California Management Review

TECHNOLOGY

Smart Buildings and the Management Paradigm Shift

by Steve Griffith and J. Mark Munoz

Image Credit | Matthew Henry

AI is providing building operators new capabilities for improving operations, incorporating internal & external datasets.

INSIGHT | FRONTIER 03 Oct 2022

Emerging technologies relating to smart buildings are being created throughout the country and worldwide (NEMA Electroindustry Magazine- Enabling AI within Smart Buildings, Jan 2022). The number of smart buildings worldwide is expected to increase by 150% to reach 115 million in 2026 from the present number of approximately 45 million (Lebow, 2022). The market size is projected to exceed $130 billion by 2027 (Reportlinker, 2022). This article highlights key developments in the industry and the accompanying changes in management practice.

RELATED CMR ARTICLES

"A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence" by Michael Haenlein & Andreas Kaplan. (Vol. 61/4) 2019.

Smart Buildings and Artificial Intelligence (AI)

Once composed solely of mechanical and electrical parts, buildings have become complex systems that combine hardware, sensors, data storage, microprocessors, software, and connectivity in several ways. Driven by increases in processing power, network connectivity, enhanced data and analytics capabilities, improvements in energy efficiency, occupant comfort, and physical and cyber security, buildings are raising the stakes for building owners, operators, investors, and tenants.

Furthermore, the development of smart devices, wireless networks, and data platforms are forcing vendors to consider how value is created and captured, how the growing amount of newly generated data is utilized and managed, and how relationships with traditional business partners and competitors are redefined. The increasing use of artificial intelligence (AI), an umbrella term for enabling technologies that allow machines to mimic human-like decision-making, is providing building operators, vendors, and other stakeholders even more advanced capabilities for improving building operations, while incorporating a vast array of additional datasets from both internal and external sources.

Several applications within a smart building can help operators achieve these goals. While all rely on data and analytics, some are likely to further benefit from incorporating AI. The capabilities of smart, connected products – whether powered by analytics, AI, or a combination of both – can be classified into four main areas: monitoring, control, optimization, and autonomy.

Monitoring

Connected devices permit the comprehensive monitoring of a product's condition, operation, and external environment through sensors and external data sources. A product can use data to alert operators to changes in situations or the performance of the device itself. Smart environmental sensors that track noise, light, CO2 particulates, and volatile organic compounds are a representative use case. AI machine learning algorithms can identify areas of high occupant density or poor air quality, directing staff to increase cleaning frequency.

Control

Users can control connected devices via remote commands or algorithms built into the device or that reside in the product cloud. These can be triggered by pre-set thresholds or by using intelligence that learns from specific patterns in data and allows the product to respond based on those conditions. A representative use case with a smart building is the building's renewable energy management system. Using AI algorithms, decentralized energy sources can send any excess electricity they produce to the grid, so utilities direct that power to where it's needed.

Optimization

The influx of data from connected devices merged with the ability to control product operation, allows buildings to optimize performance in numerous ways, many of which have not been previously possible. Intelligent lighting systems that can be optimized based on patterns of use, particularly for common areas, hallways, and building exteriors.

Autonomy

Combining monitoring, control, and optimization capabilities can permit connected devices to operate autonomously with little human input. A representative use case within the smart building is de-icing and snow melting, where AI algorithms can intake sensor data from building surfaces or adjacent sidewalks/roads and learn to heat up automatically, or melt snow, or send signals to close/restrict access to areas that are not safe for vehicles or pedestrians.

AI and Data in Smart Buildings

Modern buildings are comprised of complex mechanical equipment, powerful control systems, and numerous applications designed to improve the safety, comfort, and productivity of occupants, as well as reduce operating costs and limit the building's environmental impact. While any single building device or system can be optimized to improve efficiency or reduce operating costs, the real value is when individual building systems are linked together, combined with external data sources, and then managed as an integrated system that can provide a high degree of optimization and automation.

Whether AI is utilized or not, the smart buildings industry is driven by data. Some key data sources within a smart building are physical machine data, building sensors, cameras/microphones/occupancy sensors, ambient sensors, digital tracking technology, and external data sources. Organizations need to understand the strategic approaches for acquiring, using, storing, and sharing data, as well as the technical issues associated with integrating and making data available wherever needed to improve efficiency, provide occupant comfort, or facilitate safety. To fully reap the rewards of AI and the connected infrastructure commonly deployed in smart buildings, operators need to focus not on applications or technology but on their strategies and tactics for data use and management.

Data governance is a collection of processes, roles, policies, standards, and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals. Within a smart building environment, there are several benefits to establishing good data governance (where the data has been properly cleaned, segmented, and labeled), particularly when planning a comprehensive data quality and security strategy. Good data governance policies can provide a wealth of benefits, including:

- The ability to track and safeguard data usage, while also recognizing data errors and raising red flags that can lead to eliminating those errors

- Helping to reduce amount of time it takes to cleanse, prepare, and backfill holes in data

- Allowing an organization to focus on creating, testing, and refining analytical, physical, or AI models instead of verifying data is clean, verified, and available.

- Enabling organizations to treat data as a strategic asset, which allows for specific goal planning and measurement.

In essence, the overall operational benefits derived from the establishment of smart buildings is largely based on the quality of data gathered and how it is managed.

Managing New Challenges and Concerns

In cases where new technologies, processes or systems are introduced in organizations, difficulties may arise. Similarly, when buildings and its supporting administration become more intuitive a new set of challenges and concerns emerge.

Maintaining data accuracy and integrity. A significant barrier to effectively managing and using data across a building's entire ecosystem is the requirement that data used in statistical or neural models must be valid, clean, accurate, and properly labeled. As with any information system, bad data will result in flawed assumptions and predictions. With AI technologies, clean data is critical, as a supposedly valid AI prediction can prove misleading if the supporting information is not correct or adequately understood. Many vendors now offer data cleaning, formatting, and labeling services, either on a standalone basis or as part of their AI offering.

Ensuring privacy. One of the key concerns with data collection within a smart building is data privacy. While much of the information collected by vendors and operators is solely machine-generated, sensors that capture information about people can be subject to specific data privacy laws, such as *General Data Protection Regulation* (GDPR) or *California Consumer Privacy Act* (CCPA). That's why building operators need to make sure that certain data, such as a person's image, records of their comings and goings, and other attributes that would be considered personal or private, are properly anonymized, obfuscated, or destroyed, to ensure they are not subject to the data storage and handling requirements of personal privacy data regulations.

Elevating security. The most advanced smart buildings generally have key systems connected to the Internet, so they can send or receive data from external sources, a cloud server, or other edge servers. As such, significant security issues are at stake, as IoT devices are vulnerable to medium or high-severity attacks. To protect against increased cybersecurity risks, smart building companies should: comply with the latest cybersecurity standards, conduct a risk-based asset/threat assessment, promote internal and external cybersecurity awareness, establish procedures for incident assessment and handling, insist on security standards adherence across the supply chain, and establish data security as part of an overall data governance strategy.

Overcoming skill gaps. Most building operators are not experts in developing the software, analytical tools, and algorithms that are increasingly being utilized to enable more advanced smart building applications and have, therefore, turned to software and platform developers. Similarly, building controls and device manufacturers are experts at developing and deploying traditional devices within a structure but are often less experienced in handling complex inter-system integration work and may not have significant experience developing complex new data-driven or AI-driven algorithms.

Refining the business model. The traditional model of smart building projects starts with Capex spending on new hardware, which is also common for new buildings. Opex or as-a-service model spending is gradually being integrated but will most likely come from the project's software/application side. As a result, as vendors respond to the changing market demands and try to introduce more software, analytics, and service offerings, they need to consider new business models to position themselves for future growth, including embracing the as-a-service model (Opex model). This trend has also been boosted by the presence of IT vendors and startups in the market that were pioneers in launching as-a-service solutions (either SaaS or PaaS). In the emerging business model, companies are targeting the application first — sometimes providing an "outcomes-as-a-service"-type model.

Navigating an uneven ecosystem. Another key challenge for smart building vendors is the inertia of the construction industry and value chain. The construction market is usually very traditional; it proved to be a slow adopter of new techniques and technologies. The sector leans on traditional building technologies, which, in turn, rely upon traditional skilled and unskilled trade workers. The question is, therefore, how quickly the market can adapt to these new models.

It is evident from these mentioned challenges that organizational frameworks need to be refined to match the changing circumstances.

Shift in the Management Paradigm

Amidst all these developments, organizations need to learn to manage their operations in new ways.

1. ***Cognitive alignment***: A designated team should monitor and track data gathered and analyze them. The cognitive power of the building should be in sync with that of the organization.

2. ***Agile response***: The organization needs to match the speed of the data processing from smart buildings. Executives need to gather, analyze, and respond to information quickly.

3. ***Heighted security sensitivity***: Organizations need to be prepared to invest in talent, technology, and resources to protect data security.

4. ***Operational connectedness***: Organizations need to be accustomed to the idea of being perpetually linked to a vast external network consisting of suppliers, vendors, customers, and other stakeholders.

5. ***Structural transformation***: Organizations would have to reconfigure their organizational structure and even policies and procedures to best adapt to smart buildings.

In workplaces worldwide, it's not just people and work processes that have gained a new level of cognition. The external edifice housing the organization has become exponentially smarter, requiring a management paradigm shift to optimize business performance.

References

Lebow, S. (2022). Smart building deployments are headed through the roof. Insider Intelligence. Accessed July 27, 2022. Available at: **https://www.insiderintelligence.com/content/smart-building-deployments**

NEMA Electroindustry Magazine, January 2022/Vol. 27 No. 1. Accessed July 27, 2022. Available at: **https://www.nema.org/news-trends/ei/view/enabling-ai-within-smart-buildings**

Reportlinker.com (2022). Global smart buildings market size, share and industry trends analysis report 2021-2027. Global News Wire. Accessed July 27, 2022. Available at: **https://www.globenewswire.com/news-release/2022/05/05/2436441/0/en/Global-Smart-Buildings-Market-Size-Share-Industry-Trends-Analysis-Report-2021-2027.html**

Steve Griffith Follow

Steve Griffith is a Senior Industry Director for NEMA's Transportation Systems Division. He manages sections within this division in such areas as Intelligent Transportation Systems (ITS), Electric Vehicle Supply Equipment, Rail Electrification, Automotive Components, and Imaging & Communications. He is also the principle NEMA staff liaison for NEMA's Cybersecurity activities.

J. Mark Munoz Follow

Dr. J. Mark Munoz is a tenured Full Professor of Management at Millikin University, and a former Visiting Fellow at the Kennedy School of Government at Harvard University. Aside from top-tier journal publications, he has authored/edited/co-edited more than 20 books such as: Global Business Intelligence and The AI Leader.