

EXECUTIVE BRIEF

Why Operational Technology Belongs on the CIO's Agenda

The case from *The Smart Campus Manifesto*

The question

A CIO states: “This OT stuff isn't on my radar right now, and I have many other priorities. Why should I care about it in the context of everything else?” The concern about taking on additional responsibilities is understandable. Traditionally, building controls, utilities, and door hardware have been managed by Facilities, and the CIO's to-do list is already crowded. *The Smart Campus Manifesto* counters this by arguing that the assumption is outdated: operational technology is now a CIO's issue, even if they lack the visibility to oversee it.

The response

“You are already accountable for it. The air gap is gone: the chillers, door controllers, lab ventilation, and vendor remote-access tunnels sit on or beside your network, and when one is breached, it will be treated as a cyber incident on your watch. The choice is not whether to take on OT. It is whether you govern that exposure or inherit it unmanaged. And it is not one more item on the list, because it is where some key answers to your budget and security problems are.”

Four reasons it is already on the CIO's plate

1. **Accountability without oversight.** The technology leader is responsible for institutional security but has what the book calls a “critical blind spot”: thousands of physical devices overseen by Facilities or academic departments outside IT control. In its words, “the cybersecurity perimeter no longer ends at the firewall”; it now includes boilers, chillers, fume hoods, and life-safety systems (Ch. 1, pp. 28–29).
2. **The consequences are physical.** An IT failure halts digital services. An OT breach can freeze pipes, destroy climate-sensitive research samples, or lock down residence halls. The book's example is an unsecured thermostat used as a backdoor into financial systems, or a heating plant held to ransom during a winter storm (Ch. 3, “The Perimeter Illusion,” p. 66).
3. **It is the answer to “do more with less.”** The usual IT efficiency levers of cloud migration, vendor consolidation, and license negotiation have been pulled. The book argues that “the significant inefficiencies on campus are not in the server room, but in the boiler room,” and that applying analytics and automation to the physical plant moves IT from cost center to “value generator.” It states plainly that the shift to OT “is not scope creep” (Ch. 1, p. 29).
4. **Insurers and the board are already asking.** Cyber insurers now expect evidence of a NIST-aligned OT security program: segmentation, privileged-access control, and continuous monitoring. Risks

that touch life-safety systems are meant to be escalated as explicit Cabinet or Board decisions, not accepted silently by default (Ch. 17).

What an AI-enabled digital twin adds

It closes the blind spot. The CIO's underlying problem is that nobody can govern what nobody can see. A digital twin combines spatial data (BIM and GIS), static asset records and live telemetry into one model of the campus. Willow's knowledge graph represents each asset in relation to the system, zone, floor, and building it serves, so a fault on one floor can be traced to a valve three floors below. At Northern Arizona University, the first U.S. university to deploy Willow, this meant pulling more than eleven disconnected sources into a single view, including building automation, metering, work orders, and occupancy. For a CIO, that is a working inventory of connected OT and a shared operating picture with Facilities.

It makes the financial case concrete. NAU identified more than \$200,000 in avoidable operating costs in its first six months, and found that many offices and classrooms were occupied about half the time while being fully conditioned. Georgia Southern University, managing more than 100 buildings, reports roughly \$1 million in operating savings within nine months, in part by checking whether a closed work order had fixed the underlying fault. The twin also changes the risk picture: at NAU it surfaced hidden water leaks that experienced staff had ruled out, and flagged conditions that could have repeated a flood that had previously closed an academic building.

It works with the estate the campus already has. Most campus OT speaks BACnet or Modbus, protocols never designed for cloud connectivity. Gateways translate that traffic so decades-old equipment can join the model without replacement. The same platform addresses the workforce gap: Willow Copilot answers technicians' questions from the institution's own manuals and maintenance history, and NAU reports that new technicians become effective within their first week.

It is not a security control, and it raises the stakes. A twin concentrates operational data and, once features such as Willow's Active Control are switched on, can change setpoints on physical equipment. The Manifesto's guardrails therefore come first: zones-and-conduits segmentation, a one-way gateway from OT to the cloud wherever feasible so a cloud breach cannot manipulate hardware, and controllers that can maintain life safety on their own if the connection is lost (Ch. 17, p. 317). Willow's reported posture of ISO 27001 and SOC 2 Type 2 certification with single-tenant deployment helps, but it does not replace the institution's own architecture.

Two cautions for the executive conversation. First, a twin is only as good as the data behind it. The book warns of "semantic rot" when models are not maintained as rooms, sensors, and settings change, so data stewardship has to be funded as an ongoing cost (Ch. 3, pp. 65–66). Second, the savings figures above come from the book's case study, which draws largely on Willow's own published material, and the book itself notes research on the gap between "marketing rhetoric" and "technical realities" in this market. It recommends reference visits and a phased rollout over a "big-bang" deployment.

A proportionate first step

None of this requires the CIO to take over Facilities. The book's operating model is deliberately shared, which is what makes the ask manageable for a leader with a full agenda.

	CIO / CTO	Chief Facilities Officer
Owns	Identity, segmentation, vendor remote access, data governance	Safety standards, uptime, commissioning, maintenance, lifecycle planning
Priority model	Confidentiality, integrity, availability	Safety, reliability, availability
Shared	One cyber-physical risk register, reported to Cabinet and Board each quarter; joint incident playbooks and tabletop exercises	Same register, same playbooks

Three actions start the work without a large budget request:

- **Inventory jointly.** Catalog connected OT and vendor access with the facilities chief, using the book's Cyber-Physical Asset Audit Form (Appendix, p. 397).
- **Stand up the shared risk register** and put OT on the existing enterprise risk agenda, starting from the Top-10 OT Risks Register (Appendix, p. 441).
- **Scope a digital twin pilot** on a small set of buildings where energy cost or research risk is highest, with segmentation and data ownership agreed before anything is connected.

Source. Steve Burrell, *The Smart Campus Manifesto*: Chapters 1–3, 15, 17 and 20; the Northern Arizona University case study (pp. 419–428); and the Willow Digital Twin case study (pp. 429–438). The book generally uses “CTO” for the senior technology role; this brief applies the same argument to the CIO, as the book's glossary and Chapter 17 do. Figures and vendor claims are as reported in the book and have not been independently verified.

For more information and resources associated with *The Smart Campus Manifesto*, visit <https://thesmartcampus.com>