KPMG

From algorithm to action:

Digital infrastructure, essential services, and key national assets



AI generated image

Digital infrastructure, essential services, and key national assets

Physical AI (PAI) is increasingly used to monitor, control, and maintain critical infrastructure. In data centers, PAI can manage power and cooling, detect equipment issues, and support robots that install or service servers. At ports, AI can coordinate autonomous cranes and vehicles to move containers more efficiently. In energy networks, drones can inspect remote power lines, while AI-enabled systems can forecast demand and balance electricity loads. These applications connect AI decision-making with physical assets to improve efficiency, reliability, and resilience.

However, the consequences of failure in these systems carry a different weight since a failure here is rarely a localized event. A compromised AI in a data center could trigger a cascading hardware meltdown, destroying the critical data of countless organizations. A hijacked AI orchestrating a port could halt the flow of essential goods, creating immediate and widespread economic disruption.



AI generated image

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

What organizations must plan for

When the asset itself is a nexus of commerce, the stakes are about economic and national security. Developing safe and trusted systems is paramount. Organizations can start with the following actions:



Strategically identify PAI opportunities.

Develop a strategic roadmap for PAI deployment. This involves identifying the highest-value use cases, whether for optimizing port logistics, enhancing data center energy efficiency, or deploying autonomous inspection drones and prioritizing them based on a clear business case and risk assessment.



Implement PAI-driven predictive maintenance.

Leverage the sensing capabilities of PAI to shift from reactive repairs to predictive asset management. This includes using AI to analyze thermal, acoustic, and vibration data to foresee failures in critical machinery (such as power converters or cooling pumps) before they lead to costly downtime.



Develop a grid-responsive energy strategy.

Large power consumers such as data centers can use AI to shift flexible computing work off peak periods and pair it with on-site batteries so the facility supports the grid instead.



Conduct integrated PAI threat modeling.

Perform security assessments that model how a single cyber-attack could cascade into a kinetic event, such as a compromised PAI system causing physical equipment damage or a widespread service outage and failure of response protocols.



Design and test manual overrides.

Regularly stress-test manual fallback procedures that allow human operators to safely retake control of an autonomous system during a security incident or AI failure.



Build a unified compliance and assurance program.

Create an evidence-based compliance program that addresses the overlapping requirements of traditional OT security (NIST SP 800-82), AI risk management (NIST AI RMF), and specific, high-stakes regulatory mandates from entities like NERC for grid reliability and CISA for national security.

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Wins for our clients

The pain point	The solution	The value
Creating a robotics transformation strategy A company had a vision for an automated data center and needed to connect that high-level goal with a practical roadmap for identifying high-value robotics opportunities and integrating them safely into live operations.	**Developed a business-centric deployment strategy** Conducting detailed "as-is" process mapping to identify high-value opportunities and then defining the future state through new operational workflows and an integrated automation operating model.	**A clear, actionable strategy for automation** The organization moved from a high-level concept to a concrete, data-driven plan. It now has a prioritized roadmap for deploying robotics, a clear understanding of the expected business outcomes, and the operational model required to scale. 01
Unpredictable system-wide risks The company's complex and interconnected port operations made it difficult to anticipate how equipment failures or new optimization strategies (e.g., for crane scheduling) could create cascading bottlenecks across the entire terminal.	**Established a control tower for the port** Creating a dynamic, data-digital twin of the entire terminal. This allowed the enterprise to simulate and validate the real-world impact of new automation strategies and PAI threat scenarios in a safe, offline environment.	**Data-driven optimization and enhanced resilience** The company can now safely test and de-risk new operational strategies before deployment, identifying potential bottlenecks and security vulnerabilities and gaining the ability to optimize throughput while building a more resilient and predictable supply chain hub. 02

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Sector Experts



Vijay Subramanyam

Consulting Industry Leader – TMT and OpenAI Platform Leader
KPMG Advisory
E: vijaysubramanyam@kpmg.com

Vijay leads the firm's consulting strategy and delivery for clients across the TMT sector, helping them navigate disruption, accelerate digital transformation, and unlock sustainable growth. As the OpenAI Platform Leader for KPMG in the US, he helps clients realize the value of AI-native enterprise transformations using OpenAI platforms.



Iacopo Gambino

Digital Infrastructure Leader
KPMG Advisory
E: iacopogambino@kpmg.com

Specializes in digital infrastructure strategy and investment, providing a unique perspective on how Physical AI, connectivity, compute, data centers, and intelligent networks can strengthen the resilience and performance of digital infrastructure and nationally significant assets.



Greg Corlis

Emerging Technologies & Physical AI Leader
KPMG Advisory
E: gcorlis@kpmg.com

Focuses on emerging technologies and Physical AI, helping organizations harness robotics, autonomous systems, digital twins, and AI-driven operations to transform the management, protection, and productivity of this sector.



Chris Corteen

Emerging Technologies and Innovation Expert
KPMG Client Technology & Innovation
E: ccorteen@kpmg.com

Brings expertise in emerging technologies and innovation, helping organizations identify, incubate, and scale Physical AI capabilities that create new operating models, workforce approaches, and mission outcomes across strategic national assets, digital infrastructure, and key national assets.

We would like to thank our contributors:

Core Contributors: Brad Raiford, Stephanie Kim, Priya Roy, Cedric Carter

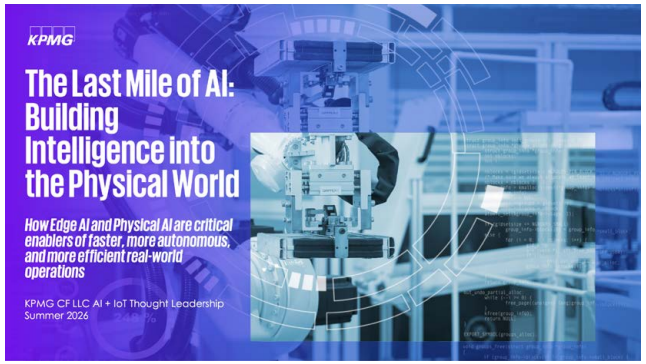
Editorial and Design Team: Rama Ramaswami, Sohini Roy, Lara Volpe

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Related thought leadership



KPMG 2026 Frontiers Report: AI as the frontier multiplier



The Last Mile of AI: Building Intelligence into the Physical World



From algorithm to action: A framework for safe and secure physical AI

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Please visit us: **kpmg.com** **Subscribe**

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future.
No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

DASD-2026-20825