

The CTO and CFaO Cross Domain Knowledge Map

There has historically exists a gap and cultural divide between Information Technology (IT) and campus Operational Technology (OT). Chief Technology Officers typically focus on the "CIA triad"—Confidentiality, Integrity, and Availability—for digital systems and data. However, they often overlook the rapidly expanding OT, which includes critical building controls and life-safety systems. Meanwhile, the Chief Facilities Officer emphasizes safety, uptime, and the management of long-lasting assets. Since CTOs implement enterprise standards related to identity, security, and data governance within the shorter IT system life cycle, they must develop into "Integrative Architects." These leaders will need to strategically unify the "wrench and the keyboard" to create, secure, and enhance a campus-wide, integrated cyber-physical system.

What the CTO Needs to Know About Facilities and OT

Facilities mission and "always-on" obligations: life safety, compliance, research continuity, and the reality that many buildings must operate 24/7 with minimal tolerance for downtime.

Deferred maintenance as a technology risk multiplier: aging equipment, "patchwork" upgrades, and failing controls increase failure rates, expand cyber-attack surface, and complicate integration.

Core OT systems and how they interrelate: BMS/BAS, EMS, SCADA (where applicable), lighting controls, metering/submetering, access control, video, district energy plants, and CMMS/work orders.

Key building standards and protocols: BACnet (esp. BACnet/IP), Modbus (RTU/TCP), LonWorks, KNX, DALI, plus IoT messaging like MQTT and typical integration patterns (gateways, drivers, brokers).

Controls modernization pathways: controller refresh vs overlays, point mapping, tagging strategy, sequence-of-operations governance, commissioning/retro-commissioning.

Facilities success metrics: IAQ, comfort, energy intensity, service calls, uptime, asset life, maintenance backlog, and customer experience.

Vendor and integrator ecosystem: mechanical/electrical contractors, controls vendors, commissioning agents, security vendors, ESCOs—each with different incentives and maturity.

Safety and regulatory context: code compliance, permitted work, life-safety boundaries, and why some systems cannot be "experimented" on in production.

Digital twin readiness: accurate spatial/static data (BIM/as-built, GIS), reliable live telemetry, and operational workflows that convert insight into action.

What the Facilities Leader Needs to Know About IT

IT mission and risk model: confidentiality, integrity, and availability—plus how cybersecurity risk, privacy obligations, and audit requirements shape architecture choices.

Cybersecurity fundamentals for cyber-physical environments: segmentation, least privilege, endpoint hardening, logging, and incident response—applied to OT without breaking uptime.

Identity and access management (IAM): authentication, RBAC, MFA, privileged access, vendor access models, and service accounts—especially for contractors and integrators.

Networks as a shared utility: routing, VLANs, firewalls, DNS/DHCP, Wi-Fi design, private cellular/CBRS, quality of service, and why small network changes can destabilize building controls.

Data estate architecture: normalization, metadata/tagging, time-series storage, APIs, event streams, and integration patterns that enable analytics and digital twins.

Service management discipline: change control, release management, SLAs, outage communications, and operational handoffs from IT to facilities workflows.

Vendor risk management: contract language, data ownership, patch responsibilities, third-party access controls, and avoiding brittle one-off integrations.

Privacy and compliance: occupancy, access, and video data implications; retention; minimization; and governance that preserves campus trust.

Operational analytics mindset: fault detection and predictive maintenance only matter if they drive dispatch, prioritization, verification, and continuous improvement.