THE ARCHON

TECHNOLOGY INTELLIGENCE

EXECUTIVE BRIEF

Why Physical AI & Robotics Now?

Global robotics spending is projected to exceed $150 billion by 2027, driven by AI-enabled machines that can perceive, decide, and act autonomously.

CONTROL FRAMEWORK

Enterprise Use Cases with Tangible ROI

Manufacturing lines use collaborative robots for precision assembly, warehouse operators deploy autonomous mobile robots to handle a large share of pick-and-pack tasks, and data centers employ robotic arms for hardware replacement, resulting in a notable reduction in labor hours.

→ Precision assembly in manufacturing

→ Autonomous mobile robots in warehouses

→ Robotic hardware handling in data centers

CONTROL FRAMEWORK

New Attack Surface for Physical AI

Sensors can be spoofed, firmware can be hijacked, and ransomware can lock robot motion, turning assets into safety hazards.

→ Sensor spoofing

→ Firmware hijack

→ Ransomware lockout

CONTROL FRAMEWORK

Safety & Security Standards to Adopt

ISO 10218-1 defines safety requirements for industrial robots, ISO/TS 15066 extends them to collaborative robots, and IEC 62443 provides a defense-in-depth model for industrial automation networks.

→ ISO 10218-1 – Industrial robot safety

→ ISO/TS 15066 – Collaborative robot safety

→ IEC 62443 – Industrial automation security

CONTROL FRAMEWORK

Integration Architecture: Edge, 5G, Digital Twin

Edge compute processes sensor data locally to meet sub-millisecond latency, 5G delivers reliable high-bandwidth links for fleet coordination, and digital twins simulate robot behavior for predictive maintenance.

CONTROL FRAMEWORK

Governance Aligned with US AI Executive Order 14110

The order mandates risk assessments, documentation of data provenance, and continuous monitoring for AI systems that affect physical safety, requiring enterprise AI governance boards.

CONTROL FRAMEWORK

Building Organizational Maturity

Successful programs combine robotics engineers, data scientists, security analysts, and operations managers in a shared governance model, with a phased rollout: pilot → expand → optimize.

- → Cross-functional teams
- → Phased rollout (pilot, expand, optimize)
- → Continuous improvement loop

EXECUTIVE TAKEAWAY

Executive Takeaway

Start with high-impact, low-risk pilots, embed safety and security best practices, align AI governance with relevant government guidance, and invest in talent pipelines to scale trustworthy physical AI.

→ Identify pilot use cases

→ Apply safety and security best practices for robotics

→ Implement AI governance aligned with government guidance

→ Develop cross-functional talent