Cybersecurity Risks to AI Adoption in Construction

Thursday, July 27, 2023

The adoption of predictive maintenance (PM), an artificial intelligence (AI) driven strategy that anticipates potential equipment failures using Internet of Things (IoT) sensors, holds immense promise for the construction industry. In a previous post, we analyzed the current and future opportunities for PM in construction, including avoiding expensive and dangerous equipment failure, increasing worker safety, and streamlining maintenance. However, the use of PM in construction also exposes companies to new risks, including heightened cybersecurity dangers and new legal questions. Below is an in-depth look at the risks posed by PM to the construction sector.

Cybersecurity Risks

The rise in PM adoption simultaneously escalates potential cybersecurity threats. The high volume of data transferred and stored, coupled with an increasing risk of data breaches and cyber attacks, brings about grave concerns. One potential genre of attack is data poisoning, in which an adversary manipulates the data used to train an AI system. By introducing misleading or incorrect data into the training set, an attacker could cause the AI system to make incorrect predictions or take inappropriate actions. If data used for training an AI system responsible for PM in the construction industry is poisoned, it could lead to critical equipment failing unexpectedly. This could cause dangerous situations, such as the collapse of structures or machinery failure that could harm workers on-site. In a similar vein as data poisoning, adversarial attacks involve introducing carefully crafted inputs designed to deceive an AI system. For example, an attacker might alter the data from a sensor used for PM in such a way that the AI system would interpret the machine as being in good working condition when it is actually about to fail.

Finally, there are infrastructure attacks that target AI systems that rely on complex infrastructure, including data storage systems, processing units, and networks for communication. Attacks on these systems, such as denial-of-service attacks or physical tampering with IoT devices, can disrupt the functioning of the AI system. Any attack on the physical infrastructure of AI systems, such as tampering with sensors, cameras, or other IoT devices, can lead to incorrect data interpretation and, therefore, incorrect actions. This could result in faulty construction or failure to identify crucial maintenance needs, leading to physical damage.

Internet of Things Vulnerabilities

IoT devices, which act as the primary data sources for AI-driven maintenance systems, present considerable cybersecurity vulnerabilities if not appropriately secured. Despite being invaluable for PM, these devices, ranging from simple machinery sensors to sophisticated wearables, have several weak points due to their inherent design and function. In case of a successful breach, cyber criminals could manipulate the IoT device's function, provide false data, or cause a system failure. They could also exploit these devices as springboards for broader network attacks, data exfiltration, or even to form a botnet for large-scale attacks.

Primarily, IoT devices' limited computing power and storage pose a substantial challenge. Their design caters primarily to their specific functions, leaving little room for advanced security features. Also, their physical accessibility makes them susceptible to direct attacks, such as malicious firmware installation, which could compromise the entire network. Securing them physically through protective measures and surveillance can mitigate such risks. Additionally, their direct connection to an organization's network can serve as an entry point for network-wide attacks. The continuous data

transmission of many IoT devices also makes them potential hubs for sensitive information interception.

Legal and Regulatory Compliance Regarding PM

The integration of PM in construction introduces complex legal and regulatory implications, notably concerning data privacy, liability, and specific industry regulations. PM heavily relies on data collection, storage, and analysis. This makes the process subject to various data privacy laws. Key among these are regulations such as the EU's General Data Protection Regulation (GDPR) and the California Privacy Rights Act (CPRA), both of which require that companies ensure that the data used for PM is anonymized when possible and stored and processed in specific ways. Non-compliance can lead to substantial penalties and damage to a company's reputation.

PM also raises complicated questions of liability. If a machine fails despite PM indicating otherwise, who bears the responsibility? Is it the construction company, the AI system developer, or the machine manufacturer? Comprehensive contracts should be drawn up to clarify the distribution of liabilities. Additionally, a distinction needs to be made about whether the AI system is a product or a service, as this determines the applicable liability laws. If the AI system is classified as a product, then product liability laws come into play. If it is deemed a service, different rules apply.

Beyond general liability and data privacy concerns, PM may also be subject to industry-specific regulations. For example, in construction, safety standards and best practices can influence how PM systems are deployed and used. These guidelines can shape the data collected, how it is analyzed, and the actions taken based on the PM insights. Compliance with these standards is crucial for legal and operational efficiency.