Trinity Consultants

WHITE PAPER

Embedding AV/IT and Security into Sustainable Data Center Design

Critical decisions at the start of design can ripple for decades, driving cost and credibility while shaping long-term carbon impact.

Data centers have become the backbone of the digital economy. Every financial transaction, streaming service, and AI workload depends on them, and the pace of construction is accelerating to keep up with demand. But building more capacity is only part of the story. Each new facility must now be delivered faster and operated with greater reliability, all while meeting higher environmental standards.

That pressure has pushed AV/IT and security systems from a supporting role to core infrastructure. They dictate how reliably facilities operate and how efficiently power and cooling are used. When they are treated as afterthoughts, the result is fragile capacity and expensive retrofits. When they are embedded early, they strengthen both operational resilience and sustainability outcomes.

With so much at stake, early design choices ripple forward for decades. Decisions about redundancy and network architecture determine whether facilities remain adaptable or lock in constraints. Coordination with mechanical and electrical systems shapes daily operations. Policies for monitoring and retention influence long-term efficiency as well as compliance with environmental and regulatory requirements.

This paper examines the market pressures behind these shifts and shows how deliberate integration of AV/IT and security from the outset can both reduce project risk and position data centers to thrive in a rapidly evolving digital economy.

THE MARKET FORCES RESHAPING DATA CENTER DESIGN

Demand for new capacity has never been higher. The shift to AI workloads, rapid growth in cloud services, and the digitization of essential services are accelerating delivery schedules. Owners want facilities that come online faster and operate reliably.

Compressed timelines demand speed and precision. Owners and developers face pressure to bring capacity online quickly; in some markets, the expected delivery window has dropped from three years to as little as 18 months.

This pace leaves no room for systems to be treated as add-ons. AV/IT and security planning must be carefully coordinated with architectural and mechanical design to prevent delays that could cascade across the schedule.

To meet those deadlines, projects increasingly rely on modular and prefabricated methods. Electrical and mechanical rooms now arrive as integrated assemblies, and racks and security panels often ship pre-built. This accelerates delivery while reducing on-site labor but locks in design decisions much earlier. Late requests for AV, IT, or security changes usually trigger costly rework. Technology is evolving at the same pace. Driven by higher bandwidth demand and lower energy loss, fiber is replacing copper as the default backbone. The growth of high-density racks and the need for advanced monitoring also increase system complexity. These changes require more coordination across disciplines and more foresight in planning. Delaying decisions only compounds risks of costly rework and stranded capacity.

At the same time, sustainability has moved from aspiration to mandate. Global electricity demand from data centers is expected to more than double by 2030, reaching nearly 1,000 terawatt-hours annually.[1] Owners are under pressure to document measurable improvements in energy use and water consumption. Many jurisdictions now tie permits or incentives to these metrics, which means AV, IT, and security decisions made in the early design phases can determine whether a project qualifies.

THE CRITICAL DECISION POINTS IN DATA CENTER CONSTRUCTION

Successful integration of AV/IT and security depends as much on timing as on technical choices. Decisions that lag behind construction milestones often resurface later in the form of costly retrofits or operational blind spots that strand capacity. For a successful integration, teams should follow a disciplined sequence that mirrors the way projects are built: early design and planning, infrastructure and pathway construction, MEP and white space coordination, system installation and pre-commissioning, and integrated systems testing and commissioning. Addressing AV/IT and security at each stage helps ensure that they function as core infrastructure rather than last-minute additions.

Phase 1: Early Design & Planning (Conceptual + Schematic Phases)

Early-stage design impacts efficiency (how smoothly systems run day to day and how resilient they are under failure) and scalability (how easily devices, zones, or capacity can be added without major construction).

This phase is where the philosophy for resilience and security is set. Redundancy strategies (whether N, N+1, or 2N) must be weighed against business priorities to avoid both over- and under-engineering. Locking them in early ensures that AV/IT and security follow the same resilience model as power and cooling.

Just as critical at this phase is reserving the physical real estate. Security, AV, and IT systems need pathways (cable trays, conduit, and risers) and dedicated spaces (MDF/IDF rooms and control rooms) designed into the building fabric from the outset. Once slabs are poured and walls are framed, these accommodations become far more expensive to add, and their absence can create bottlenecks that cascade through construction and into operations.

This is also the point to define network architecture across production, security, building management, and AV systems and to confirm that power and cooling allocations can support the full equipment load.

[1] https://www.iea.org/news/ai-is-set-to-drive-surging-electricity-demand-from-data-centres-while-offering-the-potential-to-transform-how-the-energy-sector-works

Redundancy as a Technology Strategy

Redundancy models—N, N+1, and 2N—represent strategic choices that balance uptime, cost, and sustainability:

- **N** provides just enough capacity to meet demand, with no backup.
- **N+1** adds a single layer of protection, allowing for maintenance or failure without downtime.
- **2N** doubles capacity for full failover, ensuring continuous operation even in a major outage.

The right model depends on business priorities. A financial trading platform may justify 2N to eliminate risk of downtime, while a research workload may accept N+1 to save on capital and energy. AV/IT and security systems must be aligned to the same redundancy philosophy as IT and mechanical systems, or hidden single points of failure can undermine the entire strategy.

The decisions made during schematic design and early construction planning ripple forward for decades. If security is not addressed in parallel with other core systems, the result is often rigid, siloed infrastructure that is costly to scale and difficult to integrate into future strategies.

Phase 2: Infrastructure & Pathway Construction (Shell & Core Phase)

Once slabs are poured and walls are framed, flexibility is greatly reduced. Adding new conduit, risers, or cable trays at this stage is not only costly but often disruptive to other trades. That makes it essential to commit to the backbone infrastructure early.

This is when cabling architecture is determined: specifying trunk fiber routes, copper distribution runs, and the separation of production IT and security networks into secure, redundant spaces. Security and AV devices must be supported by dedicated power and network runs to avoid competition with IT production loads, and those runs must be sized and routed early enough to prevent late-stage improvisation.

Infrastructure pathways are particularly sensitive to congestion: Poorly routed cable trays and conduits can obstruct airflow, forcing costly rework and reducing efficiency. Improper pathway placement can increase cooling loads by 10–15 percent, driving higher energy use and operating costs. Device placement also comes into focus. Cameras, access readers, and AV hardware should be positioned for clear sightlines, accessibility, and ADA compliance, coordinated with architectural and MEP layouts to prevent later conflicts.

Phase 3: MEP & White Space Coordination

By this stage, the physical backbone is set and the focus shifts to how AV/IT and security systems coexist with mechanical, electrical, and plumbing infrastructure in the white space. IT and security systems often share pathways with mechanical and electrical sensors, which makes clash detection and resolution essential. Without close coordination, conduit runs, sensors, cable trays, and even lighting can collide, delaying schedules and creating rework.

Key coordination activities at this stage include rack layouts for security servers, storage, and AV processing equipment, ensuring that they align with IT's footprint and cooling design. Coordination at this point can also prevent missteps such as trays routed directly above HVAC units, which has forced some operators into costly rework when cooling airflow was starved. Unified coordination drawings and an assigned integration lead are the best defenses against these conflicts.

Treating physical security devices as IT workloads is essential. They require rack space, VLANs, PoE power planning, and cooling just like servers do. When security is treated as "just hardware on walls," it creates fragile systems that fail under load, whether due to power loss, network congestion, or storage overflow.

Integration also extends into operations. BMS, AV, and security systems should be tied into common monitoring platforms, creating a unified view of both facility and IT events. When physical access alarms and building system alerts correlate with IT anomalies, operators gain faster visibility into real risks.

Phase 4: System Installation & Pre-Commissioning

AV/IT and security systems are installed after the backbone and MEP infrastructure are complete. If sequencing is off, devices cannot be tested properly. Cameras without network switches or access readers without live power stall commissioning.

At this stage, critical systems such as video management (VMS), access control (ACS), and intrusion detection (IDS) are installed and configured. Equally important is validation of control environments—network operations centers and security command rooms with video walls, dashboards, and alerting systems—to confirm that operators will have full situational awareness once the facility is live. Pre-commissioning also provides an opportunity to right-size specifications before they are locked in. For example, matching camera resolution and frame rate to actual use cases avoids bloated bandwidth and unnecessary storage demand. A perimeter camera may require 4K for facial recognition, while interior monitoring may only need 1080p coverage. Differentiation reduces both power draw and storage arrays.

Testing at this phase should also go beyond individual devices to confirm redundant network paths, segmentation, and interoperability between IT monitoring and security platforms. Without this integration, operators are left with siloed alerts that obscure root causes. Locking these parameters into design documents prevents last-minute “bandit fixes”—bolted-on devices, ad hoc cabling, or undersized storage arrays added in the field.

Phase 5: Integrated Systems Testing & Commissioning

Resilience is proven only through realistic failure-mode testing. Facilities should undergo simulations such as pulling breakers, severing network paths, and forcing failover during peak load. These exercises validate that AV/IT, security, and MEP systems interoperate under stress.

Comprehensive commissioning goes further than simply powering devices on. It should validate multi-factor access control—including biometrics, card-plus-PIN, and visitor management—under live conditions. Video surveillance systems must be tested to ensure camera feeds persist through both power and network disruptions. Alarm signals should be traced end-to-end, confirming that escalations reach NOC and SOC dashboards without delay.

This phase also involves verifying that redundancy functions as designed. Dual power feeds, UPS support, and network failover paths for AV/IT and security systems must all be exercised during commissioning. Without these checks, vulnerabilities such as a badge reader tied to a single-sourced PoE switch or a video wall that goes dark during failover may only surface after go-live. Integrated testing under stress is the only way to reveal and resolve these weaknesses before the facility enters production.

Together, these phases illustrate that integration is not a single milestone but a continuous discipline. But while addressing phases in sequence is necessary, coordination across disciplines is equally critical. Even the best designs falter when systems collide in the field.

THE NEED FOR CROSS-DISCIPLINE COORDINATION WITH MEP AND BUILDING SYSTEMS

In a data center, AV/IT and security systems are just as integral to uptime as cooling and power. In many projects, however, they are addressed late in the process, leading to space conflicts, undersized rooms, or expensive rework. True resilience depends on giving these systems equal footing in the design sequence. When coordination slips, problems emerge that slow construction and compromise performance. These challenges are not abstract; they show up in very tangible ways, from overcrowded cable trays to overheated control rooms and inspection failures.

To prevent these outcomes, project teams need to anticipate and resolve several recurring coordination challenges:

Pathways and Space Conflicts

Dense cable trays, risers, and conduits demand as much real estate as chilled water lines or busways. When pathways are not reserved early, overcrowding can lead to airflow congestion, reduced cooling efficiency, and expensive rework. Coordinated drawings with overlays for MEP and low-voltage trades help avoid last-minute conflicts that compromise performance.

Power and Redundancy Alignment

From cameras and readers to NOC displays, VMS servers, and storage, AV/IT and security devices require the same resilience as IT racks. They must be supported by UPS-backed, dual-fed power and carried across redundant switches and pathways. If these devices are left on "standard" outlets or connected through a single leg, they become the weak link, undermining otherwise redundant infrastructure. Coordination with MEP is essential to avoid these hidden single points of failure.

Physical Security as Part of the IT Backbone

Cameras, access readers, intrusion sensors, and intercoms now function as network endpoints. They require rack space, VLAN segmentation, redundant PoE power, and cooling capacity just like IT workloads. Treating them as "hardware on walls" creates fragile systems with unmanaged risks — from single-path cabling to inadequate storage for video retention. Early design should map these devices into IT architecture, aligning PoE planning with A/B feeds, segregating traffic for monitoring, and ensuring that security storage and analytics platforms are sized for compliance. Designing security as part of the backbone ensures scalability and allows unified monitoring with the same rigor applied to IT infrastructure.

Ownership and Accountability

Mechanical and electrical scopes usually have clear owners, but AV/IT and security often fall into gaps between trades or report to different stakeholders than MEP engineers. These split lines of responsibility create disconnects, such as missed coordination between access control and fire alarms, or between AV controls and lighting systems. Successful projects close these gaps by designating an integration lead or independent reviewer. This role drives accountability across disciplines, enforces sequencing dependencies like ensuring conduit stubs are placed before walls are closed, and validates that all systems function as part of a unified infrastructure.

Environmental and Cooling Loads

AV/IT rooms such as IDFs, MDFs, SOCs, and command centers generate significant heat from servers, video walls, and storage arrays. If MEP sizing does not account for these loads, rooms can quickly overheat, leading to performance degradation and premature equipment failure. Early coordination allows cooling requirements for AV/IT and security spaces to be integrated into overall capacity planning, avoiding the need for emergency spot-cooling units or disruptive rebalancing.

Integration with the Building Management System (BMS)

AV/IT and security monitoring platforms need to interoperate with building systems for centralized alarms and situational awareness, but BMS protocols like BACnet and Modbus do not naturally align with IT and security protocols such as SNMP, REST, or Syslog. Without middleware or defined integration strategies, alarms can be lost or duplicated across platforms. Planning for protocol translation and unified dashboards during design ensures that operators receive consistent, actionable information rather than fragmented alerts.

Sequencing and Commissioning

Many security devices (like cameras, access readers, and sensors) are mounted after walls and ceilings are finished, but they require backboxes, conduit stubs, and power during the rough-in phase. If these provisions are missed, devices cannot be installed without cutting into finished work, driving cost and schedule impacts. Coordination drawings and pre-installation meetings are essential to map these dependencies. During commissioning, integrated system tests should verify not just individual device operation but also end-to-end workflows across AV/IT, security, and MEP systems.

Code and Compliance Coordination

Life safety systems such as fire alarms, egress controls, and smoke management fall under MEP but typically interlock with security. Examples include fail-safe door hardware tied to fire alarm panels or camera views of egress paths required by local codes. If these interlocks are not designed in tandem, projects risk rejection by the Authority Having Jurisdiction (AHJ) or the need for costly last-minute fixes. Early alignment of code requirements across disciplines ensures smoother approvals and a more resilient facility. These coordination choices don't just affect delivery. They also determine whether facilities can credibly meet the rising sustainability expectations that regulators and investors demand.

AV/IT and Security as Sustainability Levers

Sustainability is no longer optional. Regulators, investors, and operators are all pressing for measurable progress on energy, water, and carbon efficiency. Data centers consume roughly 2% of global electricity,[2] (and that percentage is rapidly increasing), and their contribution to greenhouse gases is under increasing scrutiny. AV/IT and security systems directly influence this footprint. Their design determines not only how efficiently facilities operate on Day One but also how easily they scale and report progress over decades.

Design Foundations for Sustainability

Early design decisions set the long-term energy and carbon profile of a facility. Choices about redundancy, device specifications, scalability, and integration with MEP systems all carry sustainability consequences.

- Redundancy calibration: Oversized systems waste energy. Aligning backup requirements for AV/IT and security with actual business risk avoids stranded capacity and unnecessary load.
- Cooling efficiency: AV/IT and security devices add significant heat load. Coordinating device density, rack placement, and cooling strategies ensures that airflow is not compromised and avoids costly rework.
- Scalability through zones: Designing concentric security zones and access levels at the schematic stage supports future growth without ripping out pathways or overtaxing cooling and power systems.
- Lifecycle planning: Cameras, access readers, and servers become e-waste if refresh cycles are not considered in design. Selecting open standards and modular systems extends usable life.
- Telemetry and metrics: AV/IT and security platforms can feed real-time data into PUE, WUE, and carbon accounting dashboards, strengthening accountability to regulators and stakeholders.
- Regulatory context and permitting: Authorities increasingly require proof that designs include credible sustainability measures. Weak strategies can delay or derail permits, especially for facilities designated as mission-critical.

Operational Levers for Carbon Reduction

Beyond design, day-to-day AV/IT and security operations influence ongoing efficiency. Practical measures help facilities meet carbon reduction goals while maintaining resilience.

- Edge processing: Running analytics at the edge reduces the need for backhaul, lowering bandwidth and energy consumption.
- Codec selection and adaptive retention: Video compression formats and tiered storage policies have a material impact on storage and energy profiles. Edge analytics, for example, can reduce storage requirements by as much as 70 percent. Right-sizing retention to risk and compliance requirements prevents over-consumption.
- Virtualization and efficient hardware: Consolidating workloads onto fewer, more efficient platforms reduces both power draw and cooling demand.

[2] https://www.deloitte.com/us/en/insights/industry/technology/technology-media-and-telecom-predictions/2025/genai-power-consumption-creates-need-for-more-sustainable-data-centers.html

- Power policies: Devices can be programmed for low-power states during off-peak hours, cutting unnecessary consumption.
- Continuous monitoring and operational testing: Linking AV/IT and security telemetry to building systems allows operators to track efficiency, flag anomalies, and document reductions. It's important to test under real load conditions to validate efficiency, simulate failover, and confirm that devices perform within planned energy and cooling envelopes.
- Accountability across silos: Sustainability performance often falls between owners, operators, and IT/security teams. Clear accountability for monitoring and reporting ensures that sustainability plans translate into measurable outcomes.

CONCLUSION: DESIGNING FOR DECADES

Data centers have become essential infrastructure for the global economy, but the pace of delivery and growing sustainability expectations demand a different approach to design. AV/IT and security systems are no longer side considerations; they are integral to how a facility performs and demonstrates accountability.

Decisions made in the first phases of design shape outcomes for decades. Early integration of AV/IT and security systems prevents costly retrofits, strengthens resilience under stress, and ensures scalability for future demand. These systems also offer measurable levers for sustainability, whether it be by reducing unnecessary storage and compute loads, aligning data retention with actual needs, or delivering telemetry that feeds directly into energy and carbon reporting.

Organizations that elevate AV/IT and security to core infrastructure gain more than compliance. They also position themselves to avoid costly redesigns, keep systems stable under stress, meet sustainability expectations, and adapt to changing demands.