery, “median dwell times, the time it takes a corporation to notice it has been compromised, has steadily increased, and in 2018 averaged 101 days globally”.

We may conclude that, through Construction 4.0, the AECO industry is exposed to the full panoply of cyber threats and more research is needed to determine the specificities of the industry’s exposure, its behavior and the required policies and response on the part of the companies, as well as of regulators.

While we should not discount the dimension of complexity as a source of unintended and accidental disruptions, the current main focus is on the deliberate threats, especially given the variety and dynamism of the latter. The AECO sector has to contend with:

- Organized crime (local and trans-border)
- Lone wolves
- State actors and state-sponsored actors
- Ideological groups (sometimes state-sponsored) such as hacktivists
- Enemy within scenarios, either singular or multiple

The financial dimension of deliberate cyber-attacks is backed by political motivations, geopolitical, ideological, or instrumental (cybercrime as an enabler for terrorism and a tool for terrorist subversion). We cannot neglect the growing role of cyber-attacks in “hybrid warfare” or “new generation warfare” tactics and strategies, especially in the context of asymmetrical confrontation or “grey zone warfare” below the threshold of military response.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 May 2020 doi:10.20944/preprints202005.0213.v1

4. Technological responses to Construction 4.0 security

Measures to address security concerns raised by Construction 4.0 are mostly based on existing standards, particularly ISO 27001 (2013) and ISO 27032 (2012). However, in a digital economy where over 50 billion devices are communicating continuously, neither firewalls nor encryption alone can guarantee effective cyber-security (Wendzel, 2016). It is clear that a more robust systemic means of data integrity is required in the digital built environment. As a way to address the security issues related to Construction 4.0, technical responses have been implemented. The following are a couple of examples of the technical responses to address Construction 4.0 security.

4.1 Robotic Checkpointing to Secure Data Collection During Building Commissioning

Commissioning is the process of bringing something newly produced into working condition. It involves the verification of all the building systems (e.g., security controls, mechanical, electrical, and plumbing systems) to meet the desired design, quality, and safety standards and ensure proper performance in accordance with manufacturers' requirements to warrant their products. It is the responsibility of the respective contractors to ensure that the optimal desired functionality is achieved. To verify this, the owner usually hires an independent commissioning agent to oversee this process. The commissioning agent works closely with the contractor to address any identified issues during the verification process. Finally, a granting authority (e.g., government or private certified agencies) analyzes the performance of the different building systems before a certificate of occupancy is issued. This is done to certify the conformance and compliance of building systems in accordance with the building codes, laws, and local authority regulations, which essentially means that the building condition is suitable for occupancy or respective functional use according to a given rating.

In many cases, commissioning agents rely on the data provided by the owner or the contractor as they usually lack the time and resources to cross-verify the sensor data provided to them. However, due to motivating reasons for the facility owners and sensor network contractors, the data could be tampered at the sensor (by compromising the sensor) or at the display (by compromising the dashboard) or when the sensor data is in transit. A malicious owner or a rogue contractor could do this to obtain the certification faster and without fixing the violations. Alternatively, an employee in either entity could do this to damage their reputations. A malicious outsider could do this to gain control of the facility operations and demand ransom to restore normal functionality. The tampering could happen in different ways. For instance, the sensor hardware is compromised to output data that does not represent the actual sensed value, or the dashboard is compromised where the sensor outputs are incorrectly shown.

To address this issue and detect faulty or rogue sensors or deter a rogue insider, Mantha et al., 2020 suggested a randomized sensor check-pointing approach as a countermeasure. For this, they developed an autonomous multi-sensor fusing mobile robotic data collectors. This will address the cybersecurity challenges during the onsite data collection and verification process. Sensors on the robot are trustworthy compared to the sensors installed in the facility. A method is proposed to cross-check and verify the different parameters such as temperature, humidity, indoor air quality, light intensity, and occupancy gathered by the building management or automation system (BMS or BAS) by this trustworthy third-party robotic data collector. For details regarding the technical aspects of such a robotic data collector, refer to Mantha and Garcia de Soto (2019) and Mantha et al. (2020).

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 May 2020 doi:10.20944/preprints202005.0213.v1

4.2 Distributed Ledger Technologies (DLT) and collaboration

Soon after Deloitte's report highlighting prospective applications of blockchain in the public sector (Deloitte, 2016), studies by Kinnaird and Geipel (2017), Wang et al. (2017) and Turk and Klinc (2017) are among the firsts to identify the potentials of blockchain in relation to the different phases of construction projects and, in particular, to address some of the confidentiality issues raised by BIM Common Data Environments (CDEs). Further analysis of DLT and blockchain applications in the sector have been published by numerous reports in the industry (Reuters, 2018; Nguyen et al., 2019), reinforcing this trend.

Blockchain technology has the potential to provide a hacker-safe ecosystem for digital asset transfers (Turk and Klinc, 2017). It can be used to share sensitive digital information of an asset in a CDE environment in a secure way. The asset data (e.g., the BIM model) can be converted into a block representing a digital transaction of asset data, and there can be stakeholder interaction within a federated CDE environment as they receive a tracked record of the individual transaction created by the nodes sharing the block (Pärn and Garcia de Soto, 2020). Yet, DLT does not offer the immutability of the blockchain, but in contrast, it offers vastly superior synchronization time of a ledger of publicly shared, permissioned, or private transactions. The formulation of DLT as a blockchain, on the other hand, brings new functionalities in the many phases of a project, from design to end of life, but the consensus mechanism of many blockchains limits their transaction speed dramatically.

More recently, blockchain applications such as smart contracts are thought to be the key technology for improving collaboration and management of construction teams and enhance traceability during projects, reducing cash flow issues often experienced by all tiers of contractors and suppliers (Maciel, 2020). While blockchain technology is mostly aimed at solving the issues of trust, it provides a resilient framework for traceability and responsibility mechanics in the sector. However, smart contracts are code, and as such, they are exposed to the same risks inherent to software development; therefore, standard cybersecurity advice (e.g., doing a risk assessment to address potential breaches) also applies with blockchain (Horvath et al., 2018).

It is expected that blockchain will provide the mechanism for proof of authorship of construction digital assets in the preconstruction phase. This represents a significant leap from current BIM practices where the interaction with the federated BIM is envisioned to be more strictly regulated and could deter potential theft of information and protect Intellectual Property (IP). Design for Manufacturing (DfM) and digital fabrication increases the rate of dissemination of digital assets, urging for new measures for IP protection. The IP implications of the development of industrial 3D printing (Mendis et al., 2020) clarify how the existing IP framework needs to be revised, also identifying potential challenges for the additive manufacturing sector in Europe.

Currently, it is still very possible for project data to be illicitly downloaded and, more seriously, manipulated as part of fraudulent schemes such as the tampering of project costs in tendering packages and artificially fabricated design issues leading to project delays.

Cybersecurity issues become even more apparent and serious when we consider that BIM is the foundational database used for setting up building operations solutions and enabling smart cities. How to

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 May 2020 doi:10.20944/preprints202005.0213.v1

guarantee the data provenance in such complex administrative platforms? Many of the shared parameters used in IoT enable BMS are derived from COBie files exported from BIM federated models.

Some blockchain solutions have been described and proposed for BIM CDE (Ye et al., 2018), whereby building activity is blockchained at source, complementing BIM journaling mechanisms. These new methods aim to mitigate the cyber-physical disconnect of accountability in the decision-making processes at preconstruction, construction, and operation phases, adding resilience to the traceability of actors and digital assets in BIM processes. Lamb (2018) surveys some of these implications, and more recently working prototypes of blockchain-based Smart Contracts for BIM have been developed and demonstrated to show how contractual RFIs (Request for Information) can be linked directly to BIM object geometry as BIM models are developed[5] (Maciel 2019a, 2019b, 2020).

5. Overview of CIP and EU efforts

At the basis of the functioning of any society lies a foundation of interdependent and complex systems composed of both technical and organizational components called infrastructures, which operate together as part of a system-of-systems. These infrastructures are composed of roads, railways, pipelines, power plants, but also markets, public administration, laboratories, and research facilities. Some of these infrastructures are so important to the functioning of a society that they may be termed critical, in that their disruption or destruction would cause significant casualties, loss of life, material losses and loss of trust and prestige.

The European Union defines Critical Infrastructures (CI) as an *"asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions"* (Council Directive, 2008). In addition to National CIs, which are under the purview of National authorities, there are also European CIs, which affect two or more Member States, and are under the purview not just of the host states, but also of the European Programme for Critical Infrastructure Protection.

Critical Infrastructures are characterized by (inter)dependencies of various types (geographic, physical, technical, cybernetic/informational, social and political) and by their tendency to generate complex systems with emergent and ambiguous behaviors that generate potentially dangerous phenomena such as cascading disruptions and unanticipated threats (Bouchon, 2006).

In addition to various directives, regulations, and communications pertaining to different relevant sectors or categories of threats (hybrid warfare, cybersecurity, etc.), there are a number of main European documents of reference regarding CIP over the years, some of them are listed below.

- COM(2004)702 – EU Communication from the Commission to the Council and the European Parliament - Critical Infrastructure Protection in the fight against terrorism[6];
- COM(2005)576 – Green paper on a European Programme for Critical Infrastructure Protection[7];

[5] Construction Blockchain Conference 2019 [https://www.constructionblockchain.org/2019]

[6] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:EN:PDF

[7] https://ec.europa.eu/transparency/regdoc/rep/1/2005/EN/1-2005-576-EN-F1-1.Pdf

- COM(2006)786 – EU Communication from the Commission on a European Programme for Critical Infrastructure Protection[8];
- Council DIR 2008/114/EC – Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection[9];
- COM(2009)149 – Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection -"Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"[10];
- COM(2011)163 – Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection -"Achievements and next steps: towards global cyber-security"[11];
- SWD(2012)190 – On the review of the European programme for critical infrastructure protection (epcip)[12];
- SWD(2013)318 – On a new approach to the European Programme for Critical Infrastructure Protection - Making European Critical Infrastructures more secure[13].

Among the ones listed above, Directive 114/2008 is probably the most important. EPCIP also advanced through documents such as EU 2016/1148[14] – the Directive on security of network and information systems (NIS Directive).

The Member States (MS) of the EU have an obligation to transpose its Directives into National law and at least meet if not exceed the minimum levels of CIP security and best practices recommended by the EU. In practice, this has not led to full convergence of organizational systems, legislation, division of authority, or even taxonomies of critical infrastructures, as well as definitions. CIP has become, however, a principal concern of all EU Member States. This involves the identification and designation of the critical infrastructure, the regulation of the functioning of its security apparatus, clear lines of communication with MS authorities, and, where necessary, with European authorities and other Member States and exchanges of information.

The constant and consistent development of EPCIP parallels that of national systems, where a growing taxonomy of CI is taken into account as the vulnerabilities from a wide variety of interconnected systems becomes apparent, both in the day to day functioning, as well as a direct or indirect result of systemic shocks (Bouchon et al., 2006) such as the SARS-CoV-2 Pandemic.

Construction is addressed twice in the context of critical infrastructures. First, a lot of it was built and is managed by the construction industry. But more importantly, while the large majority of the built

[8] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF

[9] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

[10] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF

[11] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF

[12] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/pdf/policies/crisis_and_terrorism/epcip_swd_2012_190_final.pdf

[13] https://ec.europa.eu/transparency/regdoc/rep/10102/2013/EN/10102-2013-318-EN-F1-1.PDF

[14] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 May 2020 doi:10.20944/preprints202005.0213.v1

environment is not considered critical infrastructure for the society as such, it is still very important infrastructure for businesses and citizens. We believe everyone can learn from how states manage truly critical infrastructure and implement those procedures to infrastructures critical to them.

6. Construction 4.0 in CIP for Europe and for Member States

The current approach is to have National authorities identify and designate National and European critical infrastructures in accordance with a series of quantitative and qualitative criteria. From a Construction 4.0 perspective, we argue that:

- normal accidents, which are random disruptions due to complexity and unintended system interactions and behaviors during the course of normal operations,
- systemic weaknesses due to errors of design and building philosophies, and
- deliberate threats such as those posed by state actors and their proxies engaged in hybrid warfare…

… may affect an infrastructure from the design and building stage, before it has ever had the opportunity to become critical to the security of one or more Member States and before it has been integrated into a wider critical infrastructure system-of-systems.

Negative occurrences may result not only in vitiated functioning of the asset or system in question later on but also delays in the completion of the project or wider disruptions in its area on the basis of geographic, physical, and other interdependencies between the construction site and its surroundings. This is especially true when it comes to infrastructure being built in cities, which are an agglomeration of critical infrastructures and where all of the types of disruptions take place (Rinaldi et al., 2001), such as:

- Common cause disruptions, where multiple CI malfunction because of the same cause
- Escalating disruptions, where disruptions build on each other to reach unanticipated levels of harm
- Cascading disruptions, where disruptions reverberate throughout a system through the dependency links between different CI

This gap has always been present, but the cyber vulnerabilities of the Construction 4.0 paradigm make it imperative to address this issue by integrating it into an existing framework of security governance. Prior to the introduction of CIP, security governance already featured legislative and administrative frameworks for physical asset security, the protection of persons and of privileged information, and foresight measures diminishing the impact of disruptions such as interruptions in fuel and raw materials supply. CIP simply systematized these and offered a holistic view of the resulting CI system-of-systems that enabled a better measurement of risk, the anticipation of threat scenarios, and the formation of a toolbox with which to perform security governance processes, first from an all-hazards-approach and, afterward, from a resilience perspective. Therefore, we believe that existing CIP efforts, both at National and European levels, can accommodate the processes required to address systemic risks, vulnerabilities, and threats in the new security environment.

Our main purpose is to introduce, both for European and National CI, a new infrastructure category – the construction process of a potential critical infrastructure. This enables security decision-makers to respond to the future state of the CI system-of-systems, rather than just the current one. A future candidate for critical infrastructure status will be pre-designated as a CI or ECI even from the proposal

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 May 2020 doi:10.20944/preprints202005.0213.v1

stage, regardless of whether it will actually become a critical infrastructure once complete. This designation will be made by applying the existing criteria for CI designation[15] to the anticipated future functioning of the asset being built, as detailed in the business plan, the investment projections, and other relevant documentation. Therefore, a future port facility with a planned capacity will be pre-designated as a CI based on the systemic relevance of its planned capacity in the current methodology for CI designation. This pre-designation results in the designation of the project, from the design phase to the finalization of the construction work and delivery to the beneficiary, as a critical construction infrastructure.

The lead integrating organization (or prime contractor) for the construction site becomes the equivalent of the critical infrastructure owner/operator and must file an operator's security plan in accordance with existing rules or specialized rules that involve a more frequent updating of the security plan due to the steadily transforming nature of the construction site as it heads towards completion.

Aside from the evolving nature of the CI construction site, another difference when compared to the classical CIs stems from the challenges of the organizational make-up. The prime contractor takes on the role of CI operators for the duration of the existence of the project until it is complete, but the prime contractor coordinates an ad-hoc assembly of specialized companies and subcontractors formed for this particular project and potentially numbering in the thousands. This is still a valid and relevant approach, as complex system theory allows us to delineate a system of any given complexity so long as there is a system boundary that differentiates the complex system from the surrounding environment (not just in a physical sense) (Keating et al., 2015). The challenge and the justification for the extra governance capacity of the CIP framework lie in the disparate security standards (especially in cyber) of all of the contractors working onsite. It will require new instruments and methodologies to adequately assess the cyber vulnerabilities of such an assembly and to mitigate these in order to ensure site security. This is in contrast to classical CI, where there is an operator (who is sometimes the owner) who is the sole and permanent CI protection agent, at least until the CI or critical asset, most of which are owned and operated by private entities, passes into other hands. The nature of the consortia executing important constructing projects (civil, industrial, energy, etc.) with the capacity of becoming critical infrastructures presents specific challenges.

The construction site as CI adaptation may require other specific instruments, such as compliance with mandatory cybersecurity standards for all contractors, or becoming subject to a security audit. Future research into the subject may have to also deal with the impact which added security regulations from the CIP system will have on overall cost and complexity and establish policies for providing cost-effective regulation.

The security liaison officer (SLO) system, where the CI, the regulatory authority, the highest national level CIP authority and the European authority all have officers responsible for the exchange of relevant information, may have to be adjusted for the construction site critical infrastructure. Rather than being a high ranking member of the Security Department as close as possible in the hierarchy to the executive suite of the owner/operator, the SLO for construction site critical infrastructure may be directly under the particular Project Director, since companies may be involved in multiple projects, each of them being a pre-designated CI.

[15] Possibly with changes, based on relevant research in this area.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 May 2020 doi:10.20944/preprints202005.0213.v1

Once the project is complete and has been handed off to the beneficiary who will own it and operate it (possibly through a third party facility manager), the site loses its status, and the regulating national authority must go through the normal identification and designation process for a critical infrastructure. The construction section may remain involved, through its facilities' management branch, or through the issues of maintenance and upgrade, but these are already included in the CIP framework.

The benefit of the proposal advanced in this position paper is that it addresses an important gap in the security of CI in the context of the necessity to invest in the inventory of next-generation CI, not just in the maintenance and upgrade of the current ones. At the same time, the construction site as CI proposal causes minimum disruption to existing ways of doing things and is compatible with existing European initiatives, such as the European Reference Network for Critical Infrastructure Protection (ERNCIP) and Critical Infrastructure Warning Information Network (CIWIN). It can also be made compatible with future projects, such as an expanded EPCIP or a European Critical Infrastructure Protection Agency.

7. Proposed plan of action for immediate next steps

Following the suggestions for the conceptual integration of the Construction 4.0 paradigm in the CIP framework and the EPCIP operational framework, this section presents a series of recommendations for additional action for the near future. Not all of them are practicable in the current pandemic environment, with its limited mobility, but should be kept in mind following a return to normality. These recommendations mostly propose efforts to bring Member States on board with the Construction 4.0 paradigm, and they are intended to raise awareness in the CIP and information and communication technologies (ITC) ancillary sectors (consultancy, academic research, security products, and services) about the potential of this perspective.

1. Convene a Working Group within DG-Home, also containing representatives from The European Union Agency for Network and Information Security (ENISA) and the European Defence Agency (EDA) (given its focus on cyber and the relevance of military construction and infrastructure) and other agencies to analyze the applicability of the recommendations presented by this position paper and of the Construction 4.0 paradigm to the European CIP framework, and create an Action Plan for the next period. Many of the consequences of the Construction 4.0 paradigm spread are not described herein, and neither is the list of possible adaptations of the CIP framework.
2. Organize an event within the European Parliament on this issue in Autumn 2020, in partnership with industry and civil society stakeholders in the construction and ICT sectors. One of the results of this event and others like it should be a broadening of the studies in the field of cybersecurity to also include the construction sector in their yearly analyses, as they currently do for telecom, manufacturing, government, finance, and others. In time, this will foster a better understanding of the problem of cybersecurity in the construction sector and build up a stakeholder base for collective action.
3. Allocate funding for research into the security consequences and the mitigation measures, along with products and services, of the spread of the Construction 4.0 paradigm.
4. Instruct the Joint Research Center (JRC) of the European Commission to develop the first iteration of a methodology for assessing the security vulnerabilities of ad-hoc and limited duration organizations, especially from a cyber-perspective. This would represent a valuable resource also for Member States. The JRC has the requisite skills and competencies not just for the cybersecurity

 doi:10.20944/preprints202005.0213.v1

aspect of Construction 4.0, but also the general construction dimension, through its existing efforts in improving building security[16].

5. Consider the possibility of planning and releasing a Communication on the subject of Construction 4.0 and Critical Infrastructure Protection in the European perspective to guide stakeholders in their consideration of possible adaptations to the new security environment and how Europe may improve the future iterations of the CIP legislative and administrative frameworks.

6. Consider the funding of a two-year Consultation Forum on Security in AECO, under the relevant European institution, with the possibility of extension, which would bring together representatives from EU institutions, from relevant Member State authorities, civil society, academia, private sector to discuss the implications of the construction sector and its transformations in security, to produce relevant materials for the Commission and to conceptualize research projects that would advance the subject matter while engaging also Member States and their voluntary resources. Ultimately, despite the subject matter of this position paper, Construction 4.0 represents a positive development, and even the amelioration of its security consequences represents an opportunity for the safety, security, and defense industries of Europe to innovate and create added value through products and services that will meet future demand.

8. Conclusion

The future iteration of the European Programme for Critical Infrastructure protection (EPCIP) presents an opportunity to enhance the existing framework by taking into account, and better manage, not just the realities of complex, interdependent systems, but also the systemic changes in the security environment. This position focused on Construction 4.0 which is, in brief, the digitization of design, construction and facilities' management, which not only creates opportunities for added value in terms of efficiency, safety, growth, comfort, but also unfolds new risks, vulnerabilities and threats related to the cyber-physical systems. We believe that, in some form, the concerns raised by the Construction 4.0 paradigm can be addressed through Critical Infrastructure Protection, starting from the already existing overlap between CIP and facility management. This position paper provides a few suggestions for further integration in a way that emphasizes compatibility with existing CIP philosophy and current practice. It also underlines a series of recommendations for actions in the next period, which may be conducive, ultimately, to better security outcomes. The suggestions are compatible with any probable expansions of the European Critical Infrastructure concept, such as European Critical Health Infrastructures and others, which may eventually lead to a wider variety of infrastructures being designated for security governance under the EPCIP framework.

Acknowledgment

This position paper is one from several deliverables from the 1st Workshop on Cybersecurity Implications of Construction 4.0 (CIC4-2020) that took place in New York University Abu Dhabi (NYUAD) in February 2020. The workshop was organized by the S.M.A.R.T. Construction Research Group and generously funded by the NYUAD Institute.

[16] https://ec.europa.eu/jrc/research-topic/improving-safety-construction

References

Andersson, J., Balduzzi, M., Hilt, S., Lin, P., Maggi, F., Urano, A., & Vosseler, R. (2019). A security analysis of radio remote controllers for industrial applications. Technical report, Trend Micro, Inc., January 2019. Available at: https://documents.trendmicro.com/assets/white_papers/wp-a-security-analysis-of-radio-remote-controllers.pdf [Accessed: May 2020]

Betz, D. J. and Stevens, T. (2013). Analogical Reasoning and Cyber Security, Security Dialogue Vol. 44, No. 2, pp. 147–164. DOI: https://doi.org/10.1177/0967010613478323

Bouchon S., Gheorghe A., Birchmeier, J. (2006). Toward Guidelines for Regional Assessment of Vulnerability against Service Disruption of Critical Infrastructures. EsReDa, the 29th Seminar "System Analysis for a More Secure World" Proceedings p. 81-95, JRC ISPRA, JRC32271

Bouchon, S. (2006). The Vulnerability of interdependent Critical Infrastructures Systems: Epistemological and Conceptual State-of-the-Art. EC Directorate General Joint Research Centre, Institute for the Protection and Security of the Citizen, Luxembourg, 2006

Boyes H. (2013). Resilience and Cyber Security of Technology in the Built Environment. The Institution of Engineering and Technology, IET Standards Technical Briefing, London. Available at: https://www.theiet.org/resources/standards/-files/cyber-security.cfm?type=pdf

BSI. (2015). PAS 1192-5:2015, Specification for security-minded building information modelling, digital built environments and smart asset management, British Standards Institution

Cavelty, M. D. (2013). From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse, International Studies Review, Vol. 15, pp. 105–122. DOI: 10.1111/misr.12023

Coburn, A.W., Daffron, J., Quantrill, K., Leverett, E., Bordeau, J., Smith, A., Harvey, T. (2019). Cyber risk outlook. Centre for Risk Studies, University of Cambridge, in collaboration with Risk Management Solutions, Inc. Available at: https://www.jbs.cam.ac.uk/faculty-research/centres/risk/publications/technology-and-space/cyber-risk-outlook/cyber-risk-outlook-2019/

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection [2008] OJ L 345, 23.12.2008, p. 75–82

ESRIF. (2009). European Security Research and Innovation Forum. (2009). ESRIF Final Report. Available at: https://wbc-rti.info/object/document/7460/attach/esrif_final_report.pdf [Accessed: May 2020]

F-Secure Labs (2014). Havex Hunts for ICS and SCADA Systems, Available at: www.f-secure.com/weblog/archives/00002718.html [Accessed: May 2020].

Garcia de Soto. (2019). Building Data Security: Construction industry's long-overdue shift to digital raises threat of cyber attacks. NYUAD – June 25, 2019. Available at: https://nyuad.nyu.edu/en/news/latest-news/science-and-technology/2019/june/building-data-security.html [Accessed: May 2020]

Garcia de Soto, B., Agustí-Juan, I., Joss, S., & Hunhevicz, J. (2019). Implications of Construction 4.0 to the workforce and organizational structures. International Journal of Construction Management, 1-13. DOI: https://doi.org/10.1080/15623599.2019.1616414

Grewal-Carr, V., Marshall, S. (2016). Blockchain: Enigma. Paradox. Opportunity. Deloitte, London, United Kingdom. Available at: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-full-report.pdf [Accessed: May 2020].

Horvath, M., Care, J., & Mahdi, D. A. (2018). Evaluating the Security Risks to Blockchain Ecosystems. Available at: https://www.gartner.com/en/confirmation/doc/3869088-evaluating-the-security-risks-to-blockchain-ecosystems [Accessed: May 2020]

IET. (2013). Resilience and Cyber Security of Technology in the Built Environment, Institution of Engineering and Technology/CPNI, 2013

IET. (2014). Standards, Code of Practice for Cyber Security in the Built Environment, Institution of Engineering and Technology, 2014

ISO (2012). 27032 Information Technology – Security Techniques – Guidelines for Cybersecurity, International Organization for Standardization (ISO), Geneva, Switzerland. Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en [Accessed: May 2020]

ISO (2013). 27001 The International Information Security Standard, International Organization for Standardization (ISO), Geneva, Switzerland. Available at: https://www.iso.org/standard/54534.html [Accessed: May 2020]

Kanan, R., Elhassan, O., & Bensalem, R. (2018). An IoT-based autonomous system for workers' safety in construction sites with real-time alarming, monitoring, and positioning strategies. Automation in Construction, 88, 73-86, DOI: https://doi.org/10.1016/j.autcon.2017.12.033

Keating, C.B., & Bradley, J.M. (2015). Complex system governance reference model. International Journal of System of Systems Engineering 6, 33–52

Kinnaird, C., & Geipel, M. (2017). Blockchain Technology: How the Inventions Behind Bitcoin are Enabling a Network of Trust for the Built Environment. ARUP. Available at: https://www.arup.com/publications/research/section/blockchain-technology [Accessed: May 2020]

Klinc, R., & Turk, Ž. (2019). Construction 4.0–Digital Transformation of One of the Oldest Industries. Economic and Business Review, 21(3), 393-410, DOI: https://doi.org/10.15458/ebr.92

Lamb, K. (2018). Blockchain and Smart Contracts: What the AEC sector needs to know. Center for Digital Built Britain. CDBB 16. DOI: https://doi.org/10.17863/CAM.26272

Maciel, A. (2019a). Construction Blockchain Consortium Conference 2019: Closing Remarks [WWW Document]. https://drive.google.com/file/u/1/d/1NTNc842bLo36k6hQJaoxkDQvLhSHiFI0/view?usp=sharing&usp=embed_facebook [Accessed: May 2020]

Maciel, A. (2019b). Forge DevCon 2019: BIM, Blockchain & Smart Contracts, Forge DevCon Germany. Germany. YouTube URL https://www.youtube.com/watch?v=Wb28HudjkyI

Maciel, A. (2020). Use of Blockchain for enabling Construction 4.0. Chapter 20. In A. Sawhney, M. Riley and J. Irizarry (Eds.). Construction 4.0: An Innovation Platform for the Built Environment (pp. 441-459). 1st Edition. London: Routledge, ISBN-13: 978-0367027308. DOI: https://doi.org/10.1201/9780429398100-20

Mantha, B. R., & Garcia de Soto, B. (2019). Cyber Security Challenges and Vulnerability Assessment in the Construction Industry. Proceedings of the Creative Construction Conference, Budapest, Hungary. http://dx.doi.org/10.3311/CCC2019-005

Mantha, B. R., & Garcia de Soto., B. (2019). Task Allocation and Route Planning for Robotic Service Networks with Multiple Depots in Indoor Environments. In ASCE International Conference on Computing in Civil Engineering (i3CE), June 17-19, 2019, Georgia Institute of Technology, Atlanta, Georgia, USA, DOI: http://dx.doi.org/10.1061/9780784482438.030

Mantha, B. R., Garcia de Soto, B., & Karri, R. (2020, May 7). Cyber Security Threat Modeling in the Construction Industry: A Countermeasure Example During the Commissioning Process. https://doi.org/10.31224/osf.io/gn78a.

Mantha, B. R., Garcia de Soto, B., Menassa, C. C., & Kamat, V. R. (2020). Robots in indoor and outdoor environments. Chapter 16. In A. Sawhney, M. Riley & J. Irizarry (Eds.). Construction 4.0: An Innovation Platform for the Built Environment (pp. 441-459). 1st Edition. London: Routledge, ISBN-13: 978-0367027308. DOI: https://doi.org/10.1201/9780429398100-16

Mantha, B. R., Menassa, C. C., & Kamat, V. R. (2018). Robotic Data Collection and Simulation for Evaluation of Building Retrofit Performance, Automation in Construction, Vol 92, pp 88-92, DOI: http://dx.doi.org/10.1016/j.autcon.2018.03.026

Mendis, D., Nordemann, J. B., Ballardini, R. M., Brorsen, H., Calatrava Moreno, M. d. C., Robson, J., & Dickens, P. (2020). The Intellectual Property Implications of the Development of Industrial 3D Printing. Final Report (12 February 2020). European Commission. DOI: https://doi.org/10.2873/85090

Nguyen, B., Buscher, V., Cavendish, W., Gerber, D., Leung, S., Krzyzaniak, A., ..., & Flapper, T. (2019). Blockchain and the built environment. Version 1.2, February 2019. London: Arup Group Limited. Available at: https://www.arup.com/-/media/arup/files/publications/b/blockchain-and-the-built-environment.pdf [Accessed May 2020]

NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, National Institute of Standards and Technology. Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf [Accessed: May 2020]

O'Gorman, B., Wueest, C., O'Brien, D., Cleary, G., Lau, H., Power, J.P., Corpin, M., Cox, O., Wood, P., Wallace, S. (2019) Internet Security Threat Report. Volume 24, Symantec, February 2019, Available at https://www-west.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf

Pärn, E. A., & Garcia de Soto, B. (2020). Cyber threats and actors confronting the Construction 4.0. Chapter 22. In A. Sawhney, M. Riley & J. Irizarry (Eds.). Construction 4.0: An Innovation Platform for the Built Environment (pp. 441-459). 1st Edition. London: Routledge, ISBN-13: 978-0367027308. DOI: https://doi.org/10.1201/9780429398100-22

Reuters, T. (2018). Blockchain for Construction Whitepaper [WWW Document]. URL https://mena.thomsonreuters.com/content/dam/openweb/documents/pdf/mena/white-paper/Blockchain_for_Construction_Whitepaper.pdf [Accessed May 2020]

Rinaldi, S.M., Peerenboom, J.P., Kelly, T.K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems Magazine 21, 11–25. https://doi.org/10.1109/37.969131

Shu, X., Tian, K., & Ciambrone, A. (2017). Breaking the target: An analysis of target data breach and lessons learned. https://arxiv.org/abs/1701.04940

Tang, S., Shelden, D. R., Eastman, C. M., Pishdad-Bozorgi, P., & Gao, X. (2019). A review of building information modeling (BIM) and the internet of things (IoT) devices integration: Present status and future trends. Automation in Construction, 101, 127-139, DOI: https://doi.org/10.1016/j.autcon.2019.01.020

Turk, Ž., & Klinc, R. (2017). Potentials of blockchain technology for construction management. Procedia Engineering, 196, 638-645. DOI: https://doi.org/10.1016/j.proeng.2017.08.052

Wang, J., Wu, P., Wang, X., Shou, W. (2017). The outlook of blockchain technology for construction engineering management. Frontiers of Engineering Management 67–75. https://doi.org/10.15302/J-FEM-2017006

Wendzel, S. (2016). How to Increase the Security of Smart Buildings? Communications of the ACM, May 2016, Vol. 59, No. 5, pp. 47–49, DOI: http://dx.doi.org/10.1145/2828636

World Economic Forum. (2016). Shaping the Future of Construction A Breakthrough in Mindset and Technology. Available at http://www3.weforum.org/docs/WEF_Shaping_the_Future_of_Construction_full_report__.pdf [Accessed: May 2020]

Ye, Z., Yin, M., Tang, L., & Jiang, H. (2018). Cup-of-Water Theory: A Review on the Interaction of BIM, IoT and blockchain During the Whole Building Lifecycle. Proceedings of the 35th International Symposium on Automation and Robotics in Construction (ISARC). Berlin, Germany. DOI: https://doi.org/10.22260/ISARC2018/0066