Vulnerability Assessment of Construction Equipment: An Example for an Autonomous Site Monitoring System

M. S. Sonkor [a], X. Xu [a], S. A. Prieto [a], 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, xx927@nyu.edu, samuel.prieto@nyu.edu, garcia.de.soto@nyu.edu

Abstract –

The digital transformation of the construction industry is accelerating with the advances in information technology (IT) and operational technology (OT) and their convergence. While the benefits of such transformation in construction are apparent, cybersecurity aspects are usually overlooked. Cyber-attacks against project information can cause the exposure of confidential project data, intellectual property, and personal information and interruption of project tasks. On the other hand, cybersecurity incidents affecting the OT utilized in the project can lead to misinformation, harm people nearby, or even cause loss of life.

Given the criticality of providing robust cybersecurity in construction projects, this study aims to (1) point out the cybersecurity considerations to be taken into account before utilizing autonomous equipment on-site, (2) raise awareness about cybersecurity in construction, and (3) present an example of using vulnerability assessment systems in construction projects. This paper utilizes the Common Vulnerability Scoring System (CVSS) to assess the vulnerabilities and risks of different levels of an autonomous site monitoring system. Four assessors with different backgrounds in cybersecurity and robotic systems performed the assessment. The results revealed the most vulnerable levels of the assessed robotic system, which can be considered as a warning. The assessment suggested in this study can help construction decision-makers identify the levels they need to pay extra attention to before employing a cyber-physical system (CPS) on-site. Utilizing CVSS to conduct a vulnerability assessment for CPSs during the construction phase has not been proposed by any previous study, making this paper novel.

Keywords – Construction 4.0; Cybersecurity; Cyber-Physical Systems; Vulnerability Assessment; Construction Robots

1 Introduction

Automation emerges in various forms (e.g., process automation, information technology (IT) automation) and disrupts many industries, including construction. Automation is defined as the use of technology to minimize human input [1]. It is a considerable part of the digital transformation in the construction industry, also referred to as Construction 4.0 [2]. The automation in construction affects both IT and operational technology (OT)-related processes. As an example of the IT-related ones, generative design using visual programming tools (e.g., Dynamo) automates design optimization and helps reach the desired design outcomes much faster than conventional methods. OT-related automation utilizes cyber-physical systems (CPSs) such as robotic systems and can be seen in construction and operation and maintenance (O&M) phases. For example, repetitive construction tasks such as excavation and digging can be automated using autonomous construction equipment. Some construction machinery manufacturers such as Caterpillar and Komatsu and start-ups such as Built Robotics have been developing such equipment. Another example is autonomous data acquisition systems for progress monitoring on construction sites proposed by several studies such as [3] and [4]. The common purpose of all given automation examples is to improve efficiency, accuracy, quality of work, and the safety and well-being of workers by minimizing human involvement.

While the benefits of automation in construction are apparent and well presented in previous studies, the concerns related to cybersecurity did not receive the same degree of attention from the industry and academia [5]. Potential cyberattacks against digital platforms and tools or CPSs utilized in construction projects can lead to the disclosure of sensitive information and cause physical damage to the surrounding environment, including humans and equipment [6]. The volume of sensitive information grows depending on the criticality of the building involved in a project. For example, in 2013, hackers gained access to the blueprints of the Australian Intelligence Service headquarters when it was still under construction [7]. It shows that design documents can also

become a target for hackers when the constructed building has a critical function. A famous example of the cyberattacks against CPSs is the Stuxnet attack that targeted the Natanz nuclear plant in Iran in 2010 and damaged nearly one-fifth of the centrifuges [8]. It can be considered a cyberattack that occurred during the O&M phase.

Given the high impact of potential cyberattacks during different phases of construction projects, maintaining a robust cybersecurity level through the entire life-cycle of the project is crucial. Therefore, this study focuses on construction cybersecurity and proposes using an existing vulnerability assessment system (VAS) to evaluate the vulnerabilities of autonomous robotic systems used in construction projects. This evaluation targets identifying the most vulnerable levels of such systems so that greater attention can be paid to keeping them secure. Several VASs were analyzed to choose the most suitable one for this study. In order to demonstrate the implementation of the selected VAS, an autonomous site monitoring system (ASMS) was used. Different levels of the system were scored according to their vulnerabilities.

2 Research Methodology

The research methodology followed in this paper is divided into three main sections, described as follows.

- **Providing background information on cybersecurity:** Sections 3 and 4 provide background information by presenting prominent studies on cybersecurity efforts in the construction industry and OT cybersecurity, since the scope of the paper and the assessment conducted as a part of the study are primarily related to these two topics.
- **Overview of the different VASs:** An overview of the prominent VASs is provided in Section 5, starting from the first examples and including the most recent and widely used ones. This overview aims to give an understanding of the commonly used VASs and show their main characteristics. This overview helps decide the VAS to be utilized in the following section.
- **Vulnerability Assessment of an ASMS:** The assessment shown in this study includes an ASMS that has a prototype at the S.M.A.R.T. Construction Research Group's lab at NYUAD. A high-level overview of the system is provided in Section 6.1. For the assessment, CVSS was chosen. Its main characteristics are presented in Section 6.2 before demonstrating the proposed implementation. Finally, in Section 6.3, the proposed assessment is demonstrated. The assessment was conducted by four assessors with different backgrounds. The authors of this paper performed the assessor roles in this study for the sake of simplicity and demonstration purposes.

3 Cybersecurity Efforts in the Construction Industry

Even though cybersecurity does not stand as one of the popular topics in construction research, some studies have been conducted to point out the necessity of strong cybersecurity levels in projects considering different phases. One of the examples is the study by Zheng et al. [9]. Their study targeted to prevent BIM data leakage by proposing a context-aware access control for BIM systems instead of the conventional role-based ones. They provided examples of two different possible contexts that can be used for access control: location and time. Mantha et al. [10] developed a construction-specific cybersecurity threat model for different phases of projects. They demonstrated the use of the proposed model at the commissioning phase. Possible intrusions into the data collection process by malicious actors and a countermeasure to prevent such actions were presented in their study. Alshammari et al. [11] investigated the cybersecurity aspects of digital twins, which are envisaged to be commonly used to monitor and simulate built environments in the near future. Grundy [12] discussed cybersecurity during the O&M phase by underlining the increasing utilization of interconnected sensors/devices in smart buildings. He suggested using generic cybersecurity frameworks published by internationally recognized institutions (e.g., ISO, National Institute of Standards and Technology (NIST)) to address the raised concerns that stem from such interconnectivity. Finally, Sonkor and García de Soto [5] focused on the automated and remote-controlled equipment starting to be a bigger part of construction processes. They reviewed the literature and accentuated the lack of studies on the cybersecurity aspects of such equipment utilized on construction sites.

Some scholars suggested blockchain-based solutions to different cybersecurity problems in construction. For example, Turk and Klinc [13] did one of the first studies that analyzed the potentials of blockchain in the construction industry. They considered blockchain to provide a trustworthy environment for managing information exchange during different phases of projects. Pärn and Edwards [13] scrutinized the cyber threats affecting the built environment, mainly focusing on critical infrastructures (CIs). They proposed using blockchain technology to improve the confidentiality of sensitive information in BIM common data environments (CDEs). Lee et al. [14] stressed the diversity of stakeholders involved in construction projects and proposed an integrated framework consisting of blockchain and digital twin technologies for enhanced data traceability. Last but not least, Sonkor and García de Soto [15] proposed a data-sharing architecture that utilizes a decentralized storage approach and blockchain technology to improve cybersecurity in construction

networks. They suggested using blockchain to store the fingerprints of BIM files for validation purposes while storing the actual files in a decentralized manner over the construction network.

Besides the academic studies, several reports published by private institutions indicated the increasing cyber threat surface in the construction sector. One of them is AECOM's report [16] showing the results of a survey that involved 509 civil infrastructure professionals from Europe, North America, and Asia-Pacific. Their survey aimed to understand the cybersecurity awareness and preparedness of the civil infrastructure sector. The report concluded that "To support economic growth and social prosperity, future-proofing and protection against cyber and physical attack are essential". Moreover, a recent study by NordLocker [17] showed that the construction industry had been the primary target of ransomware attacks in 2021. This concerning finding should be considered a wake-up call for the industry to start taking immediate actions.

4 Cybersecurity of Operational Technology

OT in construction is new and still not at a mature level—especially during the pre-occupational phases—unlike in some other sectors that use industrial control systems (ICSs) and are ahead of construction in terms of digitalization. These sectors include but are not limited to water treatment, energy, oil & gas, electric power distribution, and manufacturing. Since most of these sectors are considered a part of CI, they have been the primary target of hackers [18] (e.g., patriot hackers, organized cybercriminals). The importance of availability in such environments further increases the outcomes of potential attacks [19].

Large-scale OT attacks in history have repeatedly proven the criticality of robust cybersecurity. An example is a recent attack against the largest pipeline in the US, Colonial Pipeline, that caused the operations to stop for two weeks and led to severe outcomes such as fuel price increases and fuel shortages [20]. The operations could go back to normal only when the hackers received a $4.4 million ransom. Increasing attention of hackers to these sectors caused CI owners and operators to take additional cybersecurity measures and researchers to direct their efforts toward proposing preventive methods against possible attacks.

Some examples from the extensive literature on this topic are [21]–[23], that proposed cyberattack and intrusion detection systems for ICSs. These detection systems aim to gain the cybersecurity teams of the attacked entities valuable time before any unrecoverable damages occur. In 2015, two cybersecurity researchers published a white paper showing that they could remotely control a passenger vehicle [24]. They gained access to the car's entertainment system by exploiting the software vulnerabilities. After they gained access, they could remotely control different functionalities of the car, such as the dashboard, brake, steering, and air conditioner. Another research to prove the vulnerabilities of commonly used OT was conducted by Trend Micro Research [25]. They tested radio frequency (RF) remote controllers from 17 vendors installed on cranes in industrial environments. Their results showed that millions of cranes using these remote controllers are vulnerable to cyberattacks.

5 Vulnerability Assessment Systems

Cybersecurity researchers and white-hat hackers discover new vulnerabilities every day, and these vulnerabilities have different levels of impact when they are exploited. Since it is almost impossible for organizations to address every discovered vulnerability, it is crucial to know which ones to prioritize. Therefore, government and private institutions have developed various VASs to identify the severities of vulnerabilities over the years. The Escal Institute of Advanced Technologies (SANS) published one of the early vulnerability assessment documents in 2001 [26]. It provided insights into the necessity of vulnerability assessments and gave an overview of the recommended process for conducting one. In 2016, Bugcrowd (a crowdsourced security platform) released the Vulnerability Rating Taxonomy [27], which is simpler and less comprehensive than the widely used Common Vulnerability Scoring System (CVSS). It was developed to be used by the bug bounty community. Therefore, it mainly focuses on the vulnerabilities frequently seen by bug hunters. Microsoft Security Response Center (MSRC) developed the Microsoft Exploitability Index (MEI), which mainly aims to help Microsoft customers assess the exploitability potential of vulnerabilities [28]. MEI has four levels of exploitability: 0 – Exploitation Detected, 1 – Exploitation More Likely, 2 – Exploitation Less Likely, and 3 – Exploitation Unlikely. MSRC developed MEI as a separate vulnerability scoring system that is independent from the CVSS. However, MSRC also contributes to the improvement efforts of CVSS [28].

The mentioned VASs have particular use-cases and scopes. On the other hand, CVSS released by the Forum of Incident Response and Security Teams (FIRST) has been commonly used by internationally recognized cybersecurity organizations, such as NIST, for a wide range of software vulnerabilities. CVSS is an open framework developed to assess the severities of discovered vulnerabilities [29]. It has been used by the National Vulnerability Database (NVD), one of the most extensive vulnerability databases available on the

internet. There are three groups of metrics provided by CVSS: base metric group, temporal metric group, and environmental metric group [29]. Base metrics show the characteristics of a vulnerability that do not change in different environments and over time. Temporal metrics show the vulnerability characteristics that do not change in different environments but might change over time. Finally, environmental metrics reflect the characteristics of vulnerabilities that are specific to the end user's environment. While scoring the base metrics is mandatory, temporal and environmental metrics are optional but recommended for higher precision.

Besides the original purpose of CVSS, which is to describe the severity and characteristics of vulnerabilities, Mantha and García de Soto [30] used it to assess the cybersecurity vulnerabilities of different participants in construction projects, such as the public owner, local contractor, and construction worker. Their study provided an alternative use of CVSS, showed its usefulness in the construction industry, and inspired the implementation demonstrated in the following section.

6 Vulnerability Assessment of an Autonomous Site Monitoring System

Several OT uses on construction sites have attracted attention from construction equipment manufacturers and academics. One of them is utilizing ASMSs on-site to track construction progress with minimized human intervention. This section demonstrates the implementation of CVSS (version 3.1) to perform vulnerability assessments for different levels of an ASMS. CVSS was chosen due to its well-established assessment structure and suitability to be used for various cases besides software vulnerabilities, as proven in [30]. The following subsections provide an overview of the assessed ASMS and the assessment details.

6.1 Overview of the Assessed Autonomous Site Monitoring System

The different components and levels of the assessed ASMS are depicted in Figure 1. The structure of the communications and integrations within the robotic platform is divided into five different levels based on their level of abstraction.

In Level 0 of the structure, the physical components of the robot responsible for acquiring data and interacting with the environment (i.e., sensors and actuators) can be found. They can be grouped into three major subgroups: the 3D scanner, all the sensors embedded on the robot (i.e., LiDARs, RGBD camera, encoders, and IMU), and the platform itself—housing all the different hardware such as sensors, computers, and locomotion means.

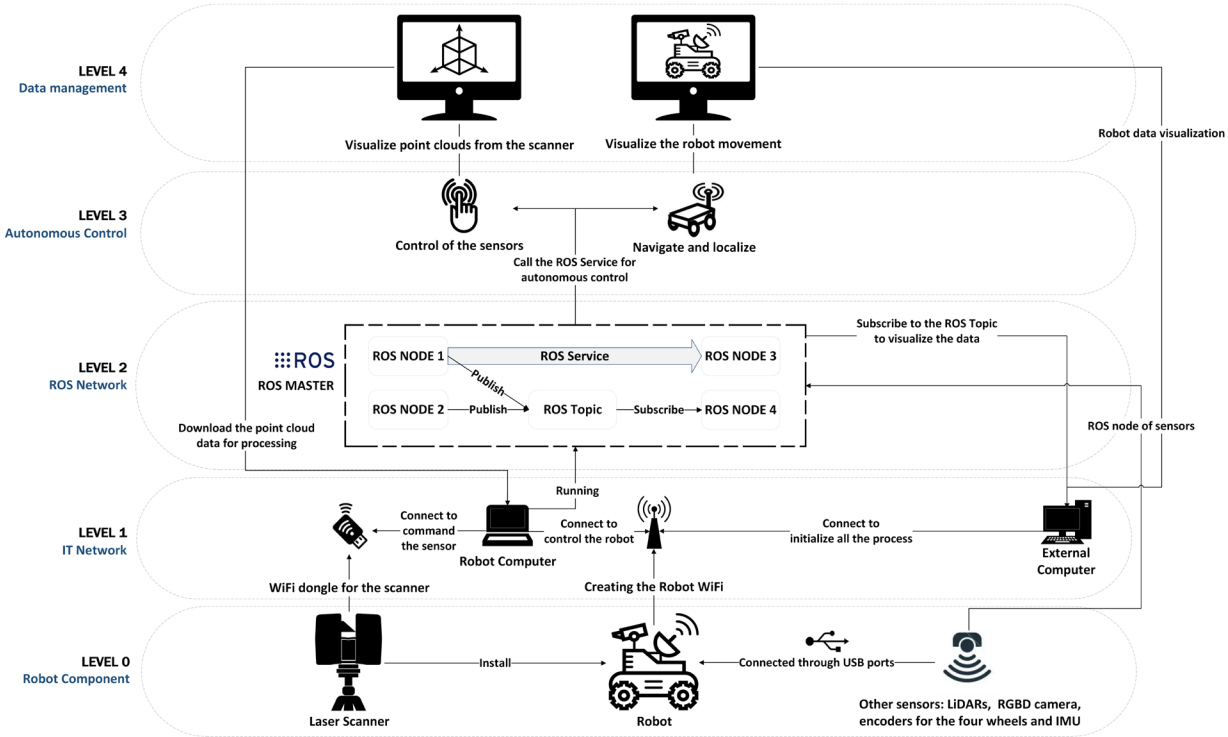

Figure 1. Diagram showing the different levels and components of the ASMS

Level 1 involves the basic connections between the elements mentioned above and the computer embedded in the robot responsible for controlling everything. Most sensors are connected to the Robot Computer by a USB protocol. The platform is equipped with a Wi-Fi router to create a Master Network, where the Robot Computer is connected via Ethernet. The laser scanner is only reachable through Wi-Fi communication and is connected to the Robot Computer through a Wi-Fi dongle. To provide a Human-Machine Interaction (HMI) interface, a second External Computer can be connected to the Master Network.

Level 2 consists of the Robot Operating System (ROS) [31] Network. The ROS Network can involve as many devices and computers as needed, as long as there is a device running the Master. In this case, the Robot Computer acts as a Master, and the External Computer connects to the ROS Network to interact with it. This interaction is bi-directional, allowing the robotic platform to attend to any command given by the External Computer, and the External Computer to visualize any data coming from the robotic platform. Within the ROS Network, multiple nodes are running, each managing all the different functionalities of the robot (e.g., the autonomous navigation, the localization, all the different sensors, control of the motors). The ROS nodes publish/receive information in the way of ROS Topics and can receive/give commands in ROS Services.

Level 3 demonstrates the basic tasks fulfilled by the robotic system, which involves the autonomous control of the robot. By using the ROS Services and publishing into the ROS Topics, the platform can communicate with all the different sensors and actuators autonomously.

Level 4 is the Human-Machine Interaction (HMI) layer. ROS provides multiple graphical user interfaces (GUIs) to interact and visualize the information of the robot, the most important one being the visualization software for the robot sensors, running in the External Computer to achieve autonomous mapping and localization using SLAM algorithms. This level overrides any command issued by Level 3.

6.2 Overview of the Scoring System

As mentioned earlier, CVSS has three groups of metrics (i.e., base, temporal, environmental), and the base metric group is mandatory to be scored. Therefore, to keep the scoring demonstrated in this study brief, only the base score will be calculated for different levels of the ASMS shown in Figure 1. Different metric categories within the base group, different metrics under each category, and possible metric values for each metric are shown in Table 1. Each possible metric value has a different numerical equivalent to be used in the formulas of the base score. Explanations of each metric, the corresponding numerical values, and the formulas to calculate the base score are presented in detail in the CVSS version 3.1 Specification Document [29].

Table 1. Different metrics and possible metric values to calculate the CVSS base score

Metric Category	Metric Name	Possible Metric Values
Exploitability	Attack Vector	[Network, Adjacent, Local, Physical]
	Attack Complexity	[Low, High]
	Privileges Required	[None, Low, High]
	User Interaction	[None, Required]
Scope	Scope	[Unchanged, Changed]
Impact	Confidentiality	[High, Low, None]
	Integrity	[High, Low, None]
	Availability	[High, Low, None]

The exploitability category covers the characteristics of the component considered in the scoring process and the properties of a successful attack that can exploit this component. For example, the attack vector metric refers to the distance of a successful attacker that exploits the vulnerable component. As the possibility of remote exploitation increases, the number of possible attackers increases, thus the base score in this assessment. Since different levels of the robotic system are scored in this paper rather than software vulnerabilities, the possibility of exploiting the corresponding level was considered while making the assessment presented in the following subsection. For example, if the assessor thinks that the components in Level 0 (shown in Figure 1) can be exploited only with physical interaction, he/she should select the “Physical” option for the attack vector.

The scope metric reflects whether a successful breach of a component can affect another component that is not in the same security authority. The security authority in this definition refers to a mechanism (e.g., an operating system) that controls access to specific components of a system. Therefore, if the same mechanism controls access to two different components, these two components are considered under the same security authority. Considering the ASMS in Figure 1, if the assessor thinks that a successful attack against Level 0 can also affect another level, the “Changed” option should be selected.

The impact category indicates the potential outcomes of a successful attack against the vulnerable components. The most likely outcomes of the potential attacks should be considered while scoring these metrics. For example,

if the breach of Level 4 is likely to cause a complete confidentiality loss, the "High" option should be selected for the confidentiality metric.

6.3 Demonstration of the Assessment and Discussion

For demonstration purposes, four assessors evaluated the different levels of the ASMS (in Figure 1) using CVSS. Descriptions of different levels of the ASMS and different metrics of CVSS were given to the assessors before they provided their input. The base scores for each level of the system were calculated using the inputs from each assessor and the formulas in [29]. As an example, Table 2 shows the input received from Assessor 1, numerical equivalents, and the calculated total base scores for each level.

Input from the four assessors was considered and combined to determine the vulnerability of the different levels of the system. In order to account for the assessors' knowledge of cybersecurity and the assessed system, different weights were applied (Table 3). Weighted averages for each level were calculated (as summarized in Table 4). The risk ratings (derived from CVSS [29]) reflect the exploitation risk for each level.

Table 2. CVSS assessment from Assessor 1 and numerical equivalents

Metric Category	Metric Name	Level 0	Level 1	Level 2	Level 3	Level 4
Exploitability	Attack Vector	Physical / 0.20	Adjacent / 0.62	Local / 0.55	Adjacent / 0.62	Adjacent / 0.62
	Attack Complexity	Low / 0.77	High / 0.44	High / 0.44	Low / 0.77	Low / 0.77
	Privileges Required	Low / 0.68	Low / 0.68	Low / 0.68	Low / 0.68	Low / 0.68
	User Interaction	Required / 0.62	None / 0.85	None / 0.85	None / 0.85	Required / 0.62
Scope	Scope	Changed	Changed	Changed	Changed	Changed
Impact	Confidentiality	None / 0	None / 0	High / 0.56	None / 0	High / 0.56
	Integrity	Low / 0.22	Low / 0.22	High / 0.56	Low / 0.22	High / 0.56
	Availability	Low / 0.22	Low / 0.22	High / 0.56	Low / 0.22	High / 0.56
Total Base Score		3.6	4.4	7.8	5.4	8.4

Table 3. Different weights for the assessors according to the level of knowledge

Knowledgeable in cybersecurity?	Knowledgeable about the assessed robotic system?	Weight
Yes	Yes	100%
Yes	No	80%
No	Yes	60%

The weighted base score averages (Table 4) indicate a relatively higher exploitation risk and vulnerability against cyberattacks for Level 2 (CVSS score: 8.6, Risk rating: High). On the other hand, Level 0 (CVSS score: 3.7, Risk rating: Low) can be considered as the lowest risk level of the assessed ASMS. In the context of this study, a higher risk implies a larger threat surface, a greater number of potential attackers, a higher probability of a successful attack, and a higher impact when a vulnerable component is exploited. The higher risk rating of Level 2 can be due to two main reasons. The first one is the high impact of a potential breach of Level 2, which involves the ROS Network. Since ROS can be used to give commands to the robot and request data, potential exploitations of the ROS Network can have severe impacts on the confidentiality, integrity, and availability of the data that can be accessed through the ROS nodes. A successful attack can affect the robot's movement—which can cause harm to the surrounding environment and people—, alter the data received from the robot—which can negatively impact the decisions made using this data—, make the robot or data unavailable—which can disrupt the related tasks—, and expose some information that the attackers can use to plan their future attacks against the construction site. The second main reason for the high-risk rating is that the ROS Nodes and Services can be accessed without a need for credentials in the assessed ASMS. Even though the computers used for accessing the ROS Network require credentials, they are in Level 1 and thus not considered while scoring Level 2. Therefore, the privileges required and the attack

complexity to exploit Level 2 are low, making the risk high. Additional security features are employed in ROS 2, such as encrypting the communication traffic and authentication [32]. However, the robotic system in this study uses ROS 1, which does not have the mentioned features. The main reasons for the low-risk rating of Level 0 include the physical interaction required to launch an attack against this level's components. Not being able to perform an attack remotely significantly reduces the number of potential attackers for this level. Moreover, potential exploitations of the components in this level do not have a high impact since the data exchange and all the communication between the robot, operating system, sensors, and utilized software happens at the other levels.

Table 4. Weighted averages of the CVSS scores from all assessors for each level

	Level 0	**Level 1**	**Level 2**	**Level 3**	**Level 4**
Total base score (weighted average)	3.7	6.6	8.6	7.5	6.5
Risk rating	Low	Medium	High	High	Medium

7 Conclusions, Limitations, and Future Work

Automation and digitalization are increasingly affecting the construction processes in different project phases. The complexity of maintaining robust cybersecurity is elevated due to the fragmented nature of construction projects, unstructured and unstable environments, and the variety of the utilized equipment in terms of purpose and security levels. CPSs, such as autonomous earthmovers and site monitoring equipment, are particularly open to cyberattacks since they are relatively new in the construction industry. Therefore, construction decision-makers should employ specific methods to assess the risk and vulnerability levels of the CPSs that they are planning to use in their projects. This study addresses this need by proposing CVSS to assess the vulnerabilities of different levels in an ASMS. Four assessors conducted the assessment, and the weighted averages according to their knowledge levels of cybersecurity and the assessed system were calculated for each level. The results provided the levels with the highest cybersecurity risks, which can be considered as a warning to pay additional attention, particularly to these levels.

One of the limitations of the study is the number of assessors. The involvement of more assessors knowledgeable about cybersecurity and robotic systems can improve the accuracy and reliability of the results. Moreover, the components in the system were not scored individually, which can be considered another limitation. Instead, the scoring was performed level by level (i.e., for each level consisting of different components). Different characteristics of the components in some levels made it more challenging to make a representative assessment. For example, in Level 1, the attack complexity required to exploit the Wi-Fi dongle and the External Computer are inherently different due to their varying software and hardware characteristics. In Level 4, two different visualization software developed by different software companies were considered together, which also caused an inaccurate assessment due to these companies' different cyber defense mechanisms. The authors are extending this study to address these limitations. The future assessment will include a larger pool of assessors and more detailed information about each component of the ASMS. It will be conducted by examining each component instead of each level. Suggestions to mitigate the potential cybersecurity risks related to the most vulnerable components will be provided. Moreover, the usefulness of the proposed assessment will be tested on other construction robotic applications.

Acknowledgment

The authors thank the Center for Cyber Security at New York University Abu Dhabi (CCS-AD) for their support.

References

[1] IBM. What is automation? *IBM*. Online: https://www.ibm.com/topics/automation, Accessed: 24/01/2022.

[2] 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.

[3] Moselhi O., Bardareh H., and Zhu Z. Automated Data Acquisition in Construction with Remote Sensing Technologies, *Applied Sciences* , 10(8). 2020.

[4] Prieto S., García de Soto B., and Adan A. A Methodology to Monitor Construction Progress Using Autonomous Robots. Oct. 2020.

[5] 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*,

147(12):4021172, 2021.

[6] 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.

[7] Watson S. Cyber-security: What will it take for construction to act? *Construction News*. Online: https://www.constructionnews.co.uk/tech/cyber-security-what-will-it-take-for-construction-to-act-22-01-2018/,

[8] Hemsley K. E. and Fisher R. E. History of Industrial Control System Cyber Incidents. 2018. Online: https://www.osti.gov/servlets/purl/1505628,

[9] Zheng R., Jiang J., Hao X., Ren W., Xiong F., and Zhu T. CaACBIM: A context-aware access control model for BIM. *Information*, 10(2):47, 2019.

[10] Mantha B. R. K., García de Soto B., and Karri R. Cyber security threat modeling in the AEC industry: An example for the commissioning of the built environment. *Sustainable Cities and Society*, 66:102682, 2021.

[11] Alshammari K., Beach T., and Rezgui Y. Cybersecurity for digital twins in the built environment: Current research and future directions. *Journal of Information Technology in Construction*, 26(March):159–173, 2021.

[12] Grundy C. Cybersecurity in the built environment: Can your building be hacked? *Corporate Real Estate Journal*, 7(1):39–50, 2017.

[13] Pärn E. and Edwards D. Cyber threats confronting the digital built environment: Common data environment vulnerabilities and block chain deterrence. *Engineering Construction & Architectural Management*, 26(2):245–266, 2019.

[14] Lee D., Lee S. H., Masoud N., Krishnan M. S., and Li V. C. Integrated digital twin and blockchain framework to support accountable information sharing in construction projects. *Automation in Construction*, 127, 2021.

[15] Sonkor M. S. and García de Soto B. Towards Secure Construction Networks: A Data-Sharing Architecture Utilizing Blockchain Technology and Decentralized Storage. 2021.

[16] AECOM. The Future of Infrastructure. 2018. Online: https://tinyurl.com/mrx3rj2c, Accessed: 20/06/2022.

[17] Nordlocker. Top industries hit by ransomware. *Nordlocker*. Online: https://nordlocker.com/recent-ransomware-attacks/, Accessed: 20/01/2022.

[18] McLaughlin S. *et al.* The Cybersecurity Landscape in Industrial Control Systems. *Proceedings of the IEEE*, 104(5):1039–1057, 2016.

[19] Drias Z., Serhrouchni A., and Vogel O. Analysis of cyber security for industrial control systems. In *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*, pages 1–8, 2015.

[20] Turton W. and Mehrotra K. Hackers Breached Colonial Pipeline Using Compromised Password. *Bloomberg*. Online: https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password, Accessed: 10/08/2021.

[21] Zhang F., Kodituwakku H. A. D. E., Hines J. W., and Coble J. Multilayer Data-Driven Cyber-Attack Detection System for Industrial Control Systems Based on Network, System, and Process Data. *IEEE Transactions on Industrial Informatics*, 15(7):4362–4369, 2019.

[22] Adepu S. and Mathur A. Distributed Attack Detection in a Water Treatment Plant: Method and Case Study. *IEEE Transactions on Dependable and Secure Computing*, 18(1):86–99, 2018.

[23] Sugumar G. and Mathur A. Testing the Effectiveness of Attack Detection Mechanisms in Industrial Control Systems. In *2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, pages 138–145, 2017.

[24] Valasek C. and Miller C. Remote Exploitation of an Unaltered Passenger Vehicle. 2015. Online: https://ioactive.com/pdfs/IOActive_Remote_Car_Hacking.pdf,

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

[26] Cima S. SANS Institute - Vulnerability Assessment. 2001. Online: https://www.sans.org/white-papers/421/,

[27] Bugcrowd. Bugcrowd's Vulnerability Rating Taxonomy. Online: https://bugcrowd.com/vulnerability-rating-taxonomy, Accessed: 04/02/2022.

[28] Microsoft. Microsoft Exploitability Index. *Microsoft*. Online: https://www.microsoft.com/en-us/msrc/exploitability-index, Accessed: 06/02/2022.

[29] FIRST. Common Vulnerability Scoring System version 3.1. 2019. Online: https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf,

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

[31] Quigley M. *et al.* ROS: an open-source Robot Operating System. In *ICRA workshop on open source software*, 3(3.2), 2009.

[32] The Construct. How to Enable and Use Security in ROS 2 | Sid Faber | ROSDevDay 2021. *Youtube*. Online: https://youtu.be/UJa4XWRA6EY, Accessed: 20/06/2022.