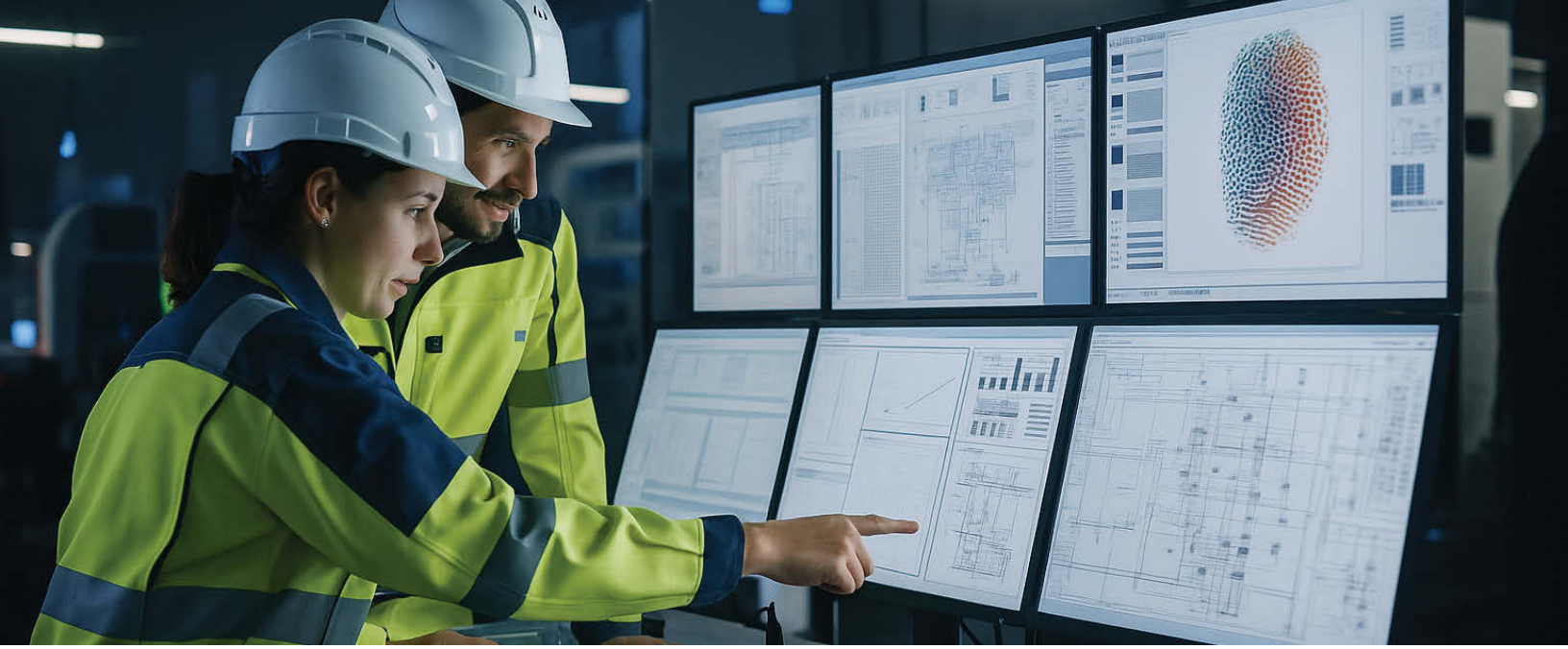
AI in Facilities Management: Balancing Innovation with Oversight

by Steve Sawyer

SolvingX



During the past four decades since the digital age began, the healthcare industry's information technology systems have been haunted by incongruity, insecurity, and a lack of interoperability. This is not only true on the clinical side but also with those of us in facilities who strive to keep everything running smoothly and cost-effectively. Abundant unstructured data streams constantly flow among multitudes of tributaries throughout the healthcare ecosystem, including through conduits that we can tap for successful facilities management.

For the most part, all that bounty of data we have available to us has not been efficiently combined into something we can meaningfully analyze without assigning substantial human effort to the task. That means much of the opportunity in that information just flows past us. As it all goes by, so do huge potential benefits for the health of our organizations and finally for the well-being of our internal and external customers.

Enter AI, which has quickly progressed from a distant vision to a present reality. In the patient care domain of healthcare, AI is being embraced for its promise in creating data-driven solutions to care. For our use in facilities management, AI is increasingly becoming the backbone for rapid, evolutionary development of computerized maintenance management systems (CMMS), combining other advancements, including the Internet of Things (IoT), edge computing, and digital twins (Lorenzi, 2025).

This innovation in facility management has accelerated with the adoption of AI-driven building management systems. Notable examples include:

- *Johnson Controls' OpenBlue Platform*. The company emphasizes its ability to combine information and operational technology, driving innovation by harnessing edge, cloud, and digital twin technology (Johnson Controls, 2025).

- *Honeywell Forge*. The company states that the platform provides comprehensive tools for building systems management and emphasizes the use of secure operational IT and OT to achieve desired business outcomes (Honeywell, 2025).

Both providers promote how their platforms use AI-generated insights to create powerful, comprehensive packages that improve efficiencies and enable autonomous building systems management.

The Promise of AI in Facilities Management

The magic place where AI can transform our work lies in its ability to sift data and redirect it back to us: taking those thousands of tributaries of unstructured data and routing them into a river of intensive analytics for our use. Core administrative and operational analytical functions tradi-

tionally involved people laboriously filtering through data and logs. By contrast, AI—especially generative AI (GenAI), with its ability to create new content—can automatically summarize and immediately act on the data regardless of how much flows in at once. (Baskher, et al., 2023).

AI-driven tools in health facilities-related applications can potentially boost profitability for healthcare facilities' operations by doing one thing humans can't do. They do this by leveraging raw data from disparate systems to streamline operations and enhance performance, leading to measurable, realized cost savings. AI can optimize workflows, accelerate predictive maintenance, automate tasks, and enable remote management of our buildings. This frees up time for humans to do what they do best.

And there's the rub...

When technology frees up more time for humans, our first impulse should be to find more productive things to do with that time they once spent sifting through logs and data. However, our first natural instinct is usually to see how much of a reduction in force we can create from gaining back those hours. The shift in AI combined with a decrease in full-time facility staff could diminish the organization's ability to perform critical tasks internally, potentially impacting service quality. This creates a loss of what I call self-performance, the ratio of tasks we are capable of performing in-house with competent staff to what we need to contract out to others.

Don't get me wrong: I'm not saying AI is bad, or that appropriately contracting out work to others is wrong. Quite the contrary. I didn't begin this article by touting all the great advances we can make by tapping into the opportunities of AI only to shoot my message down a few paragraphs later.

My point is that we need to strike a balance.

Balancing Technology with Human Oversight

On the IT/OT side of the integrated facilities management (IFM) seesaw, nothing happens efficiently and effectively-without a steady, reliable stream of intensive analytics that people can use when needed. With this, they can forecast needs, prove the value of what they do, and know where they stand. Analytical technology allows them to look in the mirror if they trust their data and their platform is intuitive. It enables leaders across departments/business units with a stake in IFM to provide transparency. It allows their team members to effectively monitor and manage the department's core considerations in real-time and collaborate with others.

Now to the human side of that seesaw. As a niche IFM

service provider, one of my primary goals is to promote enhanced staff competencies and long-term retention for the good of the integrated whole. This is true across all departments/business units in the organization with a stake in IFM, including Finance, Facilities, Supply Chain, Real Estate, Construction, and Information Technology. If embracing an AI-driven management platform leads us to significant reductions in human resources, we may ultimately experience a diminished capacity for self-performance. Our reliance on external vendors could grow to the point of no return.

This imbalance raises concerns about our ability to ensure quality and accountability, especially in two key areas:

- *Decision-making.* Human judgment is vital for complex decisions that AI may not handle effectively.

- *Emergency response.* Human presence is crucial for immediate responses to unforeseen situations. With fewer onsite personnel, clear roles and responsibilities are crucial during emergencies. Effective evacuation strategies must be developed and regularly tested to ensure safety and operational resilience.

Security Risks and Implementation Threats

The integration of AI into facility security is redefining the role of security professionals, paving the way for greater impact and career advancement, while at the same time creating new challenges. While AI-driven building management systems have not yet been the primary target, the vulnerability of healthcare IT and OT systems and the great value of attacking them should cause us in facilities to be vigilant in this area.

For decades before the rise of AI, the healthcare industry has been a prime target for cyberattacks, specifically ransomware-related breaches. Its interconnected systems, complex IT environments with various connected devices, and a web of third-party software make it a particularly vulnerable target. Add to that the critical nature of lifesaving care and the value of sensitive personal data, and you also have a particularly lucrative target. For the 13th year in a row, in 2023, the healthcare industry reported the most expensive average cost ($10.93 million) for single data breaches of any industry (World Economic Forum, 2024).

These attacks can even present an existential threat to healthcare organizations. A case in point happened in June 2023, when St. Margaret's Hospital in Spring Valley, Ill., became the first healthcare institution to permanently cease operations due in large part to the lasting fallout from a ransomware attack two years before (Southwick, 2023).

And they could be deadly. If one of our autonomously operated buildings gets shut down in a cyberattack, and we have a patient on the way to the OR at that moment, and they become trapped in an elevator, they could die. What if there is a fire and the warning and suppression systems malfunction? What happens if an imminent security threat exists in one of our autonomously managed buildings, such as an active shooter? The AI-driven electronic management tools (e.g., check-in/-check-out systems) we now have at our disposal may not fully address these issues.

Bringing Balance Through Effective Vendor Management

The examples I gave above are not doomsday scenarios—they are real things that can and will happen. Some issues make the case for balancing the seesaw between

having buildings run efficiently with a degree of autonomy and having people on site who know how to turn a wrench. Facilities must ensure that clear performance benchmarks and oversight mechanisms are instituted with vendors when we adopt these platforms. This requires implementing clear key performance indicators (KPIs) to monitor vendor performance effectively. It starts with negotiating flexible agreements that allow adaptability to changing circumstances. When setting up contracts with these vendors, we must ensure that security protocols are in place.

Clear KPIs and associated performance metrics must be incorporated into contracts with these vendors, and a few of my own come to mind immediately in this vendor management context. (Note that you may have different names from mine for these metrics.)

Some of those critical KPIs/metrics I believe should be prioritized include:

Cybersecurity Risk. How many security breaches or incidents have been attributed to the vendor? What is the character and severity of vulnerabilities identified in third-party audits? How well does the vendor adhere to standard security frameworks, such as the NIST Cybersecurity Framework and ISO 2700?

Risk Mitigation Planning. How well has the vendor prepared for potential disruptions or crises (e.g., security incidents, and natural disasters)? Do they have a documented business continuity plan? Can they demonstrate that they have been able to recover quickly from past disruptions? Do they conduct regular reviews and updates of their contingency plans?

Vendor Performance Index. This KPI is an overall score of vendor performance that considers multiple factors, including quality, price, service, and delivery. Important metrics for developing such an index include an aggregate score from multiple KPIs, including cost control, consistency of performance over time, and ability to meet all service line agreements in their contracts.

Vendor Relationship Management. This KPI measures vendors' relationship quality with your facility's operation. How often does the vendor communicate with and/or hold meetings with your team? What is their level of collaboration on new initiatives? How high do your internal teams rate them on vendor satisfaction scores?

Conclusion

Achieving the balance between technological innovation and human oversight is key to effective facility management. Combining AI capabilities with skilled personnel ensures safe, efficient, and sustainable operations. AI-powered predictive analytics will help enable proactive asset management, optimize costs, and minimize risk. This holistic integration can help deliver a collaborative approach—which has traditionally eluded facilities management—more easily within our grasp.

Looking forward, emerging cybersecurity protocols, evolving AI governance policies, and strategic vendor partnerships will further shape the role of AI in facility management. By proactively addressing these factors, facility managers can harness AI's benefits while mitigating its risks, leading to more resilient and responsive facility operations.

References

Baskher, S., Bruce, D., Lamb, J., & Stein, G. (2023, July 10) Tackling healthcare's biggest burdens with generative AI. Mckinsey. https://www.mckinsey.com/industries/healthcare/our-insights/tackling-healthcares-biggest-burdens-with-generative-ai#/

Honeywell. (2025). Honeywell Forge. https://www.honeywell.com/us/en/solutions/honeywell-forge

Johnson Controls. (2025). OpenBlue Platform and technology. https://www.johnsoncontrols.com/openblue/platform-and-technology

Lorenzi, N. (2025, Feb. 27). Maintenance software features keep expanding: Computerized maintenance management companies embrace advanced technologies. *Health Facilities Management*. https://www.hfmmagazine.com/maintenance-software-features-keep-expanding

Southwick, R. (2023, June 20). After cyberattack and other financial woes, an Illinois hospital closes its doors. *Chief Healthcare Executive*. https://www.chiefhealthcareexecutive.com/view/after-cyberattack-and-other-financial-woes-an-illinois-hospital-closes-its-doors

World Economic Forum. (2024, Feb. 1). Healthcare pays the highest price of any sector for cyberattacks — that's why cyber resilience is key. https://www.weforum.org/stories/2024/02/healthcare-pays-the-highest-price-of-any-sector-for-cyberattacks-that-why-cyber-resilience-is-key/