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.