Cyber Security Threat Modeling in the Construction Industry: A Countermeasure Example During the Commissioning Process

Bharadwaj R. K. Mantha[1], Borja Garcia de Soto[1], Ramesh Karri[2]

[1] Division of Engineering, New York University Abu Dhabi (NYUAD), 129188, UAE
[2] Department of Electrical and Computer Engineering, Tandon School of Engineering, New York University (NYU), NY, 11201, USA

ABSTRACT

The digitalization and automation of the construction sector, known as Construction 4.0, are transforming positively the way we plan, design, execute, and operate construction projects. However, they are also increasing the vulnerability of construction projects and making the architecture, engineering, construction, and facility management (AEC-FM) industry subject to cyberattacks. Although current cybersecurity practices are relevant, they cannot be directly adopted because of the unique challenges faced by the AEC-FM industry, such as complex supply chains, interoperability, and dynamic workforce from project to project. Current literature suggests that, though current standards and practices are relevant, industry-specific studies need to be conducted before they can be successfully integrated. To that extent, this study investigates the cybersecurity threat modeling for construction projects by developing a framework that identifies what might be compromised, how might it happen, why would someone intend to do it, what would be the impact, and what could be done to prevent it. Specifically, the objectives are to a) develop a preliminary threat model relevant to construction that can be used by construction stakeholders with minimal cybersecurity expertise, b) show the feasibility of the approach by using illustrative threat models for each of the life cycle phases of a construction project, and c) use the commissioning phase of a building as a case study to show a possible countermeasure for the cyber threats that could occur during the testing or certification process of a given system. This study addresses essential components to enable the full potential of (i.e., digitalization and automation of the construction industry) and define research areas needed to pave the roadmap for the future of the construction industry and successful development of Construction 4.0. The proposed framework will help analyze, examine, and address the safety and security of stakeholders and systems during crucial phases of a construction project (e.g., pre-construction, construction, and operation).

Keywords: AEC-FM industry; Building commissioning; Construction 4.0; Construction automation; Cybersecurity; Cyber-physical system; Mobile robots; Threat modeling

I. INTRODUCTION

The rapid advancements in information and communication technologies, in conjunction with the ubiquitous availability of the computing devices, steered the fast-paced digital revolution of the 21st century (Jia et al., 2019). Though delayed, this has made its impact on transforming the construction industry, which was reluctant and hesitant to technological change. This has become increasingly important as construction firms strive to remain competitive. Some of the other motivating reasons include improvements in productivity, innovation, value creation, accessibility,

satisfaction, profits, sales, strategy, and marketing (Garcia de Soto et al., 2018; Osunsanmi et al., 2018; Boton and Forgues, 2017). Tools and technologies that are assisting the acceleration of construction digitalization include robotics, additive manufacturing, virtual and augmented reality, Internet of Things (IoT), and big data (Rastogi, 2017), among others.

The push towards construction digitalization and the current transformation in the industry also closely aligns with the concept of Industry 4.0. Thus the name, Construction 4.0 for this transformation in the construction industry. The aim is to digitize the information and have connected and automated systems across the different life cycle phases of construction, starting from the project inception to the end of life, including the commissioning, operation, and maintenance phases. It is expected and shown that the availability of digital information and the ability to automate different activities can have reaping benefits to the time, cost, quality, safety, and performance of the infrastructure systems. As a result of implementing these technologies large amounts of organizational (e.g., banking records, employee information, and intellectual property), project (e.g., design, safety, and productivity), and personal (e.g., social security numbers and demographic) data is stored, transmitted, and monitored. In addition, it also enables the control and automation of different systems that are in physical contact with equipment (e.g., excavator), assets (e.g., building), and people (e.g., labor).

Due to the involvement of highly confidential, proprietary, and sensitive information and access, there is an inherent security risk to digital information and the physical asset. For example, individuals with malicious intent can cause deliberate destruction by gaining access to onsite construction equipment. It is thus important for different stakeholders involved in the construction process to implement strategies and safeguard the security of the digital data and physical assets. However, the awareness and implementation in high-level security have been very low and neglected, which makes the industry susceptible and attractive to malicious individuals (Watson, 2018). Successful integration of construction digitalization requires the consideration of cybersecurity (Mantha and Garcia de Soto, 2019a; Parn and Edwards, 2019; Boyes, 2013; Fisk, 2012). Existing cybersecurity standards and practices from other industries cannot be directly adopted into construction due to characteristic differences and challenges such as complex interactions, different stakeholder interests, and lower profit margins. Therefore, a fundamental understanding of cyber risks and vulnerabilities as it relates to construction is necessary as part of the construction cybersecurity framework before formalizing risk management strategies to address them.

II. BACKGROUND

Cybersecurity can be defined as tools, policies, and practices to protect the stored and transmitted data (e.g., drawings, schedules, and contracts) and physical assets (e.g., sensors, equipment, and personnel) (ITU, 2019). The integration of the physical assets with the computing core (e.g., software) is usually referred to as cyber-physical systems or widely known as CPS (Anumba et al., 2010). As has occurred in other industries, operating in a digital environment makes them significantly vulnerable to cyber-attacks (Li et al., 2018; Liu et al., 2017). Construction is no different, and moreover, the complex chain of interactions, dynamics, coordination, and data exchange between several inter-connected construction project participants pose unique

performance, productivity, business, and security risks. Risk can be defined as the possibility of something bad happening (DHS, 2010). A threat can be defined as an action or event which can occur naturally or intentionally and has the potential to harm information, property, people, and the environment (Hutchins et al., 2015). Whereas attack is the action taken. Since risk and attack have closely related meanings, they are used interchangeably, and it might be confusing at times. Finally, vulnerability is the point of weakness or the state of being susceptible to an attack (Hutchings et al., 2015).

Most of the reported cybersecurity incidents related to the construction industry can be categorized as a data breach (e.g., data stolen, modified, destroyed, or made public), wire fraud (e.g., redirected payments), or property and/or service loss or damage (e.g., power outage). Few of the data breach incidents include jeopardized security due to stolen construction plans and specification files of the Australian Secret Intelligence Services (ASIS) in 2013 (Motley and Mas, 2017). A lot of construction employees' tax details and social security numbers of a US-based construction company, Turner, were compromised due to data sharing through unsecured channels posing business-related risks (Watson, 2018). In a similar incident, employees' tax information of a concrete construction firm was compromised (Motley and Mas, 2017). A very well-known construction elevator and escalator manufacturer, ThyssenKrupp, also fell victim to a data breach, and hackers got hold of the sensitive and confidential trade secret information (Motley and Mas, 2017). Whiting-Turner, a US-based construction management and general contracting firm, also suffered a data breach and lost health, insurance, and tax-related information of all its employees (iSqFt, 2016). On the other hand, hackers tried to steal the proprietary details of the one arm bricklayer robot in Australia developed by Fast Brick Robots (FBR) (Pash, 2018). Economic risks were faced during the collection of deposits from applicants in the name of Komatsu, a well-known Japanese construction machinery manufacturer (Watson, 2018). Konecranes and Marous Brothers Construction lost about 17.2 million euros and 1.7 million US dollars due to unwarranted payments and wire fraud, respectively (Sawyer and Rubenstone, 2019; Watson, 2018). Power services were disrupted for more than an hour and affected about 225,000 customers in Ukraine because the company's networked computers are hacked (BBC, 2017).

Several efforts were made to assess and manage risks, specifically focusing on the built environment security and Building Information Modeling (BIM) data sharing. For example, 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 key components of threat modeling, it does not detail cyber threats and vulnerabilities in construction (NIST, 2018). That is, none of the studies adopted and employed these steps to construction. On the other hand, the Publicly Available Specification (PAS) 1192-5, developed by the British Standards Institute (BSI) in the United Kingdom (UK), focuses on information security. It provides a framework to ensure that information is shared in a security-minded manner. This is 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 (PAS 1192-5:2015; IET, 2013). Another regulation, namely General Data Protection Regulation (GDPR) which was introduced in the year 2018 in Europe 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 (GDPR, 2018). These documents provide and establish best practices to improve the security of construction and facility management practices. Even though companies adhere to the standards and practices imposed and suggested by the local governments, cybersecurity incidents still take place as discussed and mentioned previously. This is because of a lack of continued understanding of the cyber threat landscape. Hackers work relentlessly to find faults and loopholes in the existing systems and take advantage of the weak links. It is necessary to continually evaluate security as part of the risk management process.

A. *Threat Modeling Methods*

Threat modeling is an essential way to understand cybersecurity threats and to devise effective and efficient action plans (Shostack, 2014). Threat modeling is the process of identifying potential threats, vulnerabilities, attackers, and targeted assets (Bodeau et al., 2018). The objective is to understand the "how, where, why, and by whom" of an attack. An everyday example of threat modeling is when users install anti-virus in a laptop to protect themselves from hackers gaining access to personal data through malware injection. Another example is when installing a car alarm system to protect it from being stolen by a thief by breaking the windows. Several threat modeling methods such as STRIDE, OCTAVE, PASTA, and VAST have been developed. An overview, along with advantages and limitations, is presented next.

STRIDE was invented by Kohnfelder and Garg in 1999 (adopted by Microsoft in 2002) and uses data flow diagrams (DFDs), which include the entities, events, and boundaries of the evaluated system. The acronym STRIDE refers to the threat categories of Spoofing Identity, Tampering with Data, Repudiation, Information Disclosure, Denial of Service (DoS), and Elevation of Privilege. Though it is a mature threat modeling method, it requires an accurate DFD as input and may not represent all construction scenarios (Mead et al., 2018; Khan et al., 2017; Hernan, 2006). For example, the safety-related threats of incorporating new technologies (e.g., drones) to monitor progress on sites cannot be modeled in this method.

Process for Attack Simulation and Threat Analysis (PASTA), is a comprehensive threat modeling framework developed by UcedaVelez (2012). PASTA has seven stages and involves various stakeholders. Though it is comprehensive, it is tedious and requires domain-specific components such as application dependencies and design flaw analysis (UcedaVelez and Morana, 2015). Visual Agile and Simple Threat (VAST) modeling developed by Agarwal (2016) uses the ThreatModeler threat modeling platform. One of the main advantages of PASTA is scalability; it can be implemented in large organizations. However, one of the limitations is that it requires the creation of DFDs and operational threat models as the key steps. Operationally Critical Threat Asset and Vulnerability Evaluation (OCTAVE) suggested by the CERT (Computer Emergency Response Team) in 2003 (and revised in the year 2005) is comprehensive yet flexible (Alberts et al., 2003). It is a risk management approach based on strategic assessment. Only organizational risks are considered, and technology risks are out of scope. In addition, the documentation is complex, which limits its implementation (Deng et al., 2011). The characteristics of the above-discussed methods are summarized in Table I. Shevchenko et al. (2018) provide an extensive review of twelve of the most commonly used methods, including the ones discussed above.

Table I. Characteristics of few of the threat modeling approaches

Method	Characteristics
STRIDE	Mature but requires accurate data flow diagrams (DFDs)
PASTA	Comprehensive but requires domain-specific components
VAST	Scalable but has limited publicly available documentations
OCTAVE	Flexible but considers only organizational risks

Although existing studies and standards are helpful and relevant, they do not correspond to all the life cycle phases of a construction project due to the unique communication structure and corresponding cybersecurity challenges. These studies did not explore the motivation of the different stakeholders — e.g., manufacturers, installers, and facility managers — to tamper with the data or to compromise the sensors to fabricate data to facilitate the certification and commissioning, which is construction-specific. To summarize, the limitations of existing threat modeling methods and standards are, they a) focus only on building systems and data exchange security in the built environment, b) neglect bidding, planning, design, and construction phases, c) are tedious, time-consuming, and might require domain-specific knowledge, d) lack an approach where the construction-related threats, vulnerabilities, attackers and assets are identified and mapped. To address these key research gaps, the objectives of this study are to a) develop a preliminary threat modeling approach relevant to construction that can be used by construction stakeholders with minimal security expert involvement, b) show the feasibility of the approach, c) develop illustrative threat models for the life cycle phases of a construction project, and d) conduct a case study for the commissioning phase concerning the testing and/or certification.

III. THREAT MODELING APPROACH - APPLIED TO THE AEC-FM INDUSTRY

Any cybersecurity incident in construction can be summarized as follows: an attacker (i.e., people) attempts to influence (i.e., threat) something (i.e., asset) through a weak link (i.e., vulnerability). Fig. 1 shows examples of each of these key components in the context of the construction industry. Each of these is explained in the later sections of this paper. Reflecting on this and taking inspiration from the existing methods outlined earlier, a simplified threat modeling approach is proposed (Fig. 2). The objective is to develop a framework that is comprehensive, flexible, and that requires minimal cybersecurity-domain knowledge and expertise. An overview of the approach and a description of the steps is described below.

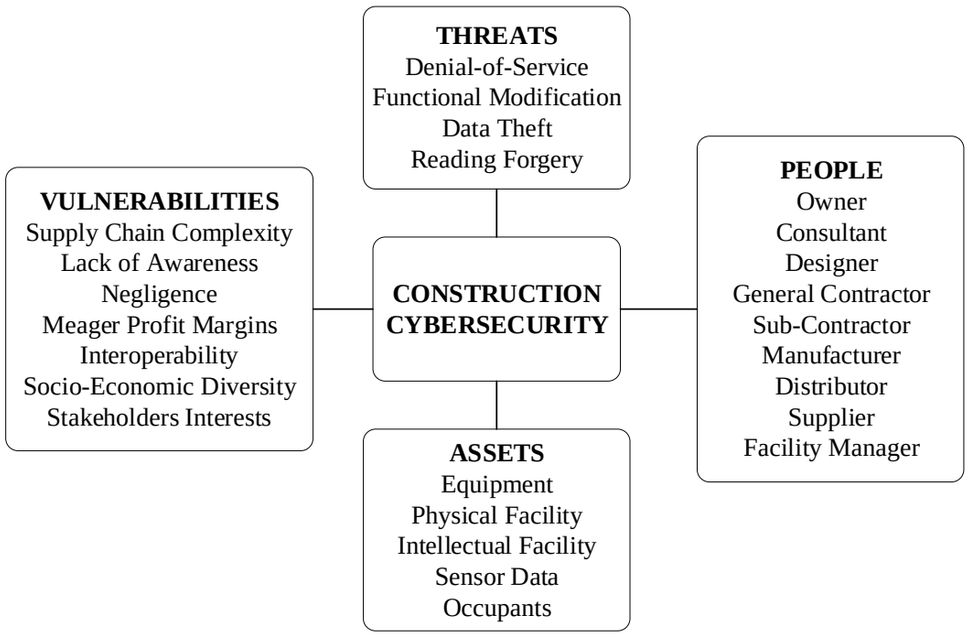

Figure 1. Key components of the construction cybersecurity.

Based on the chosen life cycle phase, the critical assets need to be identified. It is important to identify all the critical assets of interest and prominence, which may or may not seem cyber critical. For example, assets with or without any computing devices need to be identified (e.g., workers). Then, all the cyber-enabled components (e.g., processes, information, and communication exchange) for the identified assets that need cybersecurity investigation or improvement has to be developed. A crucial step in the process is the identification of potential threats based on the identified critical assets. That is, what could go wrong with the assets that might have physical, financial, and psychological (e.g., reputation) impact. Then, 1) brainstorm who would want to cause such harm, 2) how would he/she intends to do that, and 3) what can be done to mitigate it. The first item might be easy to detail; however, the other two might need some help and technical expertise in the area of cybersecurity. To assist the construction stakeholders with this process, some of the significant threats, vulnerabilities, and countermeasures are further discussed below. Each of these steps is detailed in the subsections below in the context of the architecture, engineering, construction, and facility management (AEC-FM) industry. The approach can be as generic or as specific as needed depending on the defined objectives. For example, the objective can be as specific as investigating the cybersecurity implications of introducing a specific technology (e.g., using service robots in buildings) or as general as understanding the cyber awareness of the overall onsite construction procedures (e.g., the impact of IoT on the construction supply chain, construction activities, and operation and maintenance tasks).

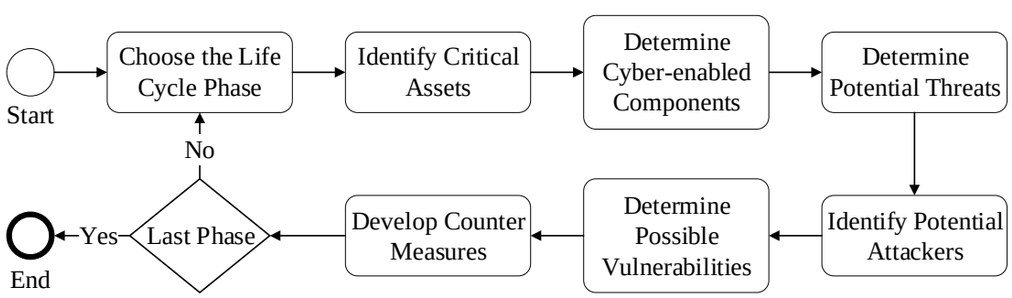

Figure 2. Proposed threat modeling approach.

A. Choose the Life Cycle Phase

The project delivery system selected by the owner sets the terms in which parties interact and enter into legal agreements with other parties and used as mechanisms to shift risk. They have implications in the organization and financing of projects. They affect the interaction and organization of parties during construction, operations, and maintenance services. The most common and established delivery method used is Design-Bid-Build (DBB) (Tanko et al., 2018; Ibbs et al., 2003). However, the adoption of lean construction and building information modeling (BIM) in the past few years has favored the use of alternative delivery systems, such as Integrated Project Delivery (IPD), which shifts efforts and responsibilities to the early phases of a project (Bilbo et al., 2015; AIA, 2007). Although the project delivery system will have implications on the organization and involvement of different project participants, the main phases of the life cycle of a project are similar.

The life cycle of any built infrastructure can be divided into five phases namely a) project initiation, b) design and engineering, c) construction and procurement, d) commissioning, e) operation and maintenance, and f) renovation and end of life (Aghimien et al., 2018; Mesároš et al., 2016; Bennett, 2007; Ries and Mahdavi, 1999; Oberlender,1993; Hendrickson and Au, 1989). Although these phases are not exhaustive, they offer a general overview of the processes in the life cycle of construction projects. For each phase, key participants, general tools, and equipment used are identified in Fig. 3. Understanding the fundamental construction processes, as well as the different phases, tools, and participants involved, form the basis for the delineation of the cybersecurity aspects in construction, which are described in the later sections of this paper. For in-depth details regarding each of these different phases and processes, the reader is encouraged to go through the construction management handbooks as the scope of this work is just to provide a general overview (Chudley and Greeno, 2014; Hearl, 2010; Oberlender,1993; Hendrickson and Au, 1989). This will assist in further discussion and analysis regarding identifying different key components of the threat model.

B. Identify Critical Assets

In a construction project, assets refer to different things such as a physical facility (that is being constructed, monitored, or operated), equipment (e.g., excavators, dozers, and dump trucks), intellectual property (e.g., 3D printer characteristics, design, and quality procedure), data (contractual documents, financial records, design, and sensors), as well as human-related assets (e.g., labor, employees, occupants, and visitors). The ultimate goal of most of the construction cyber-attacks is to disrupt, damage, or take undue advantage of one or more of these assets.

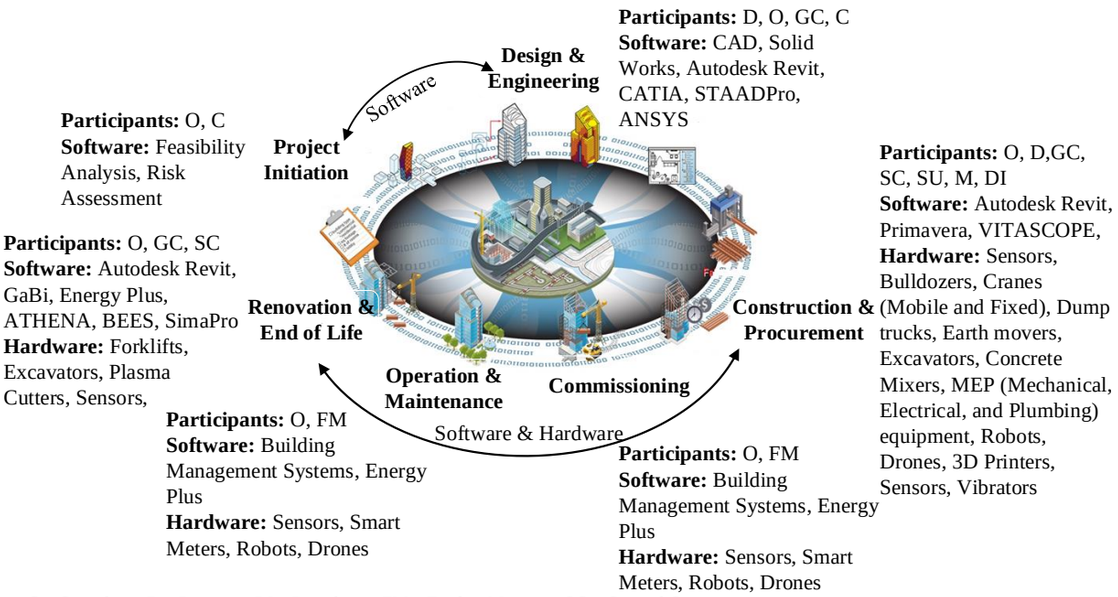

Figure 3. Participants, software, and hardware across different phases in the life cycle of construction projects (core image adapted from Autodesk, 2016).

C. Determine Cyber-Enabled Components

The purpose of this step is to develop an activity flow diagram based on the application, objectives, processes, interactions, information, and communication exchange. It can be for the whole construction life cycle to a specific process or application. For example, threat modeling can be done for the design phase, digital fabrication of structural panels, investigating the impact of installing cameras on the construction site, and human-robot interaction during operation. Important elements to consider are the applicable and appropriate sequence of activities, the interdependence of activities, information exchange channels, participant interaction, software, hardware, and cyber-enabled devices. In human-robot interaction, applicable elements include robot, people (e.g., labor and engineers), sensors, data collection, exchange, and analysis.

D. Determine Potential Threats

In the ever-evolving landscape of digital technology, cyber threats have become increasingly complex. There are several types of cyber threats that could jeopardize the safety or security of construction assets such as ransomware, data breaches, cyber-extortion, phishing, hacking, malware, denial of service, and many more. Some of these terms are used interchangeably and have overlapping contexts, meanings, and motivations (Tang et al., 2018; Motley and Mas, 2017). For example, someone can introduce malware (e.g., a computer virus) to perform data breach (e.g., steal information) or for ransom (i.e., demand money or threaten to make data public). Some of the most relevant and increasingly concerning cyber threats for the construction industry are summarized below.

Denial-of-Service: Commonly known as DoS, this refers to the class of threats that aims to render systems or equipment unusable (Tang et al., 2018). In this, an attacker (people) gains control of the system or equipment such as excavators, drones, and building management systems (BMS) and denies access to legitimate users such as contractors, owners, and facility managers, respectively. For example, a suspicious vendor can incorporate malicious behavior into the design and production of critical construction equipment to disrupt services during the construction.

Functional Modification: refers to the modification of functionality for the system to behave in an unexpected or unintended manner (Tang et al., 2018). An example of such a threat in construction could be over and excessive actuation of owner provided or guaranteed equipment onsite to degrade performance and claim schedule delays.

Reading Forgery: refers to manipulation or deliberate misrepresentation of sensor data to mislead or obtain undue advantage (Tang et al., 2018). For example, untrusted electronic chips and sensing devices could be integrated to produce misleading data and assist in the building commissioning, testing, or certification process.

Data Theft: relates to the stealing of any sensitive and confidential information related to IP (e.g., patented technology), people (e.g., employees' social security numbers), organization (e.g., financial records), equipment (e.g., process parameters), and best practices (e.g., safety and quality). For example, unpatched software systems could be exploited to gain competitive and confidential IP regarding operational procedures (e.g., 3D printer material properties).

There can be several motivations for these cyber threats such as ransom, gain power, competition, ideological activism, political, cyberwar, anger, and hatred. It is not possible to map each of these reasons to a specific type of attacker and threat. For example, an insider or an outsider can perform data theft to obtain ransom money. Similarly, a current employee can make a functional modification to damage the reputation of a company or obtain approval/ certification

E. Identify Potential Attackers

These threats occur due to the direct or indirect consequence of peoples' actions. They can be working within the organization (e.g., employees), on the project (e.g., designers and consultants), clients (e.g., potential users of the facility), and outsiders (e.g., hackers). Due to the complexity of the construction projects, several people are involved, such as owners, designers, consultants, contractors, subcontractors, suppliers, manufacturers, distributors, and sellers. It is helpful to identify the potential attacker based on the identified threat, motivations, and communication exchange channels. For example, if the threat is compromising the competitive bid data that needs to be placed, an obvious attacker is a potential contractor bidding for the project motivated to learn about competitors' bids and adjust their bid to win the project.

F. Determine Potential Vulnerabilities

The challenges encountered by construction companies compare to those faced by other industries that are adopting new technologies and are at an advanced level of digitalization. However, some vulnerabilities are specific to the construction sector for the following reasons.

Supply Chain Complexity: A large portion of the construction is usually performed by speciality subcontractors who belong to small and medium-sized enterprises (SMEs). This involvement increases the complexity of construction supply chain networks, which is responsible for the increased cyber-vulnerability of construction processes. In addition, construction is known to have meager profit margins and hence limited dedicated resources to information technology (IT) services.

Dynamic workplace and workforce: Unlike other industries, construction is dynamic with an ever-evolving pace of work, workplace, and workforce. The workplace evolves with the progress of the

project and 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 are part of the project workspace. 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 fragmented nature of construction employees that largely consists of sub-contracted workforce.

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 (Building Information Model) and CDE (Common Data Environment), 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, the exchange of confidential and sensitive data may occur outside the company's network (e.g., using personal computers). In addition, devices used on construction sites may not be 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.

Different Stakeholder Interests: Even the smallest of construction projects involve people from different backgrounds, skills, and interests. Ideally, the main goal of everyone is to complete the project successfully. However, there can be multiple conflicting interests of different stakeholders involved. For example, a contractor would like to maximize profits while at the same time, an owner tries to minimize the total budget. Similarly, a structural designer attempts to revise the specifications as part of a value engineering exercise, which might not best suit the contactor interests due to disruption and delay of initially planned activities.

Uniqueness of Projects: Although construction is fragmented with multiple teams involving architects, designers, contractors, consultants, suppliers, manufacturers, workers, engineers, supervisors, and owners, no two projects will have the same teams. Even for two very similar projects (e.g., high-rise residential buildings), the project teams can vary. In the context of cybersecurity, this is a major limitation considering that the cybersecurity policies might differ among each of these participants, and developing a synergy every time with a new set of project teams is challenging and can have productivity implications.

G. Develop Countermeasures

Countermeasures are technical or organizational strategies to mitigate or eliminate the identified threats. Multiple countermeasures can be possible for any given threat. The optimal solution can be weighed based on feasibility and economic analysis. On the other hand, countermeasures can be

reactively mitigated if the specific vulnerability due to which the attack occurred is known. For example, if design data theft occurred due to weak password control, then countermeasures such as educating employees to create stronger passwords and imposing access restrictions can be done to eradicate the threat. However, if the specific vulnerability is unknown, there can be several alternative countermeasures that can be taken based on the existing best practices, standards, and methods. Here, few of the existing standard countermeasures for most of the usual threats encountered, including the ones discussed above. Countermeasures for each of the significant threats mentioned in the determine potential threats subsection previously are briefly described below.

A large scale distributed DoS threat is known as DDoS threat, and researchers proposed DDoS Blocking Application (DBA) as one potential solution for such kind of threats. The idea is to differentiate between normal and malicious traffic through LISP (Location/ ID Separation Protocol) (Farinacci et al., 2013). Randomized checkpointing is suggested as one of the widely known solutions for functional modification and reading forgery related threats (Tang et al., 2018). This is to detect attacks based on frequent but random inspections. Since the attacker has no idea about the checkpoint locations, the attacker just hopes to evade detection. Up-to-date software patches (updating the software and antivirus), data encryption (ciphered or coded data which is unable to be deciphered without the decryption key), and cyber deception (deceit of data via dummy records in the database) are some of the recommended and usual countermeasures for data theft related threats (Ullah et al., 2018). Finally, this process is iteratively performed through all the steps discussed until all the life cycle phases are completed. Below is the illustrative section. An overview of each phase is briefly described, and an example threat model is developed and further discussed.

IV. THREAT MODELS FOR DIFFERENT PROJECT LIFE CYCLE PHASES

This section presents the flexibility of the proposed approach by developing illustrative threat models for each of the key phases of a construction project. This is done based on an overview of the processes and activities involved. That is, activities, participants, and tools involved in each of the phases are detailed, and the proposed method is applied to develop illustrative threat models. Thus, along the process, it is necessary to determine a few things, such as the sequential order of the activities involved, participants responsible, tools used, and aim/goals of different activities. As previously indicated, for simplicity, the DBB project delivery method is used. The underlying process will still be the same if the variations caused by the adoption of different project delivery systems are to be captured.

A. *Project Initiation*

The overall aim of this phase is to determine the feasibility of the project and subsequently define the specific project objectives. Fig. 4 shows a brief list of activities involved in the project initiation phase. Initially, the owner's team briefly identifies the need for the project and subsequently documents a justification. This, in project management terms, is referred to as a business problem or opportunity (Brioso, 2015). After the need is justified, the owner, in conjunction with the consultant, evaluates the technical aspects of the project and prepares preliminary cost estimates to verify the feasibility of the project. For example, factors such as capability, resource availability, geographical constraints, political, and cultural considerations are evaluated and analyzed. At this stage, if the

team concludes that the project is not feasible, the project will be terminated. If not, different alternatives are examined, and an optimal one is chosen, which best addresses the need for the project (identified during the beginning of the project).

Based on the process overview, some of the critical assets during this phase could be project definition (e.g., the world's tallest tower) and organizational data (e.g., social security numbers). Some of the cyber-enabled components in the process include technical evaluation and project definition. Since the critical asset directly involves dealing with data, the direct potential threat could be a data theft. Given the sensitivity involved, multiple parties such as competing contractors, consultants, and other stakeholders could be interested in obtaining such information to gain undue advantage.

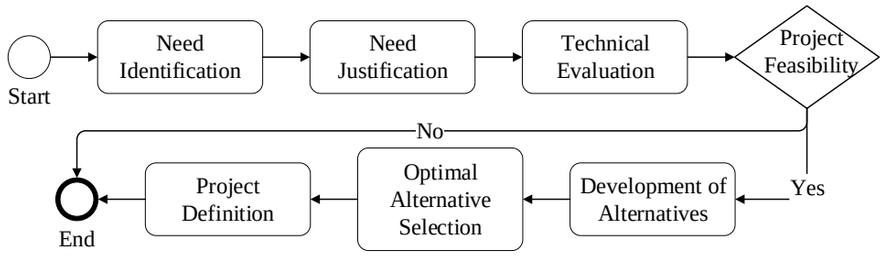

Figure 4. Activities involved in the project initiation phase.

For example, the concept for constructing the next tallest tower in the world could be of potential interest to many stakeholders and governments all across the world. These individuals or entities usually try to exploit any unsecured network transfers and cloud storage systems to obtain such information. To address these issues, some of the potential countermeasures could be to educate employees and conduct frequent audits to verify the security of the systems and network involved. This threat model is shown in the form of a table in Table II.

Table II. Significant Threat Modeling Aspects involved in the initiation phase

Critical Assets	Potential Threats	Potential Attackers	Potential Vulnerabilities	Countermeasures
Project definition Organizational data	Data theft	Consultant Contractor/subs Employees Owner	Unsecured network transfer Unsecured cloud storage applications	Educate employees Conduct frequent audits

B. Design & Engineering

After defining the project, the design and/or construction team is chosen by the owner with possible recommendations of the consultant. This selection could be made by issuing a request for proposals followed by a competitive bidding process or other selection methods (e.g., direct appointment). Based on the identified project objectives, designers put together preliminary designs. Then, cost estimates and baseline schedules are provided to the owner by the design team for the final approval of the design. Several value-engineering and brainstorming sessions are typically done before the owner finally approves the design to meet quality, budget, and time constraints. The final design is submitted to the local authority to obtain the required approvals and construction permits in order to start with the construction of the facility. Once the design is completed, and permits are obtained, a

contractor is chosen by the owner. The selection could be made through a competitive bidding process (from a request for bids) or other selection methods (e.g., direct appointment). Fig. 5 shows a simplified version of the activities involved in this phase.

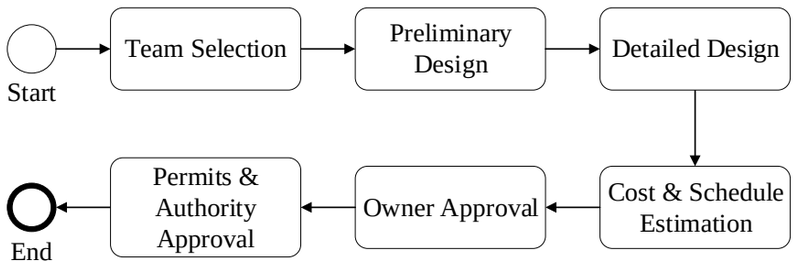

Figure 5. Activities involved in the design and engineering phase.

An example of the critical asset during this phase is the proprietary information regarding the operational procedures (e.g., in-situ fabrication or mass printing of customized elements) suggested and/or submitted by the contractor during the initial team selection or cost and schedule estimation. The threat is that this could be stolen or made public (i.e., threat) due to potential unpatched or outdated software systems (i.e., vulnerability). For example, consultants or designers could directly gain access to such information since they are working on the project and could have intentions to use this information on other similar projects. To address this, all the software systems need to be periodically checked to ensure they are up-to-date. In addition, sufficient access control protocols could also be imposed, such as hierarchical (e.g., certain individuals have only access to a particular level detail) and temporally restricted access (e.g., access permission is only for a particular period). The key elements are summarized in Table III.

Table III. Significant Threat Modeling aspects involved in the design and engineering phase

Critical Assets	Potential Threats	Potential Attackers	Potential Vulnerabilities	Countermeasures
Proprietary information (PI)	PI stolen	Consultant Designer	Unpatched software	Up-to-date software patches

C. Construction & Procurement

This phase refers to the actual implementation of the project. A simplified representation of the activities involved in this phase is shown in Fig. 6. In this phase, the main party is the general contractor (and subcontractors). Initially, resources such as manpower, material, and equipment are procured and/or transported to the construction site. This process is commonly termed as mobilization in the construction industry. With the help of these resources, construction activities are performed. Main construction tasks can be broadly classified as the construction of structural core (e.g., slabs, columns, beams), MEP (mechanical, electrical, and plumbing systems such as heating, cooling, ventilation, lighting, water, and drainage pipes), and finishing (e.g., exterior: roofing, façade, curtain wall, windows; interior: insulation, plastering, and painting). The process of constructing a structural core includes excavation (i.e., breaking the ground), foundation (lowest part of the facility which transfers the load from the structure to the soil safely), and structural core, also known as the structural shell. Then, mechanical, electrical, and plumbing (MEP) works such as laying sewer pipes, installing ducts for ventilation, and electrical wires for lighting are performed.

Finally, the structural core on the outside and the inside are enclosed with the help of activities such as plastering, cladding, painting, and flooring commonly referred to as finishing works.

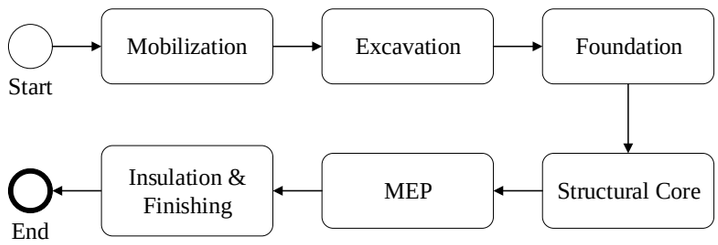

Figure 6. Activities involved in the construction and procurement phase.

Table IV shows one example of a threat model for this phase. Productivity is arguably one of the very important aspects of this phase. One of the critical assets during this, which has significant implications on productivity, is the equipment such as excavator, dump truck, and tower crane. Sometimes it is possible that the owner supplies the equipment to the contractor to perform certain construction operations. Contracts (i.e., attacker) might intend to overuse the equipment (i.e., vulnerability) to directly or indirectly lower the performance (i.e., Threat) in an aim to claim or justify project delays. Alternatively, malicious outsiders (i.e., attackers) can introduce fabricated chips (vulnerability) during the procurement process (i.e., cyber-enabled process) to cause physical damage (i.e., Threat) to workers (i.e., asset) at the time of construction. These can be potentially addressed by having equipment logs and conducting company audits.

Table IV. Significant Threat Modeling Aspects Involved in the construction and procurement phase

Critical Assets	Potential Threats	Potential Attackers	Potential Vulnerabilities	Countermeasures
Equipment	Performance degradation Physical damage	Contractor/subs Malicious outsider	Excessive usage Fabricated chips	Regular equipment log check and audits

D. Commissioning

Before transfer to the owner and occupancy or use of the finished building, the installed building systems and equipment need to be commissioned. Summary of activities involved in such a process is shown in Fig. 7. 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.

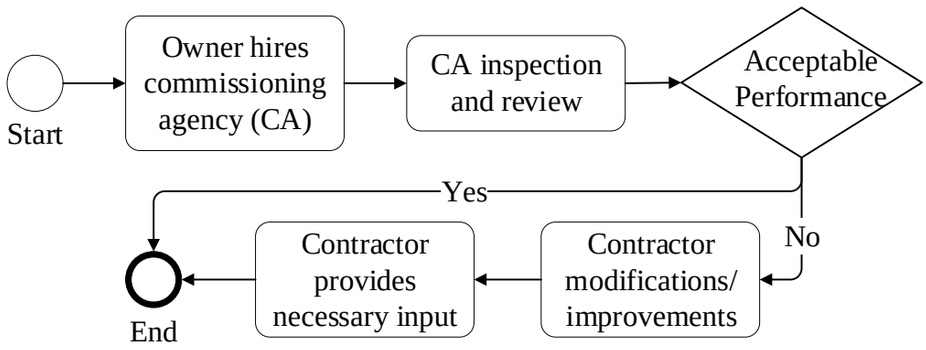

Figure 7. Activities involved in the commissioning phase.

As can be noted from the description of the process, the acceptable performance of the asset is one of the critical elements and is the focus of the example threat model, as shown in Table V. Most of the modern buildings rely on the data from building management or automation systems (BMS/ BAS) (i.e., critical asset) to facilitate the certification process. Owners and/or contractors (i.e., attackers) during the review process (i.e., cyber-enabled process) can tamper or modify the sensor data (i.e., vulnerability) to expedite this process and obtain occupancy certificate.

Table V. Significant threat modeling aspects involved in the commissioning phase

Critical Assets	Potential Threats	Potential Attackers	Potential Vulnerabilities	Countermeasures
Building Management Systems (BMS)	Data tampering Actuation tampering	Owner Contractor Consultant Employee Outsider	Dashboard compromised Sensor compromised	Randomized checkpointing

E. Operation & Maintenance

Although every facility undergoes commissioning process initially, continuous maintenance is necessary because the performance of the systems degrade over time, there might be a change in functional use, and there can be unanticipated faults due to excessive or inadequate use (Heo et al., 2012). To address this, these systems need to be continuously monitored and maintained. The facility manager who usually belongs to the owner's team is responsible for this. The preliminary monitoring is typically done with the help of manual inspections. The aim of manual inspections is to identify the overall appeared physical condition of the facility and the different building systems and equipment. If the preliminary physical condition assessment fails, further analysis is performed with the help of monitored sensor data. Then, a maintenance program is made based on the analysis of the results. If maintenance is required, the objectives need to be determined, and cost-benefit analysis has to be performed before proceeding with the execution of the maintenance activities. This process is iteratively performed until the end of the functional use of the facility (or system/equipment). A simplified representation of the activities involved in this phase is shown in Fig. 8.

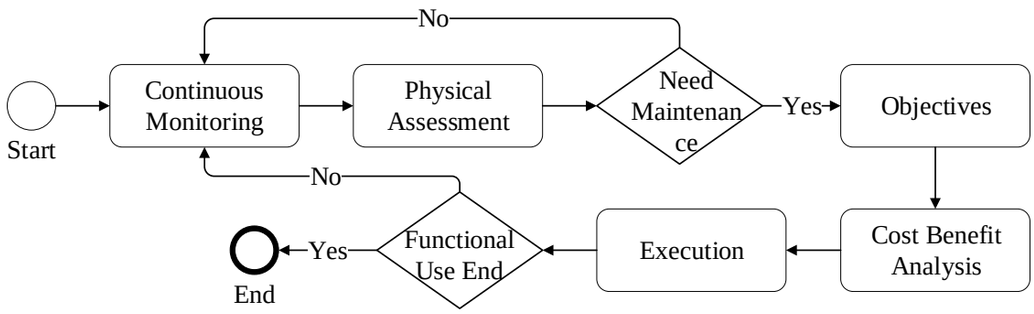

Figure 8. Activities involved in the operation and maintenance phase.

Table VI shows an example threat model that could potentially impact the physical asset or the occupants using the asset (i.e., critical asset). This could be done by malicious outsiders or external suppliers (i.e., attackers) through activities such as actuation tampering and chip insertion during the fabrication process (i.e., vulnerability) with an intent to spy and cause deliberate destruction (threat).

Table VI. Significant Threat Modeling Aspects Involved in the operation and maintenance phase

Critical Assets	Potential Threats	Potential Attackers	Potential Vulnerabilities	Countermeasures
Physical asset Occupants	Spying Deliberate destruction	Malicious outsiders External suppliers	Chip insertion	Use low-tech sweeping devices

F. Renovation & End of Life

If either the functional use reaches an end or the condition of the facility deteriorates to an extent where maintenance cannot suffice, repair, renovation, and demolition of the facility, or replacement of equipment need to be done. For this discussion, renovation refers to major maintenance where structural core needs to be removed or altered significantly. Initially, the renovation objectives need to be determined, and multiple alternatives are generated based on life cycle cost (LCC) and environmental impact assessments. Depending on the objective (e.g., minimize cost), an optimal option is chosen. In the process, a lot of waste is generated and needs to be optimized. The process flow is shown in Fig. 9.

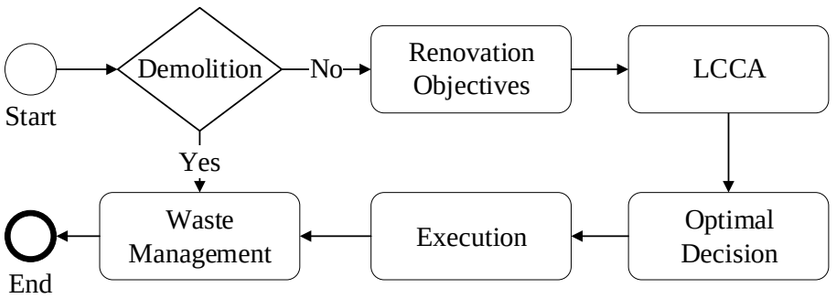

Figure 9. Activities involved in the renovation and end of life phase.

A common activity of waste management is the disposal of sensors or equipment without completely erasing the data (i.e., vulnerability). Malicious outsiders (i.e., attackers) obtain such equipment and reverse engineer the data/information (i.e., threat) regarding the facility, credentials, and other sensitive information (i.e., asset) that was either stored, accessed, or transmitted. The corresponding threat model is shown in Table VII.

Table VII. Significant Threat Modeling Aspects Involved in the renovation and end of life phase

Critical Assets	Potential Threats	Potential Attackers	Potential Vulnerabilities	Countermeasures
Physical asset	Data retrieval	Outsiders Others	Disposed sensors and equipment	Remove/destroy hardware before disposal

V. CASE STUDY

The objective of this case study is to analyze the threat model developed for the commissioning phase based on the proposed methodology and discuss a potential countermeasure. In addition to the discussion of the commissioning process (Fig. 7), inspection and review is a critical cyber-enabled process because of the use of sensors, data acquisition, verification, and approval. The commissioning agent verifies the conformance of all the building systems (e.g., building management systems, security controls, mechanical, and plumbing systems) to meet the desired design, quality, safety, and local code standards. This is done by monitoring the performance data of building systems, ambient indoor data, and outdoor parameters. The respective contractors and owners are responsible for ensuring that the desired functionality is achieved. This data is typically collected in the buildings (i.e., facility) using stationary sensor network systems containing wired and wireless sensors. Although many studies proposed frameworks and methodologies to develop such sensor and data collection networks, cybersecurity implications, and related challenges, have not been considered.

Fig. 10 shows an overview of the tasks involved in the inspection review process conducted by the commissioning agent. Initially, sensors gather information from the physical facility. Sensors measure different parameters, such as temperature, humidity, occupancy, and light intensity. This data is represented as dashboards developed by the manufacturers of the sensors. In parallel, controllers gather this data from sensors and determine the responses that are sent to the actuators to implement the controller actions.

A. Randomized Checkpointing Using Robots to Secure the Data Validation Process

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.

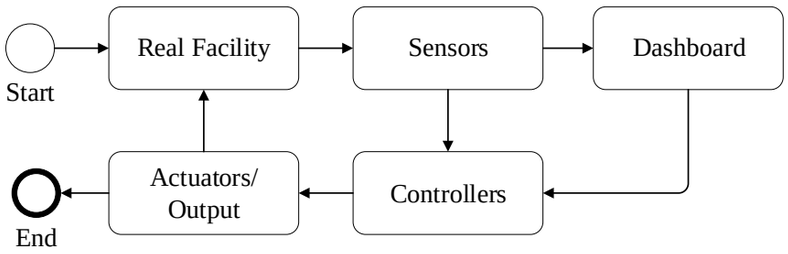

Figure 10. Sample process for the inspection and review by the commissioning agent.

To address this issue and detect faulty or rogue sensors or deter a rogue insider, we propose a randomized sensor check-pointing as a countermeasure. For this, we developed an autonomous multi-sensor fusing mobile robotic data collector. 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. We propose 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, (2019b) and Mantha et al., (2018). An overview of the onsite functional testing process, including the mobile robotic system, is shown in Fig. 11. Fig. 12 shows the multi-sensor mobile robotic platform.

B. Verification and Validation

To verify and validate the robotic randomized data collection and check-pointing, we consider an example floor plan with fixed sensors (i.e., the location of the BMS sensors is fixed). The objective is to identify potential rogue sensors within the fixed stationary sensor network system. To achieve this, the robot needs to visit all locations, gather time-stamped data, and cross-verify it with the BMS data. For the purpose of this study, an intricate indoor building environment consisting of a stationary sensor network is considered. The graphical network representation of an indoor floor plan with 25 nodes and 34 edges is shown in Fig. 13. As can be seen, the considered floor plan is not symmetric and considerably large.

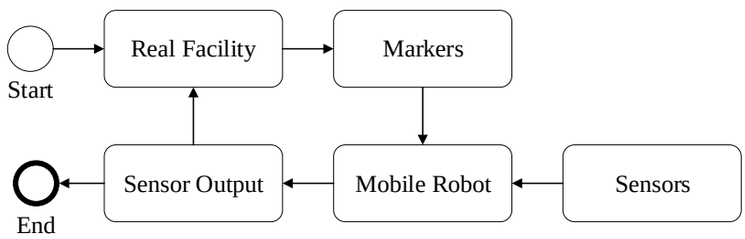

Figure 11. On-site review tests with the help of an autonomous mobile indoor robot.

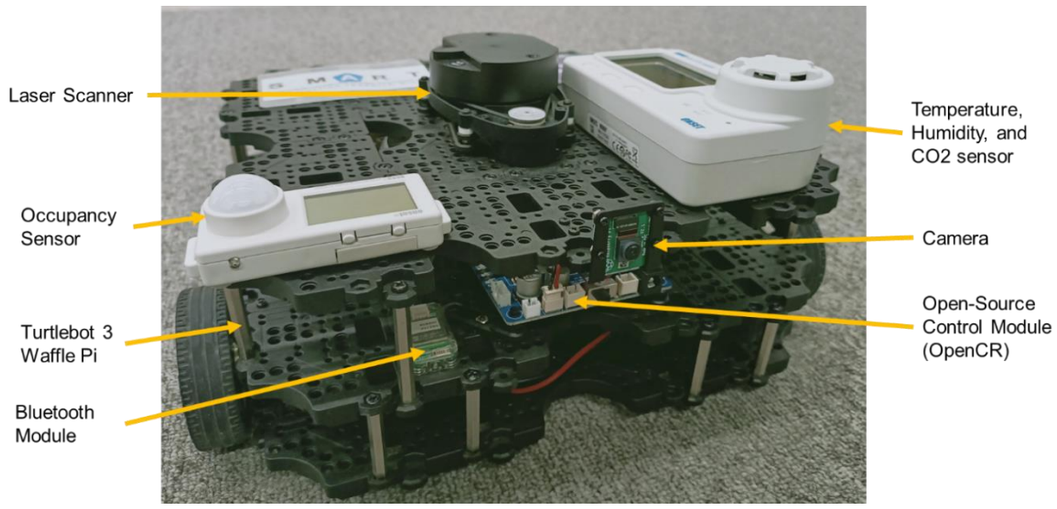

Figure 12. Mobile robotic platform with sensors.

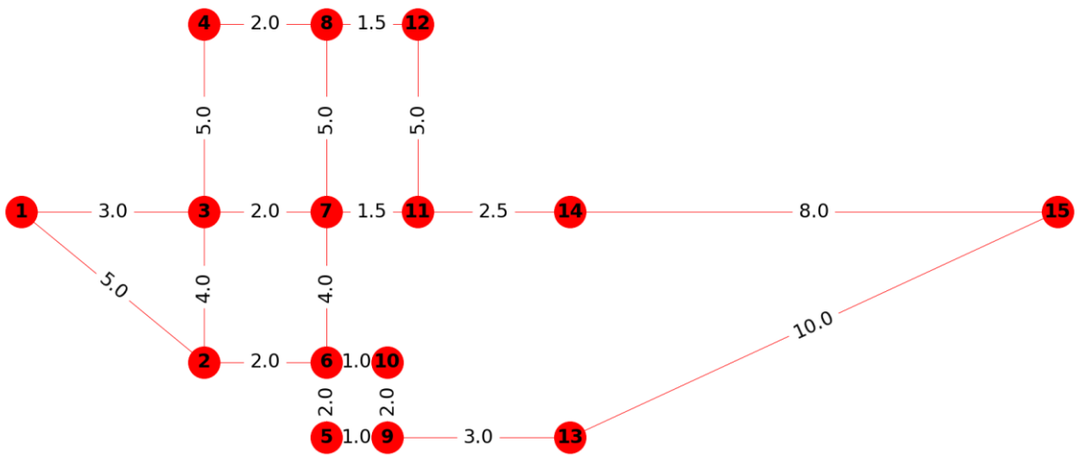

Figure 13. Graph network of an example floor plan with 25 nodes and 34 edges.

1) SCENARIO 1: COVER ALL EDGES (CHECK-POINTING ALL THE SENSORS)

Ideally, this is a problem of finding a path for the robot to cover all these sensor locations. This is usually achieved by first converting the existing built environment into a graphical network where the nodes represent the locations in the building, and the edges represent the physical links (e.g., corridors and stairs) connecting the nodes. Further details regarding converting building floor plans into a graphical network can be found in Mantha et al., 2019 and Mantha et al., 2018. Then, the graphical network is solved to determine an optimal path covering all the edges in the network so that the rogue sensor is not missed. Multiple paths are possible, and the most optimal path can be determined using existing algorithms (Ahr and Reinelt, 2006; Nobert and Picard, 1996). This is a classical Chinese Postman Problem (CPP) in graph network theory.

Given any start node, a path to visit all the edges in the network and return to the same node can be determined. In this example, if the start node is 1, the most optimized (i.e., shortest in this case) path to visit all the edges and return to node 1 is 1 → 3 → 4 → 8 → 7 → 11 → 12 → 8 → 12 → 11 → 14 → 15 → 13 → 9 → 10 → 6 → 7 → 3 → 2 → 6 → 5 → 9 → 5 → 6 → 2 → 1. Hence, if the rogue sensor is located at the visited nodes or edges, it can be checked by verifying the data from the rogue sensor with the sensor on the robot. So, in this situation, even if the attacker knows the map of the robot, the rogue sensor can be detected.

2) SCENARIO 2: PARTIAL EDGE COVERAGE (RANDOMIZED CHECK-POINTING)

Given a full CPP tour, the attacker can undermine it. That is, it is possible for the attacker to possibly have prior knowledge of the tour and tamper the sensors accordingly to report the correct results. To thwart such a coordinated response, a randomized tour can be adopted by the mobile check-pointing robot. Starting at a particular node, the next edge to be covered or the node to be visited is randomly determined. In this scenario, the robot need not (or is unable to) cover all the edges in the network because of time and distance constraints. For example, the robot can travel a certain distance due to battery restrictions (i.e., battery-informed distance constraint). Cybersecurity studies have shown that this randomness in the verification process creates uncertainty for the rogue attacker and improves the cybersecurity of a process (Casey et al., 2014). Thus, the objective is to determine random paths with the help of existing algorithms and heuristics such that most of the edges are covered with a maximum distance constraint.

One approach is as follows. Initially, periphery nodes at the farther end of the graph network generated are identified. All simple paths (ASP) between different permutations and combinations of these periphery nodes are estimated. Simple paths are the paths that start at a particular node (source) and end at a destination node without repeating any nodes in between (Black, 2017). Each path can be considered as a random path starting from the source node to the destination node.

3) RESULTS AND DISCUSSION

Table VIII shows the results of scenario – 1 and 2 on the network shown in Fig. 13, considering the position of the rogue sensor located at the edge 14 → 15. For Scenario 1, the optimal route to visit all the edges in the network takes 169 units. Since the robot covers all the edges in the network, the rogue sensor will always be detected when comparing the sensors in the network and on the robot. Though this is ideal and preferred, this might not always be possible because of battery constraints. For example, what if the robot can only travel 100 units in a single charge? To address this issue, only part of the edges can be traversed, and the rest of the results and analysis show a systematic approach to identify a near-optimal solution. The periphery nodes for this network are 1, 2, 4, 23, and 24. The average path distance and the unique number of edges are an average for all the simple paths generated for that combination of the periphery nodes. For example, for the periphery node pair of 1 and 23, the total number of paths generated was 348. Path distance, number of unique edges, and a binary variable for the presence of the edge (14 → 15) is stored. The average of all the distances came out to 52.1, the number of unique edges to 13.9, and in 156 out of 348 instances, the edge 14 → 15 was present in the paths generated. Thus, the probability of detecting (P(d)) rogue sensor is the number of instances the edge with the rogue sensor present is divided by the total number of simple paths generated (156/348 =0.45). This is mathematically represented in the form of a fraction and shown in Equation 1. As can be seen, with about 45% (i.e., 0.45) probability, the rogue sensor can be detected with this approach except for combinations including node 4 (i.e., 4, 23, and 4, 24). In general, the less probability might be due to the low number of unique edges.

$$P(d) = \frac{number\ of\ sensor\ detected\ paths}{total\ number\ of\ paths} \qquad \text{Eq. (1)}$$

Table VIII. Likelihood of rogue sensor's detection with full and partial paths

Description	Average path distance	Average # of unique edges	$P(d)$
CPP	169.0	34.0	1.00
ASP (b/w 1 - 23)	52.1	13.9	0.45
ASP (b/w 1 - 24)	52.1	13.9	0.45
ASP (b/w 2- 23)	51.6	13.8	0.44
ASP (b/w 2 - 24)	51.6	13.8	0.44
ASP (b/w 4 - 23)	48.8	13.8	0.27
ASP (b/w 4 - 24)	48.7	13.8	0.27

To improve this, additional heuristics or constraints such as the number of unique edges to be traversed are imposed. Since the average number of unique edges was 14 in the original analysis above, we increased it to 17 for discussion and analysis. Table VIII shows the results after imposing the number of unique edges constraints. A path is feasible if there exist at least 17 edges that are unique, and the total distance of the path does not exceed 100 units. The results are summarized in Table IX. Contrary to expectations, the probability of detection was reduced. For example, a combination of node pairs (2,23) yielded the worst results with the probability of detection reducing from 0.45 → 0.09. This could occur because the algorithm optimizes the total distance traveled by the robot and does not take into consideration the number of edges traversed along the way.

Table IX. Likelihood of detecting the rogue sensor when the average number of unique edges is 17 and the maximum distance constraint is 100 units.

Description	Average path distance	Average # of unique edges	$P(d)$
1 – 23	73.6	17.4	0.20
1 – 24	65.6	17.5	0.27
2 – 23	61.2	17.3	0.09
2 – 24	62.9	17.4	0.14
4 – 23	58.0	17.3	0.13
4 – 24	59.3	17.3	0.17

To investigate this further, a minimum distance constraint was imposed. The objective of this scenario is not to optimize the total distance but maximize the number of edges covered while visiting as many edges as possible. By imposing this minimum distance constraint, indirectly, a minimum number of edges to be covered by the robot is imposed. Further to the results shown in Table IX, a minimum distance constraint of 65 units was imposed. The results are shown in Table X. The probabilities (of detection) increased for all the cases compared to that of Table IX (maximum and unique edge constraint). This holds true when compared with the results from Table VIII (maximum distance constraint only) with two exceptions for the node pairs (2,23) and (2,24) where the probabilities were slightly reduced. However, note that the probability of detection significantly increased for the node pairs (4,23) and (4,24) from 0.27 to 1.0, implying the rogue sensor was detected in all the random paths. It can thus be concluded that maximizing the number of unique edges visited along with distance constraints produces the best results for the network considered for

randomized check-pointing of the robot. This is because the objective is to maximize the number of edges covered while at the same time consider real-world constraints (e.g., robot battery distance).

Table X. Likelihood of rogue sensor's detection with an average number of unique edges as 17 and maximum (100) and minimum (65) distance constraints.

Description	Average path distance	Average # of unique edges	$P(d)$
1 - 23	72.1	17.6	0.57
1 - 24	74.3	17.7	0.65
2- 23	68.0	17.7	0.33
2 - 24	70.3	17.8	0.38
4 - 23	80.0	17.4	1.00
4 - 24	80.3	17.5	1.00

VI. CONCLUSIONS

Several cyberattacks have already occurred in the AEC-FM industry with an intention to steal proprietary information, gain access to unauthorized files, and tamper existing records. With the proliferation of construction digitalization, cyberattacks will be on the rise. Construction professionals need to be able to identify and understand the fundamentals of these cyberattacks. This paper presents a preliminary threat modeling framework that can be used by construction experts with limited to no expertise in cybersecurity to determine some of the key cybersecurity components such as assets, attackers, threats, motivations, vulnerabilities, and countermeasures of construction activity or process. This is illustrated with the help of a building commissioning process. An on-demand autonomous mobile robotic data collection and validation approach is proposed to address the cybersecurity challenges faced during the testing process. The proposed approach has the capability to assist granting authorities (e.g., government or a third party) to validate the BMS data and possibly identify rogue sensors (e.g., tampered, manipulated, or improperly calibrated) during the testing process. Future work aims to test the proposed threat modeling framework for other construction phases such as construction, procurement, and operation and maintenance.

ACKNOWLEDGMENT

The authors would like to thank the support from the Center for Cyber Security (CCS) at New York University Abu Dhabi (NYUAD).

REFERENCES

Agarwal, A. (2016). Vast methodology: Visual, agile, and simple threat modeling. Various Interviews. Transformational Opportunities, Prescott Valley.

Aghimien, D., Aigbavboa, C., Oke, A., And Koloko, N. (2018). Digitalisation in Construction Industry: Construction Professionals Perspective, Available at: https://www.researchgate.net/profile/Douglas_Aghimien2/publication/329141252_DIGITALISATION_IN_CONSTRUCTION_INDUSTRY_CONSTRUCTION_PROFESSIONALS_PERSPECTIVE/links/5c02fc6f45851523d1569bca/DIGITALISATION-IN-CONSTRUCTION-INDUSTRY-CONSTRUCTION-PROFESSIONALS-PERSPECTIVE.pdf, Accessed on: September 19, 2019.

719 Ahr, D., and Reinelt, G. (2006). A tabu search algorithm for the min–max k-Chinese postman
720 problem. Computers & operations research, 33(12), 3403-3422, DOI:
721 https://doi.org/10.1016/j.cor.2005.02.011
722 AIA (The American Institute of Architects). (2007). Integrated Project Delivery: A Guide. V1.
723 Available at: https://info.aia.org//IPD_Guide_2007.pdf. Accessed on: March 19, 2019.
724 Alberts, C.; Dorofee, A.; Stevens, J; and Woody, C. (2003) Introduction to the OCTAVE
725 Approach. Software Engineering Institute, Carnegie Mellon University. August 2003.
726 https://re-sources.sei.cmu.edu/library/Asset-view.cfm?assetid=51546
727 Anumba, C. J., Akanmu, A., and Messner, J. (2010). Towards a cyber-physical systems approach
728 to construction. In Construction Research Congress 2010: Innovation for Reshaping
729 Construction Practice (pp. 528-537), DOI: https://doi.org/10.1061/41109(373)53.
730 Autodesk (2016) Construction process lifecycle Available at:
731 https://adsknews.autodesk.com/news/autodesk-adds-fusion-connect-and-fusion-lifecycle-
732 to-its-cloud-connected-product-innovation-platform. Accessed on: January 19, 2020.
733 BBC (2017), Ukraine power cut 'was cyber-attack', Available at:
734 https://www.bbc.com/news/technology-38573074, Accessed on: September 19, 2019.
735 Bennett, F. L. (2007). The management of construction: A project lifecycle approach. Routledge.,
736 ASIN: B00872DTE2.
737 Bilbo, D., Bigelow, B., Escamilla, E., and Lockwood, C. (2015). Comparison of construction
738 manager at risk and integrated project delivery performance on healthcare projects: A
739 comparative case study. International Journal of Construction Education and Research,
740 11(1), 40-53, DOI: http://dx.doi.org/10.1080/15578771.2013.872734.
741 Black P. E. (2017), "simple path", in Dictionary of Algorithms and Data Structures [online], Paul
742 E. Black, ed. 24 August 2017. (accessed TODAY) Available at:
743 https://www.nist.gov/dads/HTML/simplepath.html, Accessed on: June 1, 2019.
744 Bodeau D. J., McCollum C. D., and Fox D. B., (2018) Cyber Threat Modeling: Survey,
745 Assessment, and Representative Framework, The Homeland Security Systems Engineering
746 and Development Institute (HSSEDI)TM Operated by The MITRE Corporation, Available
747 at: https://www.mitre.org/publications/technical-papers/cyber-threat-modeling-survey-
748 assessment-and-representative-framework, Accessed on: August 8, 2019.
749 Boton, C., and Forgues, D. (2017). Construction industrialization and its integration: how tall wood
750 buildings can show the right path towards construction 4.0. In Proceedings of the 2017
751 Modular and Offsite Construction (MOC) Summit (Shanghai, China, Nov. 10-12, 2017),
752 pp. 201-207. Available at: http://espace2.etsmtl.ca/id/eprint/18344.
753 Boyes, H. (2013). Resilience and Cyber Security of Technology in the Built Environment. The
754 Institution of Engineering and Technology, IET Standards Technical Briefing, London.
755 Available at: https://www.theiet.org/resources/standards/-files/cyber-
756 security.cfm?type=pdf, Accessed on: July 9, 2019.
757 Brioso, X. (2015). Integrating ISO 21500 guidance on project management, lean construction and
758 PMBOK. Procedia Engineering, 123, 76-84, DOI:
759 https://doi.org/10.1016/j.proeng.2015.10.060.

760 Casey, W., Wright, E., Morales, J. A., Appel, M., Gennari, J., and Mishra, B. (2014). Agent-based
761 trace learning in a recommendation-verification system for cybersecurity. In 2014 9th
762 International Conference on Malicious and Unwanted Software: The Americas
763 (MALWARE) (pp. 135-143). IEEE. DOI:
764 http://doi.org/10.1109/MALWARE.2014.6999404.
765 Chudley, R., and Greeno, R. (2014). Building construction handbook. Routledge, ISBN-13: 978-
766 1138907096
767 Deng, M.; Wuyts, K.; Scandariato, R.; Preneel, B.; and Joosen, W. (2011), A Privacy threat
768 analysis framework: supporting the elicitation and fulfillment of privacy requirements.
769 Requirements Engineering. Volume 16. Issue 1. March 2011. Pages 3-32. DOI:
770 http://dx.doi.org/10.1007/s00766-010-0115-7
771 DHS (Department of Homeland Security), (2010), DHS Risk Lexicon: 2010 Edition Available at:
772 https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf, Accessed on: March 9,
773 2019
774 Farinacci, D., Fuller, V., Meyer, D., and D. Lewis (2013), "The Locator/ID Separation Protocol
775 (LISP)", RFC 6830, DOI: http://doi.org/10.17487/RFC6830, January 2013,
776 <https://www.rfc-editor.org/info/rfc6830>.
777 Fisk D. (2012). Cyber security, building automation, and the intelligent building, Intelligent
778 Buildings International, 4:3, 169-181, DOI:
779 https://doi.org/10.1080/17508975.2012.695277.
780 Garcia de Soto, B., Agustí-Juan, I., Hunhevicz, J., Joss, S., Graser, K., Habert, G., and Adey, B.
781 T. (2018). Productivity of digital fabrication in construction: Cost and time analysis of a
782 robotically built wall. Automation in Construction, 92, 297-311. DOI:
783 https://doi.org/10.1016/j.autcon.2018.04.004.
784 GDPR (General Data Protection Regulation) (2018) 2018 reform of EU data protection rules
785 Available at: https://ec.europa.eu/commission/priorities/justice-and-fundamental-
786 rights/data-protection/2018-reform-eu-data-protection-rules_en Accessed on: March 9,
787 2019.
788 Hearl, C. M. (2010). United States Special Operations Command (USSOCOM): Construction
789 Management Handbook (No. Nps-Cm-10-010). Naval Postgraduate School Monterey Ca
790 Graduate School of Business and Public Policy, Available at:
791 https://www.researchgate.net/publication/235174628_United_States_Special_Operations
792 _Command_USSOCOM_Construction_Management_Handbook, Accessed on:
793 September 20, 2019.
794 Hendrickson, C. and Au, T. (1989). Project management for construction: Fundamental concepts
795 for owners, engineers, architects, and builders. Chris Hendrickson, ISBN-13: 978-
796 0137312665.
797 Heo, Y., Choudhary, R., and Augenbroe, G. A. (2012). “Calibration of building energy models for
798 retrofit analysis under uncertainty.” Energy and Buildings, 47, 550-560, DOI:
799 https://doi.org/10.1016/j.enbuild.2011.12.029.
800 Hernan, S., Lambert, S., Shostack, A., and Ostwald, T (2006). Uncover Security Design Flaws
801 Using the STRIDE Approach. MSDN Magazine., Available at:

http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=516617, Accessed on: June 22, 2019.

Hutchins, M. J., Bhinge, R., Micali, M. K., Robinson, S. L., Sutherland, J. W., & Dornfeld, D. (2015). Framework for identifying cybersecurity risks in manufacturing. Procedia Manufacturing, 1, 47-63. DOI: http://dx.doi.org/10.1016/j.promfg.2015.09.060.

Ibbs, C. W., Kwak, Y. H., Ng, T., and Odabasi, A. M. (2003). Project delivery systems and project change: Quantitative analysis. Journal of Construction Engineering and Management, 129(4), 382-387, DOI: http://dx.doi.org/10.1061/(ASCE)0733-9364(2003)129:4(382).

IET (Institution of Engineering and Technology) Standards (2013), Resilience and Cyber Security of Technology in the Built Environment, Institution of Engineering and Technology/CPNI, 2013, Available at: https://www.theiet.org/publishing/iet-standards/?utm_source=redirect&utm_medium=legacyredirects&utm_campaign=2019relaunch&type=pdf, Accessed on: May 2, 2019.

International Telecommunication Union (ITU) (2019), Definition of cybersecurity. Available at: https://www.itu.int/cybersecurity.aspx Accessed on: July 03, 2019.

iSqFt (2016), Data Breaches, Cyber Security and the Construction Industry, Available at: https://www.isqft.com/start/blog-data-breaches-cyber-security-and-the-construction-industry/, Accessed on: December 9, 2019.

Jia, M., Komeily, A., Wang, Y., and Srinivasan, R. S. (2019). "Adopting Internet of Things for the development of smart buildings: A review of enabling technologies and applications." Automation in Construction, 101, 111-126. DOI: http://dx.doi.org/10.1016/j.autcon.2019.01.023.

Khan, R.; McLaughlin, K.; Laverty, D.; and Sezer, Sakir (2017), STRIDE-based Threat Modeling for Cyber-Physical Systems. In Proceedings of the 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe. September 2017. DOI http://dx.doi.org/10.1109/ISGTEurope.2017.8260283.

Kohnfelder, L. and Garg, P. (1999), 'The threats to our products', Microsoft Interface, Microsoft Corporation p. 33.

Li, X., Zhou, C., Tian, Y.-C., Xiong, N., and Qin Y. (2018). Asset-Based Dynamic Impact Assessment of Cyberattacks for Risk Analysis in Industrial Control Systems, IEEE Transactions on Industrial Informatics, 14(2), pp. 608-618, DOI: https://doi.org/10.1109/TII.2017.2740571.

Liu, J., Wang, D., Zhang, C., Tang, Z., and Xiang, Y. (2017). Reliability Assessment of Cyber Physical Distribution System, Energy Procedia, Volume 142, pp. 2021-2026, DOI: https://doi.org/10.1016/j.egypro.2017.12.405

Mantha B. R., and, Garcia de Soto., B. (2019a). Cyber security challenges and vulnerability assessment in the construction industry. In Proceedings of the 2019 Creative Construction Conference, June 29 – July 2, 2019, Budapest, Hungary, Available at: https://repozitorium.omikk.bme.hu/bitstream/handle/10890/13197/CCC2019-005.pdf?sequence=1&isAllowed=y

Mantha B. R., and, Garcia de Soto., B. (2019b). 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., Menassa, C. C., and Kamat, V. R. (2018). Multi-Robot Task Allocation and Route Planning for Indoor Building Environment Applications. In Construction Research Congress, pp 137-146, April 2–4, 2018, New Orleans, Louisiana, USA, DOI: http://dx.doi.org/10.1061/9780784481264.014.

Mantha, B. R., Menassa, C. C., Kamat, V. R., and D'Souza C. R. (2019) "Evaluation of Preference and Constraint-Sensitive Path-Planning for Assisted Navigation in Indoor Building Environments", Journal of Computing in Civil Engineering, 34(1), 04019050, DOI: http://dx.doi.org/10.1061/(ASCE)CP.1943-5487.0000865.

Mead, N., Shull, F., Vemuru, K., and Villadsen, O. (2018). A Hybrid Threat Modeling Method. Carnegie Mellon University-Software Engineering Institute-Technical Report-CMU/SEI-2018-TN-002. Available at: https://128.237.30.12/asset_files/TechnicalNote/2018_004_001_516627.pdf, Accessed on: June 29, 2019.

Mesároš, P., Mačková, D., Spišáková, M., Mandičák, T., and Behúnová, A. (2016). M-learning tool for modeling the building site parameters in mixed reality environment. In 2016 International Conference on Emerging eLearning Technologies and Applications (ICETA) (pp. 211-216). IEEE, DOI: http://dx.doi.org/10.1109/ICETA.2016.7802094.

Motley, C., and Mas, I. P. (2017). Key Issues for Lawyers as Cyber Risk Leaders. American Bar Association Forum on Construction Law. 2017 Annual Program. April 20-22, 2017. JW Marriott, Washington, DC.

NIST (National Institute of Standards and Technology). (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf, Accessed on: May 13, 2019.

Nobert, Y., and Picard, J. C. (1996). An optimal algorithm for the mixed Chinese postman problem. Networks: An International Journal, 27(2), 95-108, DOI: https://doi.org/10.1002/(SICI)1097-0037(199603)27:2<97::AID-NET1>3.0.CO;2-8.

Oberlender, G. D (1993). Project management for engineering and construction (Vol. 2). New York: McGraw-Hill, ISBN-13: 978-0071822312.

Osunsanmi, T., Aigbavboa, C., and Oke, A. (2018). Construction 4.0: the future of the construction industry in South Africa. World Academy of Science, Engineering and Technology, International Journal of Civil and Environmental Engineering, 12(3), 206-212. DOI: https://doi.org/10.5281/zenodo.1315923.

Parn, E., and Edwards D. (2019). Cyber threats confronting the digital built environment: Common data environment vulnerabilities and block chain deterrence, Engineering, Construction and Architectural Management. DOI: https://doi.org/10.1108/ECAM-03-2018-0101.

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

885 at: https://www.cpni.gov.uk/system/files/documents/18/6f/BIM-Introduction-To-
886 PAS1192-5.pdf, Accessed on: May 2, 2019.
887 Pash C. (2018) How hackers and spies tried to steal the secrets of Australia's one-armed robot
888 bricklayer, Available at: https://www.businessinsider.com.au/one-armed-bricklaying-
889 robot-security-secrets-2018-11#VvEiLeDRcbrblGKj.99, Accessed on: May 2, 2019
890 Rastogi, S. (2017) Construction 4.0: The 4th Generation Revolution, Indian Lean Construction
891 Conference – ILCC 2017, Available at:
892 Https://Www.Researchgate.Net/Profile/Subhash_Rastogi3/Publication/331131645_CON
893 STRUCTION_40_THE_4_Th_GENERATION_REVOLUTION/Links/5c66ca2592851c
894 1c9de43efa/CONSTRUCTION-40-THE-4-Th-GENERATION-REVOLUTION.Pdf,
895 Accessed on: January 10, 2020.
896 Ries, R., and Mahdavi, A. (1999). The "Ecologue" Approach to Computational Building Life
897 Cycle Analysis. Nakahara, Yoshida, Udagawa and Hensen, ed. Building Simulation, 99,
898 13-15.
899 Sawyer, T. and Rubenstone, J. (2019). Construction Cybercrime is on the Rise. Engineering News-
900 Record. BNP Media. Available at: https://www.enr.com/articles/46832-construction-
901 cybercrime-is-on-the-rise. Accessed on: January 14, 2020.
902 Shevchenko, N., Chick, T. A., O'riordan, P., Scanlon, T. P., and Woody, C. (2018). Threat
903 Modeling: A Summary of Available Methods, Available at:
904 https://resources.sei.cmu.edu/asset_files/WhitePaper/2018_019_001_524597.pdf,
905 Accessed on: January 10, 2020.
906 Shostack (2014), A. Threat Modeling: Designing for Security. Wiley, 2014. ISBN 978-
907 1118809990
908 Tang, J., Ibrahim, M., Chakrabarty, K., and Karri, R. (2018). Toward Secure and Trustworthy
909 Cyberphysical Microfluidic Biochips. IEEE Transactions on Computer-Aided Design of
910 Integrated Circuits and Systems, 38(4), 589-603, DOI:
911 http://dx.doi.org/10.1109/TCAD.2018.2855132.
912 Tanko, B. L., Abdullah, F., and Ramly, Z. M. (2018). "Benefits of Adopting Value Management
913 to Mitigate the Problems in the Nigerian Construction Industry." Advanced Science
914 Letters, 24(5), 3818-3822. DOI: https://doi.org/10.1166/asl.2018.11490
915 UcedaVélez, T. (2012), Real World Threat Modeling Using the PASTA Methodology. Technical
916 report. Open Web Application Security Project (OWASP). 2012. Available at:
917 https://www.owasp.org/images/a/aa/AppSecEU2012_PASTA.pdf, Accessed on: May 18,
918 2019.
919 UcedaVélez, T. and Morana, M. M. (2015) Risk Centric Threat Modeling: Process for Attack
920 Simula-tion and Threat Analysis. Wiley. 2015. ISBN 978-0-470-50096-5.
921 Ullah, F., Edwards, M., Ramdhany, R., Chitchyan, R., Babar, M. A., & Rashid, A. (2018). Data
922 exfiltration: A review of external attack vectors and countermeasures. Journal of Network
923 and Computer Applications, 101, 18-54. https://doi.org/10.1016/j.jnca.2017.10.016.
924 Watson (2018), Cyber-security: What will it take for construction to act? Available at:
925 https://www.constructionnews.co.uk/tech/cyber-security-what-will-it-take-for-
926 construction-to-act-22-01-2018/?search=https%3..., Accessed on: September 19, 2019.