Is Your Construction Site Secure? A View From the Cybersecurity Perspective

M. S. Sonkor[a] and B. García de Soto[a]

[a] S.M.A.R.T. Construction Research Group, Division of Engineering, New York University Abu Dhabi (NYUAD), Experimental Research Building, Saadiyat Island, P.O. Box 129188, Abu Dhabi, United Arab Emirates
E-mail: semih.sonkor@nyu.edu, garcia.de.soto@nyu.edu

Abstract –

The construction industry is increasingly using information technologies (IT) and operational technologies (OT) to enhance processes and operations through digitalization. Creating, editing, storing, and sharing information in digital environments is only one side of the coin; the other involves monitoring and controlling physical processes on construction sites. Given the nature of construction sites, where humans and machines/equipment work collaboratively, safety concerns arise. Utilizing interconnected and cyber-physical systems such as (semi)autonomous and remote-controlled machines on-site magnifies the importance of robust cybersecurity. Therefore, it becomes necessary to understand the threats against each networked equipment, analyze the vulnerabilities, assess the risks, and provide mitigation methods. Cybersecurity frameworks are effective solutions for this purpose; however, they are usually generic and thus require customization to be employed in the construction site environment.

Against this background, this paper reviews existing cybersecurity frameworks/standards and selects the most suitable one to implement in the construction environment. The implementation was performed by customizing the selected generic framework considering the needs of a hypothetical construction site that utilizes autonomous earthmoving equipment. For the evaluation, a scoring system that was not included in the original framework was proposed. Given the paucity of studies in this field and lack of cybersecurity awareness in the construction industry, this study aims (1) to raise awareness about the potential cyber threats against construction sites that are increasingly interconnected, (2) to point out the need for a customized cyber assessment method on-site, and (3) help building a security-minded approach within the construction industry.

Keywords –

Construction 4.0; Cybersecurity; Cyber-Physical Systems; Cybersecurity Frameworks; Vulnerability Assessment; Autonomous Earthmoving Equipment

1 Introduction

Construction is one of the industries that has been increasingly globalized over the years with the advances in transportation and communication, and with trade agreements, leading to an increasing interconnectedness across countries [1]. The increasing globalization forces construction companies to re-engineer their processes and utilize novel technologies to stay competitive [2]. These technologies transform the way data is created, stored, and exchanged and how construction activities are performed, controlled, and monitored. The efforts to employ increasingly digitized processes in the construction industry are often called Construction 4.0, and the use of cyber-physical systems (CPSs) is an essential component of it [3].

Some potential benefits of digitalization in construction projects are cost efficiency, reduced durations, improved quality, and enhanced site activity tracking. On the other hand, cyber threat surface increases with the use of common data environments (CDEs) to exchange information in cyberspace and networked CPSs to perform different tasks during the construction and operation & maintenance (O&M) phases.

Information technologies (IT) and operational technologies (OT) domains have been isolated from each other for many years [4]. However, the need for enhanced performance, reduced costs, and improved control over the operations necessitated IT-OT convergence [4]. It is possible to see the examples of this convergence on construction sites, such as retrofitting legacy equipment with control systems (e.g., conventional excavators retrofitted with sensors and control units for autonomous operation) and employing new equipment designed with both IT and OT components (e.g., 3D concrete printers,

autonomous earthmovers, automated site-measuring robots, reinforcement positioning robots [5]). The report published by Trend Micro Research [6], analyzing the security levels of remote controllers used in industrial applications, indicates that millions of vulnerable radio frequency (RF) remote controllers are installed on heavy machinery in various industries, including construction. Long life spans of industrial equipment and high replacement costs lead companies to retrofit their legacy machinery with these remote controllers [6], which results in significant cybersecurity vulnerabilities. State-of-the-art equipment designed to operate connected to a network comes with enhanced cybersecurity and protection against known threats; however, evolving cyber threat-environment requires companies to stay cautious and proactive [7].

So far, several studies have been conducted to research cybersecurity aspects of OT utilized in environments such as manufacturing, water treatment plants, and smart buildings. The common point of all these environments is that they are more structured and stable than construction sites. The changing environment and lack of stability on-site [8] increase the challenge of providing robust cybersecurity during the construction phase. In addition, the collaboration between humans and machines raises safety concerns [8] considering potential cyber-physical attacks. Therefore, understanding the potential threats against OT on construction sites, detecting security vulnerabilities, and providing mitigation methods are paramount. A few studies have focused on the OT cybersecurity aspects of construction sites, such as [9] that proposed a preliminary threat modeling method for construction projects based on the Quantitative Threat Modeling Method (QuantitativeTMM) and demonstrated it with a 3D concrete printer, [10][11] that implemented the Common Vulnerability Scoring System (CVSS) to evaluate and quantify the vulnerabilities of construction networks, [12] that investigated the gaps in the cybersecurity of OT utilized in construction and suggested future directions for the industry and academia, and [13] that pointed out the potential physical damages that might occur as a result of hijacked autonomous construction equipment. To the authors' knowledge, there is no previous study investigating the use of cybersecurity frameworks during the construction phase.

This study proposes implementing a generic cybersecurity framework considering the characteristics of construction sites utilizing autonomous earthmoving equipment (AEE). The implementation was performed only considering AEE to keep it more specific. A hypothetical site with AEE was designed to demonstrate the practical aspects of the proposed implementation. The rest of this paper is structured as follows. Section 2 provides summaries of the prominent cybersecurity standards/frameworks, presents the selection process of a suitable generic cybersecurity framework to employ in this study, and gives a brief overview of the selected framework and its structure. Section 3 explains the implementation of the selected framework on the designed hypothetical construction site and demonstrates it step by step. In Section 4, the provided implementation is discussed considering its benefits for the construction sector and its limitations to be further studied. Finally, Section 5 presents the conclusions and planned future work.

2 Cybersecurity Frameworks/Standards

The increasing need for identifying cyber vulnerabilities and threats, assessing the level of cybersecurity, protecting the assets from potential attacks, and managing risks requires a well-organized and systematic approach. For this reason, many organizations and government bodies developed cybersecurity frameworks and standards. In addition, some governments enforce compliance with a cybersecurity standard. For example, in 2018, the United Kingdom (UK) government published the Minimum Cyber Security Standard (MCSS) [14] to set the minimum requirements expected to be accomplished by government departments. However, cybersecurity frameworks/standards are invaluable for companies to assess where they stand compared to the best practices even without legal obligations. Some local and international institutions developing such guidelines are the National Institute of Standards and Technology (NIST), National Cybersecurity Centre (NCSC), Institution of Engineering and Technology (IET), International Electrotechnical Commission (IEC), and International Organization for Standardization (ISO). Relevant documents from these institutions are summarized next.

2.1 Review of Cybersecurity Frameworks and Standards

This section presents the most prominent cybersecurity frameworks/standards developed by government bodies and internationally recognized non-governmental organizations. These documents were reviewed considering their suitability to the construction site environment. Additionally, their usefulness for assessing OT cybersecurity was considered since this research particularly focuses on the potential threats against OT utilized on-site.

ISO/IEC 27001:2013: This standard [15] provides a set of requirements for companies to establish and maintain an information security management system (ISMS). It is a generic standard and targets organizations of all sizes

from all sectors regardless of their work environment. The standard employs the "Plan-Do-Check-Act" model to structure the processes of ISMS. The organizations that claim conformity to this standard are expected to meet all given requirements or provide justification and evidence if they exclude any of them.

ISO 19650-5:2020: This international standard [16] provides a guideline for a security-minded approach in construction projects and built environments that utilize building information modeling (BIM) processes. One of the focuses of this document is the cybersecurity of the sensitive information exchanged during the lifecycle of built environments from the design to O&M phases. While ISO/IEC 27001 sets out generic information security requirements that can be applied across various sectors, ISO 19650-5 differentiates itself by targeting collaborative data sharing processes of the built environment industry.

Cyber Assessment Framework v3.0 by NCSC: This is an extensive framework [17] published by NCSC (UK) in 2019 and designed to be utilized for the cybersecurity assessment of organizations by their internal teams or by third-party companies. The assessment structure includes four main objectives: protecting against cyber-attack, managing security risk, detecting cybersecurity events, and minimizing the impact of cybersecurity incidents. Overall, there are fourteen principles under these main objectives that are broken down into thirty-nine contributing outcomes for a detailed assessment. The organizations using this framework are expected to evaluate whether each contributing outcome is achieved, partially achieved, or not achieved.

Network and Information Systems (NIS) Directive by the European Union (EU): This is a legislative document [18] that aims to enhance the overall cybersecurity within the EU. More specifically, it requires each member state to improve its national cybersecurity by adopting a national information system and network security strategy. Moreover, it promotes EU-level cooperation among the member states for improved cybersecurity. It also sets out requirements for reporting incidents and risk management for essential and digital service providers.

Code of Practice for Cyber Security in the Built Environment by IET: This code of practice [19], published in 2014, provides cybersecurity guidance to the stakeholders involved throughout the lifecycle of built environments. It analyzes the specific cybersecurity needs, potential threats, hostile agents to be considered for each building lifecycle phase. Additionally, different aspects such as the procedures, the involvement of humans in the processes, cybersecurity policies for buildings, and the trustworthiness of utilized software are discussed in the built environment context.

Framework for Improving Critical Infrastructure Cybersecurity v1.1 by NIST: This document by NIST [20] addresses the cybersecurity risks associated with critical infrastructures (CIs) and aims to provide a flexible, repeatable, and voluntarily applied framework to CI owners and operators. It has three main parts: the Framework Profiles, the Implementation Tiers, and the Framework Core. The Framework Core uses various references such as industry standards and guidelines to help companies identify their current profiles and prioritize cybersecurity activities to achieve their targets.

2.2 Selection of the Suitable Cybersecurity Framework

Given each document's scopes and brief overviews presented above, a comparison has been conducted to choose the most suitable option for this study. The review of ISO/IEC 27001:2013 shows that it mainly focuses on the information security aspects, as its name suggests. Therefore, it does not adequately address the OT-specific cybersecurity issues on-site. The NIS Directive by the EU provides an extensive set of requirements; however, its structure is not as modifiable as the other reviewed documents. Finally, the Code of Practice for Cyber Security in the Built Environment by IET thoroughly addresses both IT and OT security aspects in all phases of built environments. However, it does not provide a structured framework format that can be utilized to create a checklist for cyber assessment. As a result, although these three documents are comprehensive enough, they do not meet the requirements of this study.

The remaining documents—ISO 19650-5, the Cyber Assessment Framework by NCSC, and the Framework for Improving Critical Infrastructure Cybersecurity (FICIC) by NIST—address both IT and OT cybersecurity aspects, which increases their suitability for this research. In addition, they all can be used for creating bespoke cyber assessment checklists for organizations due to their well-organized and flexible structures. However, the FICIC differs from the other two in a significant way: its ability to use the related frameworks and standards. The informative references in the Framework Core (e.g., ISO/IEC 27001:2013, NIST SP 800-53 Rev. 4) allow users to go through the sections of different sources relevant to each category (e.g., Risk Assessment (ID.RA), Response Planning (RS.RP)), and subcategory (e.g., ID.RA-3: Threats, both internal and external, are identified and documented). Furthermore, the FICIC is "[…] *applicable to organizations relying on technology, whether their cybersecurity focus is primarily on information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), or connected devices more generally, including the Internet of Things (IoT)*" [24, p. vi], which adequately addresses the cybersecurity issues escalating with the utilization of automated equipment on construction sites. For these

reasons, this study employs the FICIC v1.1 by NIST for the implementation and demonstration steps presented in Section 3.

2.3 Overview of the Selected Cybersecurity Framework

The FICIC encompasses three main components with different purposes. These components are briefly explained as follows:

Framework Core: This framework component provides a group of outcomes to achieve better cybersecurity management and introduces reference documents as guidelines. The Framework Core has four main parts, namely Functions, Categories, Subcategories, and Informative References. The structure of the Framework Core and five different functions can be seen in Figure 1.

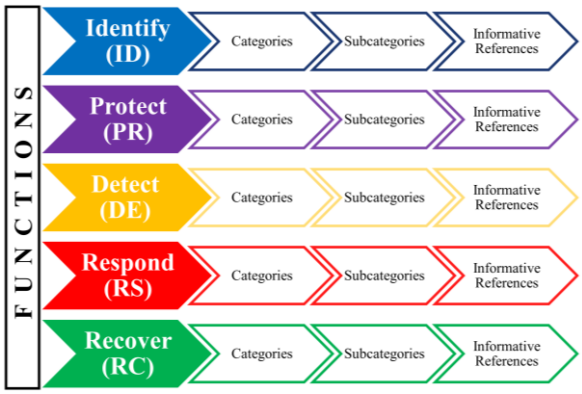

Figure 1. Structure of the Framework Core of the FICIC (adapted from [20])

In total, there are 23 categories and 108 subcategories, and several informative references are presented under each subcategory. The Framework Core does not provide a checklist with questions to assess the current cybersecurity level. Instead, it guides organizations to create their assessment schema by providing different cybersecurity aspects in each subcategory and related reference documents. Moreover, it allows for flexibility by letting organizations customize the framework by selecting the necessary subcategories and references for their particular needs. As an example, Table 1 presents a section from the Framework Core that includes two subcategories under the Risk Assessment category in the Identify function.

Implementation Tiers: The implementation tiers indicate to which extent the organization implements cybersecurity risk management practices in its processes. There are four tiers: Tier 1-Partial, Tier 2-Risk Informed, Tier 3-Repeatable, and Tier 4-Adaptive. Organizations are suggested to take necessary actions to progress towards higher tiers if their cost-benefit analysis also supports it. Therefore, organizations can decide on their target tier by determining the most cost-effective solution.

Table 1. Section from the Framework Core of the FICIC for a specific function, category, subcategory, and related informative references

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Risk Assessment (ID.RA)	ID.RA-1: Asset vulnerabilities are identified and documented	**CIS CSC** 4 **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 **NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	**CIS CSC** 4 **COBIT 5** BAI08.01 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.6.1.4 **NIST SP 800-53 Rev. 4** SI-5, PM-15, PM-16

Framework Profiles: The profiles show the alignment of an organization's risk tolerance and commercial requirements with the outcomes in the Framework Core. Organizations can identify their Current Profile by assessing which outcomes from the Framework Core are currently achieved. Next, the Target Profile for reducing cybersecurity risks can be established considering the company's business-specific needs and cyber-risk tolerance. After the Current and Target Profiles are identified, an action plan can be prepared to bridge the gaps starting from the business priorities.

3 Implementation of the Selected Cybersecurity Framework

As the FICIC by NIST has been developed to suit the needs of various industries and work environments, it includes different generic categories and subcategories that must be customized for specific applications. For this study, a hypothetical scenario was created considering the ongoing adoption of new technologies in construction sites, and the customization of the framework was performed based on this scenario. The scenario assumes a construction site that utilizes AEE to support earthworks activities. AEE is chosen for the hypothetical scenario since automating repetitive earthworks tasks has been a trending construction automation topic in the last decades. The mining industry was one of the first to employ the use of self-driving tech. For instance, Caterpillar started with its automation program more than 30 years ago. More recent examples include the works by [21] that proposed using a time-delayed neural network architecture for automatic bucket-filling and demonstrated it with a wheel-loader and [22] that introduced an autonomous excavator system that can perform earthmoving tasks for long durations without any human intervention. In addition, heavy equipment manufacturers, such as Komatsu and Caterpillar, and

start-ups such as Built Robotics, are working on making self-driving bulldozers and excavators common on construction sites.

3.1 Hypothetical Construction Site with an Autonomous Earthmover

The hypothetical construction site considered in this study is presented in a diagram shown in Figure 2. Different elements of the diagram and their roles in the hypothetical scenario are explained as follows:

A. Control Room: The control room serves as a bridge between the autonomous equipment and the technical office. There is an operator in the control room who manages the human-machine interface. As the monitored equipment is assumed to be autonomous—not semi-autonomous or teleoperated—the human-machine interface (HMI) aims to provide interactive oversight over the equipment's actions and allows the operator to intervene only when necessary [23]. Therefore, the operator can simultaneously manage multiple machines by following the notification system without actively monitoring all of them [23].

B. CDE: The CDE of the construction project provides a centralized platform for simultaneous data exchange between different stakeholders. The HMI is connected to the CDE and the AEE via a wireless communication network. The type of wireless network is assumed to be 5G due to the low latency and high mobility requirement [24].

C. Technical Office: The technical office exchanges data with the HMI over the CDE. For example, the HMI can receive the BIM model from the CDE and send the required directions to the AEE related to the excavation and fill operations to be executed based on the information and requirements from the BIM model and planned schedule. Similarly, the technical office can access the excavation/fill amount performed by the AEE to date (and in real-time).

D. AEE: As suggested by [8], it is assumed that the control system of the AEE has three main units, namely the vision unit, control unit, and execution unit. The vision unit receives data from the Light Detection and Ranging (LiDAR) system and cameras placed on the AEE for object detection and collision avoidance and passes the collected data to the control unit for further processing. The execution unit receives data from the real-time location systems (e.g., Global Positioning System (GPS), Ultra-Wideband) for accurate positioning [25] and from the pressure sensors to measure the reaction forces on the bucket [21]. The control unit conveys the vision unit data and the execution commands received from the HMI to the execution unit. Finally, the execution unit sends the required commands to the actuators (e.g., boom actuator, arm actuator, bucket actuator), steering, brakes, and accelerator.

E. Other equipment and workers on-site: The AEE interacts with other equipment and workers on-site, which increases the significance of providing robust cybersecurity for the communication network.

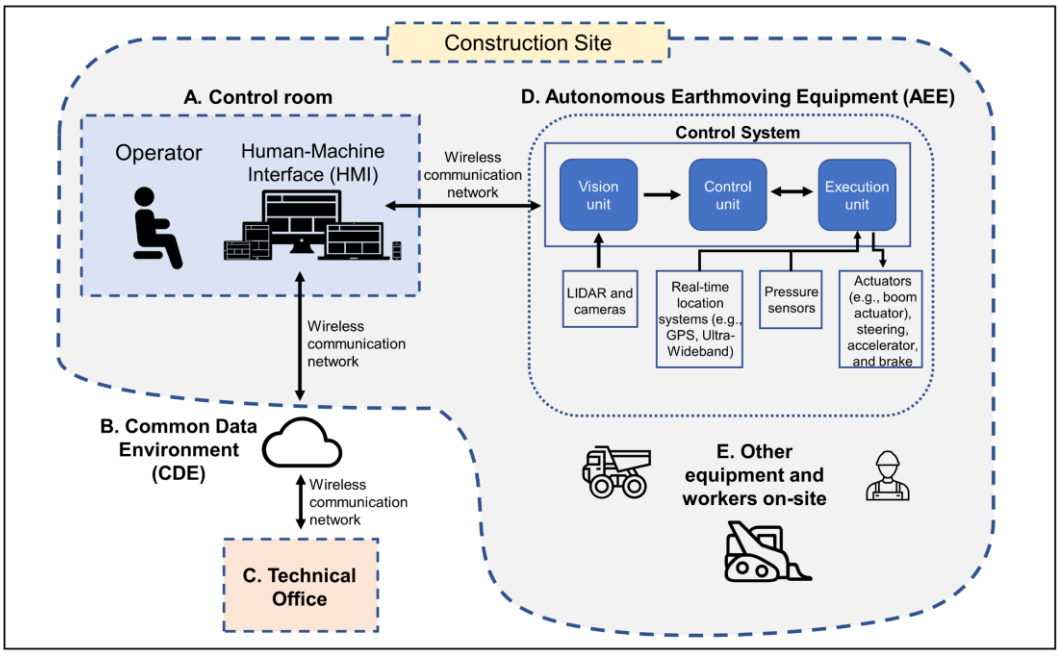

Figure 2. Diagram of the different components for the hypothetical construction site used in this study

3.2 Customization of the Framework

To customize the Framework Core, initially, the most relevant categories from each function and the most suitable subcategories from the selected categories were selected considering the characteristics of the hypothetical construction site. The selected categories and subcategories are shown in Table 2. This study does not intend to go over all functions, categories, and subcategories but to show a couple of applications as examples. In particular, the number of selected subcategories chosen was nine (Table 2). Of course, in real-life applications, these categories and subcategories can be extended to cover a broader range of cybersecurity aspects and increase the assessment's accuracy depending on the project needs.

Table 2. Selected Subcategories for Customization

Function	Category	Subcategory
IDENTIFY (ID)	Asset Management (ID.AM)	**ID.AM-5:** Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value
	Risk Assessment (ID.RA)	**ID.RA-1:** Asset vulnerabilities are identified and documented **ID.RA-3:** Threats, both internal and external, are identified and documented
PROTECT (PR)	Identity Management, Authentication and Access Control (PR.AC)	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
	Maintenance (PR.MA)	**PR.MA-1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools
DETECT (DE)	Anomalies and Events (DE.AE)	**DE.AE-2:** Detected events are analyzed to understand attack targets and methods
	Security Continuous Monitoring (DE.CM)	**DE.CM-1:** The network is monitored to detect potential cybersecurity events
RESPOND (RS)	Response Planning (RS.RP)	**RS.RP-1:** Response plan is executed during or after an incident
RECOVER (RC)	Recovery Planning (RC.RP)	**RC.RP-1:** Recovery plan is executed during or after a cybersecurity incident

Following the selection of the categories and subcategories, an additional column was added to the Framework Core to include questions, which is not included in the original FICIC. These questions aim to assess the implementation level of the outcomes in each subcategory and transform the Framework Core into a checklist format. Thus, the utilization of the framework becomes more practical, and the evaluation of the different cybersecurity practices being implemented is facilitated.

Several questions were created by going through the provided informative references. For example, two questions were created for the subcategory "ID.RA-1: Asset vulnerabilities are identified and documented" under the Risk Assessment category in Identify function (Table 3). Initially, each informative reference provided in the Framework Core for the subcategory "ID.RA-1" was scrutinized to find the appropriate options for the demonstrated construction site scenario in Figure 2. The Framework Core provides five different documents and their relevant sections for this subcategory. Two sections from two different documents were selected for creating Q3 and Q4 presented in Table 3: Section 4 (i.e., Continuous Vulnerability Assessment and Remediation) of the Center for Internet Security (CIS) Critical Security Controls (CSC) and Section CA-8 (i.e., Penetration Testing) of NIST SP 800-53 Rev. 4. The former suggests scanning the network for vulnerabilities with an automated tool on a weekly basis or more often. The latter recommends conducting penetration testing on the required systems with an organization-defined frequency. The mentioned suggestions were converted into questions to evaluate the security of the network that connects the HMI and AEE (Figure 2) on the hypothetical site, considering this connection's safety-critical role. Table 3 shows Q3, Q4, and four other questions created with the explained logic.

The questions created during the customization of the framework have a crucial role in developing a cybersecurity assessment checklist. However, the assessment also needs to provide a structured way to answer these questions to interpret the results better. Therefore, the following subsection proposes an evaluation method to address this need.

Table 3. Section of the customized Framework Core with questions

Function	Category	Subcategory	Informative References	Questions
IDENTIFY (ID)	Asset Management (ID.AM)	**ID.AM-5:** Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and	**NIST SP 800-53 Rev. 4** SA-14 **CIS CSC** 14	**Q1.** Is there a functional criticality analysis in place to assess the most critical components of the network that connects the AEE and HMI? **Q2.** Do all network switches allow Private Virtual Local Area Networks (VLANs) to limit the communication between the components of the AEE and the private devices connected to the same network?
	Risk Assessment (ID.RA)	**ID.RA-1:** Asset vulnerabilities are identified and documented	**CIS CSC** 4 **NIST SP 800-53 Rev. 4** CA-8	**Q3.** Is there an automated vulnerability scanning tool employed to scan the network that connects the AEE and HMI on a weekly-basis? **Q4.** Does the organization conduct penetration testing on the network connecting the AEE and HMI in a monthly basis to detect potential vulnerabilities?
		ID.RA-3: Threats, both internal and external, are identified and documented	**NIST SP 800-53 Rev. 4** PM-16 **NIST SP 800-53 Rev. 4** PM-12	**Q5.** Is there a threat awareness program in place to inform the employees about the constantly changing threat environment targeting the CPSs utilized on construction sites? **Q6.** Is there an insider threat program in place to continously monitor critical systems (including the systems linked to the AEE) and detect potential malicious insider activity?

3.3 Evaluation Method

For assessing the cybersecurity implementation level of the construction site, a score-based evaluation method is proposed in this study. According to the proposed method, there are five different implementation levels to

be selected in response to each question under each subcategory. The Implementation Tiers of the FICIC were partially considered while deciding on the implementation levels in the score-based evaluation method. These implementation levels and the corresponding scores can be seen in Figure 3.

SCORECARD	
0	No awareness
1	Awareness without implementation
2	Partial implementation
3	Full and repeatable implementation
4	Adaptive Implementation

Figure 3. The scorecard to be used for evaluation

Different scores presented in Figure 3 are explained as follows:

0 – There is no awareness about the mentioned cybersecurity practice.

1 – There is awareness about the mentioned cybersecurity practice; however, there is no current implementation.

2 – The mentioned cybersecurity practice is not formalized but partially implemented and utilized on an ad-hoc basis.

3 – The mentioned cybersecurity practice is formally approved and updated regularly.

4 – There is a continuous adaptation of the mentioned cybersecurity practice into the changing threat landscape. Lessons learned and predictive tools are utilized to improve the implemented practices.

The average scores for each category and subcategory are calculated and used to identify gaps between the current practices and targets. The score-based evaluation also allows obtaining a qualitative overview of different cybersecurity practices' current implementation levels (i.e., low score = low implementation level, and vice versa), thus channeling resources into the required areas and prioritizing cybersecurity actions.

3.4 Demonstration of the Evaluation Method

A demonstration of the evaluation method described in the previous subsection is presented in Figure 4, considering the hypothetical construction site. The responsible person for the cybersecurity assessment on-site is assumed to conduct this evaluation, and his/her hypothetical scores are shown in Figure 4.

The scores shown in Figure 4 indicate the implementation levels of the cybersecurity practices covered in each category and subcategory. For example, according to the scores in Figure 4, the Asset Management-related cybersecurity practices are implemented at a lower level—1.5 on average—than the ones related to the Risk Assessment—2.25 on average. Based on the scores and the organization's priorities, a roadmap can be developed to improve the low-scored cybersecurity practices and achieve the target levels.

Function	Category	Average Category Scores	Subcategory	Average Subcategory Scores	Questions	Scores
IDENTIFY (ID)	Asset Management (ID.AM)	1.5	ID.AM-5	1.5	Q1	1
					Q2	2
	Risk Assessment (ID.RA)	2.25	ID.RA-1	3	Q3	3
					Q4	3
			ID.RA-3	1.5	Q5	2
					Q6	1

Figure 4. Demonstration of the evaluation method

4 Discussion and Limitations

The customization of the framework—including the questions created for each subcategory—and the proposed evaluation method—that was not included in the original framework—provides an efficient way to assess the implementation levels of different cybersecurity practices on construction sites that utilize OT. As demonstrated in Section 3.4, the assessment results aim to guide the organization to set a roadmap towards a more secure construction site. Scores for each question lead to the average scores of subcategories and categories, as shown in Figure 4.

The average scores show where the construction site stands in terms of the evaluated cybersecurity practices. However, the scores by themselves are not sufficient for a thorough evaluation. Deciding on the actions to improve the current cybersecurity level also requires setting target levels for each practice. These targets can be set by the cybersecurity experts and the project management team based on the priorities and risk appetite of the organization. In this study, a methodology for setting targets is not provided, which is a limitation. Another limitation is using equal weights for each question, subcategory, and category. Assigning different weights for each aspect would lead to a more comprehensive evaluation. Finally, having one person conducting the assessment instead of a group of evaluators with mixed backgrounds reduces the accuracy of the results.

5 Conclusions and Future Work

There has been a lack of attention from the industry and academia towards the cybersecurity aspects of the construction industry. Moreover, to the best of the authors' knowledge, the implementation of cybersecurity frameworks on construction sites has never been discussed in the previous studies. Therefore, this study targets to raise awareness about the potential cybersecurity vulnerabilities of construction sites—that

are increasingly interconnected and automated—and points out the need for customized cyber assessment frameworks to evaluate these vulnerabilities and mitigate them. With this purpose, an implementation of a generic cybersecurity framework (i.e., the FICIC by NIST) that assesses the employed countermeasures against the construction-specific cyber threats was presented in this paper. The implementation included customizing the existing framework (i.e., selecting the necessary categories and subcategories and adding questions to each subcategory), proposing a score-based evaluation method—which was not included in the original document—and demonstrating the assessment on a hypothetical construction site that utilizes AEE.

Future work will extend this study to include a complete evaluation, covering more subcategories, categories, and functions. Also, a more comprehensive scoring system—where each cybersecurity aspect has an individual weight, and a mixed group of evaluators conducts the assessment—will be proposed for more accurate results. This paper did not include an implementation on a real construction site since the primary purpose was to direct the attention of the industry and academia towards the potential cybersecurity issues on smart construction sites and introduce the authors' approach to address these problems. However, a case study that implements the complete evaluation on a real site will be conducted in future work to present more concrete findings.

***Acknowledgment*:** The authors thank the Center for Cyber Security (CCS) at New York University Abu Dhabi for their support during this research.

References

[1] Ngowi A. B., Pienaar E., Talukhaba A., and Mbachu J. The globalisation of the construction industry - A review. *Building and Environment*, 40(1):135–141, 2005.

[2] Kärnä S. and Junnonen J. M. Project feedback as a tool for learning. In *13th International Group for Lean Construction Conference: Proceedings*, pages 47–55, Sydney, Australia, 2005.

[3] Klinc R. and Turk Ž. Construction 4.0 - digital transformation of one of the oldest industries. *Economic and Business Review*, 21(3):393–410, 2019.

[4] Harp D. R. and Gregory-Brown B. IT / OT Convergence Bridging the Divide. 2015. On-line: https://ics.sans.org/media/IT-OT-Convergence-NexDefense-Whitepaper.pdf.

[5] Bock T. and Linner T. *Construction Robots: Elementary Technologies and Single-Task Construction Robots*, volume 3. Cambridge University Press, Cambridge, UK, 2016.

[6] Andersson J. *et al.* A Security Analysis of Radio Remote Controllers for Industrial Applications. 2019. On-line: https://documents.trendmicro.com/assets/white_papers/wp-a-security-analysis-of-radio-remote-controllers.pdf.

[7] FireEye. M-Trends 2021. 2021. On-line: https://content.fireeye.com/m-trends/rpt-m-trends-2021.

[8] Gu R., Marinescu R., Seceleanu C., and Lundqvist K. Formal Verification of an Autonomous Wheel Loader by Model Checking. In *FormaliSE '18: 6th Conference on Formal Methods in Software Engineering*, pages 74–83, Gothenburg, Sweden, 2018.

[9] Mohamed Shibly M. U. R. and García de Soto B. Threat Modeling in Construction: An Example of a 3D Concrete Printing System. In *ISARC 2020 - 37th International Symposium on Automation and Robotics in Construction*, pages 625–632, Kitakyushu, Japan, 2020.

[10] Mantha B. R. K. and García de Soto B. Assessment of the Cybersecurity Vulnerability of Construction Networks. *Engineering, Construction and Architectural Management*, 2020.

[11] Mantha B. R. K., Jung Y., and García de Soto B. Implementation of the Common Vulnerability Scoring System to Assess the Cyber Vulnerability in Construction Projects. In *Creative Construction e-Conference 2020*, pages 117–124, Budapest, Hungary, 2020.

[12] Sonkor M. S. and García de Soto B. Operational Technology on Construction Sites: A Review from the Cybersecurity Perspective. *Journal of Construction Engineering and Management*, 2021.

[13] García de Soto B., Georgescu A., Mantha B. R. K., Turk Ž., and Maciel A. Construction Cybersecurity and Critical Infrastructure Protection: Significance, Overlaps, and Proposed Action Plan. *Preprints 2020*, 2020.

[14] UK Government. Minimum Cyber Security Standard. 2018. On-line: https://www.gov.uk/government/publications/the-minimum-cyber-security-standard.

[15] ISO/IEC. ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. Geneva, Switzerland, 2013. On-line: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en.

[16] ISO. ISO 19650-5:2020 Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) — Information management using building information modelling — Part 5. 2020. On-line: https://www.iso.org/standard/74206.html.

[17] NCSC. Cyber Assessment Framework v3.0. 2019. On-line: https://www.ncsc.gov.uk/files/NCSC_CAF_v3.0 .pdf.

[18] European Union. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. 2016. On-line: http://data.europa.eu/eli/dir/2016/1148/oj.

[19] Boyes H. Code of Practice for Cyber Security in the Built Environment. 2014.

[20] NIST. Framework for Improving Critical Infrastructure Cybersecurity v1.1. Gaithersburg, MD, 2018.

[21] Dadhich S., Sandin F., Bodin U., Andersson U., and Martinsson T. Field test of neural-network based automatic bucket-filling algorithm for wheel-loaders. *Automation in Construction*, 97:1–12, 2019.

[22] Zhang L. *et al.* An autonomous excavator system for material loading tasks. *Science Robotics*, 6(55):3164, 2021.

[23] Czarnowski J., Dąbrowski A., Maciaś M., Główka J., and Wrona J. Technology gaps in Human-Machine Interfaces for autonomous construction robots. *Automation in Construction*, 94:179–190, 2018.

[24] BehrTech. 6 Leading Types of IoT Wireless Technologies and Their Best Use Cases. On-line: https://behrtech.com/blog/6-leading-types-of-iot-wireless-tech-and-their-best-use-cases/, Accessed: 08/06/2021.

[25] Naghshbandi S. N., Varga L., and Hu Y. Technologies for safe and resilient earthmoving operations: A systematic literature review. *Automation in Construction*, 125:103632, 2021.