PUBLICATION

Automation and Artificial Intelligence in Construction: How to Capitalize on Technological Advancements While Mitigating Your Risk

Authors: Vivien F. Peaden
November 20, 2025

(1) The Good, the Bad, and the Ugly of Artificial Intelligence in Construction

The commercial construction industry is undergoing a seismic shift as artificial intelligence (AI) tools rapidly reshape how projects are planned, managed, and delivered. Advancements in AI and machine learning, including those in generative AI (GAI), robotics, augmented reality (AR), and virtual reality (VR), are streamlining every stage of the engineering and construction processes, from preconstruction to project completion. AI is presently being used to prepare cost estimates, develop bids and project proposals, compare as-built and as-planned conditions, monitor schedule progress, perform inspections, identify design conflicts, and track material prices, among other things. The automation of these processes not only boosts project efficiency but also improves the sector's post-COVID-19 productivity challenges.

According to Autodesk, a leading provider of construction management software, a recent survey shows that the "AI in construction" market is expected to grow from around $11.1 billion in 2025 to $24.3 billion by 2030. Despite the advantages that AI affords contractors, engineers, and similar professionals, it is imperative to understand and mitigate risk as the construction sector experiences a gradual but transformative movement towards digitalization and AI adoption.

(2) AI Is a Tool, Not a Replacement for Professional Judgment

AI should be used by contractors, engineers, and design professionals to augment their roles in the planning, design, and building phases – not to supplant their own professional judgment and expertise. The American Society of Civil Engineers' (ASCE) Code of Ethics instructs civil engineers to "consider the capabilities, limitations, and implications of current and emerging technologies when part of their work." ASCE Code of Ethics, Sec. 1(h). As the incipient legal landscape governing the use of AI in the construction industry develops over the coming years, the policy statements of professional associations and trade organizations serve as a present guidepost.

In July 2024, ASCE released a policy statement emphasizing an engineer's unwavering ethical duties and professional responsibility, notwithstanding the adoption of AI tools. ASCE cautions that "AI cannot serve as a replacement for the professional judgment of a licensed Professional Engineer" and that such technology is no substitute for an engineer's training and experience. See Policy Statement 573 – Artificial Intelligence and Engineering Responsibility | ASCE. The message to civil engineers and the greater construction industry is clear: engineers will be held accountable for the data upon which they base their decisions, recommendations, and representations, regardless of whether such data was computer-generated. Id. An engineer – not the AI application used by the engineer – will ultimately be responsible for violating any applicable standard of care. Id.

The National Society of Professional Engineers' (NSPE) February 2025 policy statement provides that engineers using AI are held to the same professional licensure standards as traditional engineers for purposes of public safety, health, and welfare. See NSPE Position Statement No. 03-1774. Similarly, the National Council of Architectural Registration Boards (NCARB) has stated that "[a]ny proposed regulation that addresses AI usage in practice must ensure the licensed practitioner remains in responsible control and continues to be accountable for all technical submissions under their seal." See October 17, 2024, NCARB Press Release. In other words, AI tools cannot stand in for an architect's or professional engineer's stamp on drawings.

(3) Privacy and Data Governance Concerns With AI

AI has significantly changed how the construction sector approaches project planning and field operations. Integrating AI into commercial construction workflows and processes means that companies are handling unprecedented volumes of data that boost forecasting, site safety, and productivity. For example, AI-enabled computer vision technologies provide real-time site monitoring that alerts site managers whenever workers are not wearing protective gear or when equipment is malfunctioning in violation of standard protocols. Further, GAI also delivers quicker outputs, enabling faster conceptual model development and accelerating design standardization. The speed and scale of AI adoption require organizations to adopt robust AI governance concerning what data they have, how new technologies are integrated, and who is accountable for outcomes.

(a) "Black Box" AI

All commercially available large language models (LLM), including OpenAI's ChatGPT, Google's Gemini, Anthropic's Claude, and xAI's Grok, share the common problem of the "black box" myth, meaning that users can see their inputs and the resultant outputs without clear insight into how the model arrived at its conclusions. This lack of transparency has led to hesitation by some companies to adopt LLMs more broadly in their business operation. According to recent research by Anthropic in March 2025, Claude and other LLMs are capable of "hallucinations," or false results, in generating their chain-of-thought in order to please a user. This finding makes it paramount for organizations to implement technical and operational safeguards to verify an AI model's outputs before relying on such information.

These transparency and interpretability requirements are further reflected in Article 13 of the EU AI Act, which mandates that providers of high-risk AI systems disclose their limitations (such as accuracy, robustness, and cybersecurity) and intended purpose, in addition to providing appropriate measures for implementing human oversight. Where AI is used for safety purposes as prescribed under certain EU regulations, these risk management requirements concerning high-risk AI use are set to take effect in August 2026 – e.g., 24 months after the EU AI Act officially went into effect.

(b) "Shadow AI"

Shadow AI is becoming a growing issue for organizations that are still experimenting with AI pilot programs. For decades, "shadow" adoption of emerging technologies has plagued enterprise security teams, from sales departments storing customer data in unauthorized Dropbox accounts to the creation of rogue Excel spreadsheets. Today, it has evolved into something far more powerful called "Shadow AI," which refers to the unsanctioned use of AI applications by an employee to perform work-related tasks without formal oversight by an employer's procurement, IT, or compliance review teams.

According to an MIT survey, while only 40 percent of companies have officially adopted LLM subscriptions, more than 90 percent of workers report regular use of personal AI tools for work. While employees' unauthorized use of public AI tools can drive productivity, such use can simultaneously expose an organization's proprietary information (including pricing information and sensitive personal data), waive privilege, and result in breaches of contractual obligations.

(c) Data Leaks in Using Open-Source AI

Shadow AI often begins subtly, introducing significant risks such as data leaks or exposure to malicious AI models. Some examples include the following:

- A project manager feeds a public chatbot with project information and past RFP responses to draft a proposal, exposing existing customers' site logistics, cost estimates, and pricing information.
- An executive assistant uses public ChatGPT to summarize a confidential strategic slide deck for board members' review. The open-source ChatGPT retains the prompts and outputs, including non-public information on product release dates and competitively sensitive information, to train its own model.
- A marketing coordinator uses a private Midjourney account to generate images with client identifiers that create IP and confidentiality risk.

Many non-enterprise AI tools are becoming generally accessible through web browsers and mobile app add-ons to existing platforms. As a result, most organizations lack visibility to conduct a meaningful audit or assessment of potential risks posed by widespread internal adoption of Shadow AI.

To mitigate the hidden threat of Shadow AI, organizations must stay vigilant by implementing AI-driven governance, monitoring, and protection mechanisms. One key step is to establish and enforce clear policies governing employees' and contractors' access to non-enterprise AI models and the permitted and prohibited uses of company information input into any third-party AI tools. Another effective step is to build or deploy corporate firewalls or gateways that automatically block sensitive data submission and scan activities according to company security policies. Organizations should closely monitor anomalous data flows and Application Programming Interface (API) connections to mitigate risks of model poisoning and manage high-risk usage.

Lastly, organizations should comply with applicable AI frameworks, such as the EU AI Act, the Colorado AI Act, the Texas Responsible Artificial Intelligence Governance Act, and California's regulations on automated decision-making technologies (ADMT).

(4) Courts and Legislatures Are Not Excusing Negligence in the Wake of AI Use

At this point, AI tools remain prone to producing hallucinations. This is evidenced by the recent flurry of court cases across the country in which attorneys were disciplined for their use of fabricated, AI-generated legal authority. Numerous courts have sanctioned attorneys for their blind reliance on AI-assisted tools in the performance of legal research, namely citing to non-existent cases in court filings. See *Mata v. Avianca, Inc.*, 678 F. Supp. 3d 443 (S.D.N.Y. 2023).

State-enacted consumer protection acts govern unfair and deceptive acts and trade practices, and these statutes contain provisions applicable to contractors. It should be noted that states are adopting legislation that does not exempt contractors from liability under consumer protection acts for AI-generated misrepresentations made to consumers. See, e.g., Utah's Artificial Intelligence Policy Act (effective May 2025). In other words, it is not a defense to a claim of violation of a consumer protection act that the representation was made by an AI tool, and contractors remain subject to penalties for such violations. It has been and remains the majority rule across jurisdictions that the use of technology does not supersede the duty of care.

(5) What Does This Mean for the Construction Industry?

AI is a tool to bolster and augment construction and engineering processes; however, it is not a substitute for professional judgment in the planning, designing, and building phases of construction projects. Always verify AI-generated outputs for accuracy before relying upon such information internally or disseminating it externally. As with any emerging technology, it is pivotal to understand and mitigate your exposure when using AI platforms, to regulate your employees' use of such applications, and to protect your company's proprietary information from inadvertent disclosure. The construction sector's adoption of AI goes beyond risk mitigation. Organizations should focus on responsible governance of their enterprise AI ecosystem through a cross-functional AI risk committee involving IT, cybersecurity, finance, marketing, and legal departments.

If you have any questions related to AI within the construction industry, please contact Viviene Peaden, Jordyne Richartz, or your Baker Donelson Construction attorney.