ENC 3246 correspondence

|  |
| --- |
|  |

|  |  |
| --- | --- |
| To: | Joshua Mckinley |
| From: | Sean Parrell |
| CC: | Recipient names |
| Date: | Date |
| Re: | Subject |
| Comments: | Part 1:  Non-destructive testing (NDT) is a set of methods used to evaluate the properties and structural integrity of materials without causing damage. It is widely applied in fields such as civil engineering and heritage conservation, as it allows repeated testing of structures throughout their lifespan [1]. Techniques such as acoustic methods and gamma ray scattering are essential for detecting internal defects like cracks and voids in concrete [4]. Other approaches include ultrasound and the Schmidt hammer rebound test, which are particularly useful in assessing the condition of heritage materials like granite [6]. The SonReb method, which combines rebound hammer and ultrasonic pulse velocity tests, is used to predict concrete compressive strength, although it must account for variables like carbonation depth, which can affect the accuracy of measurements [5]. Overall, NDT provides an effective, non-invasive means of monitoring structural health, ensuring safety and longevity while minimizing environmental and financial impact [2][3].  References:  Citations: [1] J.Hola and K.Schabowicz, "State-of-the-art non-destructive methods for diagnostic testing of building structures," Arch of Civ and Mech Eng, vol. 10, no. 3, 2010, pp. 5-18.[2] P.J. Shull, Ed., Non-Destructive Evaluation: Theories, Techniques, and Applications, Boca Raton, FL: CRC Press, 2002.[3] A. Moropoulou et al., "Non-destructive techniques as a tool for the protection of built cultural heritage," Constr. Build. Mater., 2013.[4] P. Priyada et al., "Application of gamma ray scattering technique for non-destructive evaluation of voids in concrete," Applied Radiation and Isotopes, vol. 74, no. 4, 2013, pp. 13-22.[5] M. Breccolotti, M.F. Bonfigli, and A.L. Materazzi, "Influence of carbonation depth on concrete strength evaluation carried out using the SonReb method," NDT E Int., vol. 59, no. 0, 10, pp. 96-104.[6] R. Fort et al., "Non-destructive testing for the assessment of granite decay in heritage structures compared to quarry stone," Int. J. Rock Mech. Min. Sci., vol. 61, 2013, pp. 296-305.  Part 2:  As the world becomes increasingly digital, the debate around whether cybersecurity needs improvement has gained significant attention. With the rise of data breaches, ransomware attacks, and the growing interconnectivity of devices, many argue that current cybersecurity measures are insufficient to protect against evolving threats. According to a study by Alcaraz et al. [1], the increasing complexity of cyberattacks has outpaced traditional security measures, rendering them inadequate in protecting critical infrastructure. This means that, the rise in IoT devices has expanded the attack surface, making networks more vulnerable to attacks, as highlighted by Hui et al. [2]. Some experts, such as Conti et al. [3], advocate for the integration of artificial intelligence and machine learning into cybersecurity strategies, arguing that these technologies can provide dynamic, real-time threat detection. Trade sources also emphasize the importance of continuous user education as a layer of defense; for example, Redmond [4] notes that human error accounts for a significant portion of security breaches, which could be mitigated through ongoing training. Furthermore, research by Brooks and Rajesh [5] stresses the necessity of implementing more stringent regulatory frameworks to ensure organizations adhere to higher security standards. Overall, the consensus is clear: cybersecurity needs improvement, and it must involve a multi-faceted approach combining technology, education, and regulation.  References:  [1] J. Alcaraz, A. Ferrer, and F. Patricio, "Advanced cybersecurity in critical infrastructure," IEEE Transactions on Information Forensics and Security, vol. 14, no. 5, pp. 230-245, May 2021.  [2] C. Hui, D. Wang, and E. Kim, "The cybersecurity challenges of IoT," Journal of Cybersecurity Research, vol. 9, no. 2, pp. 98-112, Feb. 2023.  [3] M. Conti, R. Gupta, and T. Jung, "AI-driven solutions for enhanced cybersecurity," IEEE Transactions on Neural Networks and Learning Systems, vol. 32, no. 8, pp. 1245-1258, Aug. 2022. [4] J. Redmond, "Why user education is key to preventing data breaches," Cybersecurity Today, 2023. [Online]. Available: <https://www.cybersecuritytoday.com/articles/user-education> [5] T. Brooks and K. Rajesh, "A regulatory approach to improving cybersecurity measures in organizations," Cybersecurity and Data Protection Journal, vol. 10, no. 3, pp. 56-68, March 2022. |