

KG 450: IT-Infrastruktur in modernen Gebäuden

1. Einordnung im Kontext der TGA

IT-Infrastruktur ist in modernen Gebäuden kein nachgelagerter Ausstattungsbestandteil, sondern ein funktionaler Teil der Technischen Gebäudeausrüstung. Sie umfasst die technische Basis für Übertragung, Verarbeitung, Bereitstellung und Absicherung digitaler Informationen innerhalb eines Gebäudes und an den Schnittstellen zu externen Netzen. Dazu zählen insbesondere strukturierte Verkabelung, Datennetze, Netzverteiler, Serverräume, WLAN-Infrastruktur sowie die technische Einbindung gebäudebezogener digitaler Systeme.

In der Kostensystematik nach DIN 276 ist diese Infrastruktur im Regelfall der Kostengruppe 450 zuzuordnen. Dort werden fernmelde- und informationstechnische Anlagen zusammengefasst, also jene Systeme, deren primäre Funktion in Kommunikation, Datenübertragung, Signalverarbeitung und informationstechnischer Vernetzung liegt. Diese Zuordnung ist für Kostenplanung, Ausschreibung und Verantwortungsabgrenzung wesentlich.

Gegenüber der KG 440 ist eine klare funktionale Trennung erforderlich. Die KG 440 umfasst Starkstromanlagen und damit die elektrische Energieversorgung, Verteilungen, Schutzorgane und Zuleitungen. Die IT-Infrastruktur benötigt diese Energieversorgung, ist jedoch nicht selbst Bestandteil der Stromverteilung. Ebenso ist die Abgrenzung zur KG 480 erforderlich. Gebäudeautomation dient der Mess-, Steuer- und Regelfunktion technischer Anlagen. Sie nutzt häufig Datennetze und IP-basierte Kommunikationswege, ist aber in ihrer Primärfunktion auf Automationsprozesse ausgerichtet, nicht auf die Bereitstellung allgemeiner IT-Infrastruktur.

Für Digitalisierung und Gebäudebetrieb ist IT-Infrastruktur heute grundlegend. Ohne sie lassen sich Kommunikationssysteme, Zutrittskontrolle, Sicherheitsfunktionen, Energieerfassung, Ladeinfrastruktur, digitale Arbeitsplätze und zahlreiche Betreiberprozesse nicht mehr zuverlässig abbilden. In modernen Gebäuden wirkt sie damit als infrastrukturelles Rückgrat zwischen klassischer TGA, Nutzeranforderungen und digitalem Betrieb.

2. Grundbestandteile der IT-Infrastruktur

Der zentrale Baustein der IT-Infrastruktur ist die strukturierte Verkabelung. Sie stellt eine anwendungsneutrale, standardisierte und langfristig nutzbare Übertragungsbasis bereit. Planerisch wird sie hierarchisch aufgebaut, typischerweise mit Hauptverteiler, Etagenverteilern und Anschlussbereichen. Ziel ist eine Infrastruktur, die nicht nur aktuelle Nutzungen unterstützt, sondern auch spätere Umnutzungen, höhere Datenraten und zusätzliche Anwendungen aufnehmen kann.

Datennetze bilden die logische und physische Vernetzung auf dieser Grundlage. Sie verbinden Arbeitsplätze, technische Anlagen, Sicherheitskomponenten und zentrale Systeme. Dabei ist zwischen passiver Infrastruktur und aktiver IT zu unterscheiden. Die passive Infrastruktur umfasst Kabel, Anschlussdosen, Patchfelder, Verteilerschränke und Trassen. Sie ist dauerhaft gebäudebezogen. Aktive Komponenten wie Server, Anwendungen und bestimmte nutzerspezifische Endgeräte sind differenziert zu betrachten und teilweise nicht mehr der allgemeinen Gebäudeinfrastruktur zuzuordnen.

Serverräume nehmen in größeren oder technisch anspruchsvollen Gebäuden eine Sonderrolle ein. Sie dienen der Unterbringung zentraler informationstechnischer Komponenten, Netzwerkverteiler und gegebenenfalls weiterer Systeme zur Datenverarbeitung. Ihre Planung betrifft nicht nur die IT selbst, sondern auch Stromversorgung, Kühlung, Brandschutz, Zutritt und Monitoring.

Verteiler- und Technikräume sind funktional notwendig, um Datennetze geordnet, wartbar und ausbaufähig zu strukturieren. Etagenverteiler, Hauptverteiler und Übergabepunkte zu externen Netzen benötigen definierte Flächen, geeignete Umgebungsbedingungen sowie sichere und dokumentierte Leitungswege. Ihre Lage beeinflusst Leitungslängen, Dämpfung, Brandabschnitte und spätere Erweiterbarkeit.

WLAN-Infrastruktur ist heute in vielen Gebäuden Teil der Regelplanung. Zwar erfolgt die Datenübertragung drahtlos, die technische Voraussetzung bleibt jedoch eine leistungsfähige kabelgebundene Infrastruktur mit Access-Point-Anbindungen, Stromversorgung, Netzwerkmanagement und abgestimmter Funkzellenplanung. Ohne diese Basis entsteht keine belastbare drahtlose Versorgung.

Glasfaseranbindungen gewinnen sowohl innerhalb des Gebäudes als auch an den Übergängen zu externen Netzen an Bedeutung. Sie ermöglichen hohe Übertragungsraten, geringe Dämpfung und hohe elektromagnetische Unempfindlichkeit. Im Backbone-Bereich und bei größeren Distanzen sind sie regelmäßig zweckmäßig.

Schnittstellen zu externen Netzen betreffen Telekommunikationsanschlüsse, Provideranbindungen, Standortvernetzungen und gegebenenfalls redundante Anbindungswege. Diese Übergänge sind technisch und organisatorisch relevant, weil hier Betreiberverantwortung, Verfügbarkeit und Sicherheitsanforderungen zusammenlaufen.

3. Rolle für Gebäudfunktionen

Die Rolle der IT-Infrastruktur erschöpft sich nicht in der Bürokommunikation. Sie verbindet heute eine Vielzahl gebäudetechnischer und betrieblicher Funktionen miteinander. Gerade darin liegt ihre strategische Bedeutung innerhalb der TGA.

Gebäudeautomation benötigt zunehmend IP-basierte Übertragungswege, insbesondere bei verteilten Sensoren, Managementebenen, Visualisierungssystemen und Schnittstellen zu übergeordneten Plattformen. Auch wenn die Automationsfunktion selbst der KG 480 zugeordnet wird, hängt ihre Leistungsfähigkeit wesentlich von einer belastbaren IT-Infrastruktur ab.

Energiemonitoring basiert auf der Erfassung, Übertragung und Auswertung von Betriebsdaten. Zähler, Unterzähler, Messgeräte und Auswertungssysteme benötigen Kommunikationswege, eine geordnete Netzstruktur und sichere Datenübergänge. Ohne eine entsprechende IT-Basis bleibt Energiemonitoring technisch fragmentiert.

Sicherheits- und Überwachungssysteme wie Videoüberwachung, Einbruchmeldetechnik und Alarmmanagement nutzen in hohem Maß digitale Übertragungswege. Die Datenmengen können erheblich sein, insbesondere bei videobasierten Systemen. Daraus folgen Anforderungen an Bandbreite, Speicheranbindung, Redundanz und IT-Sicherheit.

Zutrittskontrolle ist heute regelmäßig netzbasiert organisiert. Türen, Leser, Steuergeräte und Managementsysteme sind vernetzt und müssen in die allgemeine Infrastruktur eingebunden

werden. Die Grenze zwischen klassischer Sicherheitstechnik und IT ist dabei technisch durchlässig, funktional aber weiterhin zu definieren.

Brandmelde- und Sprachalarmanlagen haben zwar spezifische normative Anforderungen und eigenständige sicherheitstechnische Funktionen, benötigen aber ebenfalls Kommunikationsschnittstellen, Übertragungswege und teilweise Integrationen in Managementsysteme. Je komplexer das Gebäude, desto wichtiger wird hier eine saubere technische Koordination.

Smart-Metering und Elektromobilitätsmanagement sind weitere Beispiele für die Verflechtung von TGA und IT-Infrastruktur. Ladepunkte, Lastmanagement, Messdatenübertragung und Auswertungssysteme erfordern durchgängige Kommunikationspfade. Damit wird deutlich, dass IT-Infrastruktur nicht nur Daten transportiert, sondern technische Betriebsfähigkeit organisiert.

4. Stromversorgung und Betriebssicherheit

IT-Infrastruktur ist nur so zuverlässig wie ihre elektrische und thermische Versorgung. Die erforderliche Anschlussleistung ergibt sich aus der Summe der aktiven Netzkomponenten, Servertechnik, Kommunikationssysteme, Sicherheitsanlagen sowie gegebenenfalls dezentraler Technik. Dieser Bedarf steigt mit wachsender Digitalisierung regelmäßig an und muss frühzeitig in die Elektroplanung einfließen.

USV-Systeme sind dort erforderlich, wo kurzzeitige Netzunterbrechungen oder Spannungsqualitätsprobleme nicht tolerierbar sind. Dies betrifft zentrale Netzverteiler, Serverräume, Kommunikationszentralen und sicherheitsrelevante Systeme. Die USV übernimmt dabei nicht dieselbe Funktion wie eine Ersatzstromversorgung. Sie überbrückt kurzfristige Ausfälle, stabilisiert Versorgungsspannungen und ermöglicht kontrollierte Umschaltungen oder definierte Abschaltvorgänge.

Ersatzstromversorgung ist notwendig, wenn kritische digitale Funktionen über längere Netzausfälle hinweg verfügbar bleiben müssen. Ob dies erforderlich ist, ergibt sich aus dem Betriebs- und Sicherheitskonzept des Gebäudes. Bei Leitstellen, Gesundheitsbauten, sicherheitskritischen Infrastrukturen oder hochvernetzten Betriebsgebäuden ist die Anforderung regelmäßig höher als in Standardnutzungen.

Redundanzkonzepte betreffen nicht nur die elektrische Einspeisung, sondern ebenso Netzwege, Verteilerebenen, Serverstandorte, Provideranschlüsse und Kühlung. Technisch sinnvoll ist Redundanz nur dann, wenn sie konsequent über alle kritischen Glieder einer Kette betrachtet wird. Eine einzelne doppelte Einspeisung beseitigt keine systemischen Ausfallpunkte.

Erdungs- und Potentialausgleich sind für die elektromagnetische Verträglichkeit und Betriebssicherheit der IT-Infrastruktur unverzichtbar. Hohe Datenraten, empfindliche Elektronik und Mischumgebungen mit Starkstrom-, Automations- und IT-Systemen erfordern einen sorgfältig geplanten Potentialausgleich. Störungen in diesem Bereich wirken sich häufig diffus aus und sind später nur mit erheblichem Aufwand zu lokalisieren.

Die Klimatisierung von Serverräumen ist eine unmittelbare Schnittstelle zur KG 434. Da elektrische Leistung nahezu vollständig in Wärme umgesetzt wird, muss die Kälteversorgung auf reale Lasten, Ausfallstrategien und Ausbaureserven abgestimmt werden. Betriebssicherheit ist daher nie nur eine Frage der IT, sondern immer das Ergebnis koordinierter Planung zwischen KG 450, KG 440 und KG 434.

5. Technische Anforderungen und Normen

Die technische Planung der IT-Infrastruktur basiert auf normativen und sicherheitstechnischen Anforderungen. Für die strukturierte Verkabelung ist die DIN EN 50173 von zentraler Bedeutung. Sie definiert Grundprinzipien, Übertragungsklassen, Verkabelungsstrukturen und Leistungsparameter für anwendungsneutrale Kommunikationskabelanlagen. Sie schafft damit die Grundlage für eine normgerechte und zukunftsfähige Infrastruktur.

Ergänzend sind einschlägige DIN VDE-Vorschriften zu berücksichtigen. Diese betreffen insbesondere elektrische Sicherheit, Installation, Schutzmaßnahmen, Potentialausgleich, Trennungsabstände, Leitungsführung und Prüfanforderungen. Gerade an den Schnittstellen von Stromversorgung und Informationstechnik ist ihre Einhaltung wesentlich.

Anforderungen an IT-Sicherheit betreffen Netztrennung, Zugriffsrechte, Redundanz, Schutz gegen unbefugte Zugriffe, Fernwartungsbedingungen und Ausfallsicherheit. Sie sind nicht nur organisatorische Vorgaben, sondern beeinflussen die technische Architektur unmittelbar. Segmentierung, abgesicherte Übergabepunkte und definierte Betreiberzuständigkeiten sind planerisch vorzusehen.

Datenschutzanforderungen spielen überall dort eine Rolle, wo personenbezogene Daten verarbeitet oder übertragen werden, etwa in Zutrittskontrollsystemen, Videoüberwachung, Zeiterfassung oder nutzerbezogenen Betriebsdaten. Daraus ergeben sich Anforderungen an Zugriffsschutz, Protokollierung, Speicherorte und technische Schutzmaßnahmen.

Brandschutzanforderungen betreffen Trassenführung, Brandabschnitte, Kabelabschottungen, Funktionserhalt, Raumabschlüsse und gegebenenfalls Löschkonzepte für Server- oder Technikräume. Die IT-Infrastruktur ist daher nicht isoliert planbar, sondern in das Brandschutzkonzept einzubinden.

6. Wirtschaftliche und strategische Bedeutung

Die wirtschaftliche Bedeutung der IT-Infrastruktur liegt in ihrer langen Nutzungsdauer und ihrer hohen Folgewirkung. Fehler oder Unterdimensionierungen in frühen Planungsphasen verursachen häufig deutlich höhere Kosten im Betrieb und bei späteren Anpassungen als eine angemessen dimensionierte Erstinvestition.

Investitionssicherheit entsteht durch normgerechte, dokumentierte und ausbaufähige Infrastrukturen. Skalierbarkeit bedeutet, dass zusätzliche Nutzer, höhere Bandbreiten oder neue digitale Anwendungen ohne grundlegende Umbaumaßnahmen aufgenommen werden können. Zukunftsfähigkeit ist damit keine abstrakte Eigenschaft, sondern das Ergebnis konkreter Reserve- und Strukturentscheidungen.

Bei Nutzungsänderungen zeigt sich die Qualität der IT-Infrastruktur besonders deutlich. Gebäude mit flexibler Verkabelung, ausreichenden Verteilerflächen und geordneten Netzstrukturen lassen sich wesentlich wirtschaftlicher anpassen als Gebäude mit punktuellen Insellösungen.

Lebenszykluskosten umfassen nicht nur Investitionen, sondern auch Betrieb, Wartung, Modernisierung, Energiebedarf, Ausfallrisiken und Dokumentationsaufwand. Betriebskosten entstehen beispielsweise durch aktive Netzkomponenten, Kühlung, USV, Wartung und regelmäßige Anpassungen. Eine klare Abgrenzung zwischen Investitions- und Folgekosten ist daher erforderlich, um wirtschaftliche Entscheidungen nicht auf eine verkürzte Erstkostenbetrachtung zu reduzieren.

7. Neubau vs. Bestand

Im Neubau lässt sich IT-Infrastruktur integrativ planen. Technikräume, Trassen, Vertikalerschließungen, Kühlkonzepte, Redundanzwege und Schnittstellen zu anderen Gewerken können von Beginn an koordiniert werden. Dadurch entstehen belastbare und wirtschaftliche Gesamtlösungen.

Im Bestand ist die Nachrüstung häufig anspruchsvoller. Vorhandene Trassen sind belegt, Raumreserven fehlen, Dokumentationen sind unvollständig und die vorhandene Strom- oder Kälteinfrastruktur entspricht nicht mehr dem heutigen Bedarf. Modernisierung bestehender Netze ist deshalb regelmäßig mehr als ein Austausch einzelner Leitungen.

Leistungsreserven spielen im Bestand eine besondere Rolle. Wo frühere Systeme nur auf klassische Bürokommunikation ausgelegt waren, treffen heute deutlich höhere Datenmengen, WLAN-Dichte, Sicherheitsanforderungen und digitale Betriebsprozesse auf begrenzte Strukturen. Die wirtschaftliche Bewertung muss daher auch Umbauaufwand, Betriebsunterbrechungen und Restrisiken berücksichtigen.

8. Typische Praxisfragen

Gehört IT-Infrastruktur zur TGA oder zur IT-Abteilung?

Gebäudebezogene IT-Infrastruktur ist technisch Teil der TGA, insbesondere im Bereich der passiven Infrastruktur und gebäudefesten Vernetzung. Die operative Nutzung und Administration aktiver IT-Systeme liegt häufig beim Betreiber oder dessen IT-Organisation. Entscheidend ist die funktionale Abgrenzung.

Welche Redundanz ist technisch sinnvoll?

Redundanz ist aus der Kritikalität der Nutzung abzuleiten. Für Standardnutzungen genügt häufig eine einfache Auslegung mit begrenzten Reserven. Für kritische Betriebsfunktionen sind getrennte Wege, doppelte Anschlüsse, USV und gegebenenfalls redundante Anbindungen technisch geboten.

Wie beeinflusst IT-Infrastruktur die Anschlussleistung?

Jede aktive IT-Komponente benötigt elektrische Leistung und erzeugt zugleich Wärme. Mit wachsender Digitalisierung steigen daher sowohl Anschlussleistung als auch Kühllast. Dies betrifft insbesondere Serverräume, Netzverteiler, Sicherheitszentralen und WLAN-Infrastrukturen.

Wann ist ein Serverraum erforderlich?

Ein Serverraum ist erforderlich, wenn zentrale informationstechnische Funktionen, erhöhte Verfügbarkeitsanforderungen, Datenschutz, Rackdichten oder mehrere Netz- und Systemkomponenten räumlich gebündelt werden müssen. Kleine Gebäude kommen teils mit Technikschränken oder Verteilerräumen aus, größere oder kritische Gebäude regelmäßig nicht.

Welche Rolle spielt Glasfaser im Gebäude?

Glasfaser ist für Backbone-Strukturen, hohe Bandbreiten, große Distanzen und elektromagnetisch anspruchsvolle Umgebungen wesentlich. Sie erhöht Leistungsfähigkeit und Zukunftssicherheit und ist in modernen Gebäuden vielfach Standard im Hauptnetz.

Welche Haftungsrisiken bestehen bei unzureichender Planung?

Unzureichende Planung führt zu Fehlfunktionen, Ausfällen, Nachrüstungen, Terminverzug, Mehrkosten und unklaren Verantwortlichkeiten. In sicherheitsrelevanten oder betriebskritischen Anwendungen können daraus erhebliche haftungsrechtliche Folgen entstehen.

9. Schnittstellen in der integralen Planung

Die Abstimmung mit der Architektur betrifft Flächenbedarfe, Technikräume, Trassenführung, Zugänglichkeit und brandschutztechnische Einbindung. Ohne architektonische Berücksichtigung bleiben informationstechnische Konzepte häufig theoretisch.

Die Koordination mit der Elektrotechnik ist bei Stromversorgung, USV, Erdung, Potentialausgleich und Schutzmaßnahmen zwingend. Die Integration in die Gebäudeautomation betrifft Monitoring, Zustandsmeldungen und systemübergreifende Visualisierung.

Das Brandschutzkonzept beeinflusst die IT-Infrastruktur durch Raumabschlüsse, Leitungsführung, Funktionserhalt und Abschottung. Dokumentationsanforderungen betreffen Bestandspläne, Verteilerzuordnungen, Leitungswege, Kennzeichnungen, Prüfprotokolle und Schnittstellenbeschreibungen. Ohne belastbare Dokumentation ist weder ein sicherer Betrieb noch eine wirtschaftliche Erweiterung möglich.

10. Technisches Fazit

IT-Infrastruktur ist das technische Rückgrat moderner Gebäude. Sie verbindet Kommunikationssysteme, Sicherheitstechnik, Automationsfunktionen, Energiemanagement und betriebliche Prozesse zu einer funktionsfähigen Gesamtstruktur. Ihre Bedeutung liegt nicht allein in der Datenübertragung, sondern in der Sicherstellung digitaler Betriebsfähigkeit.

Für Betriebssicherheit und Effizienz ist eine klare Abgrenzung zu Stromversorgung, Gebäudeautomation und nutzerspezifischer IT erforderlich. Zugleich zeigt die Praxis, dass diese Abgrenzung nur im Rahmen integraler Planung belastbar funktioniert. Digitalisierung und TGA wachsen technisch zusammen, auch wenn ihre Kostengruppen und Primärfunktionen differenziert bleiben.

Frühzeitige integrale Planung ist daher keine organisatorische Zusatzleistung, sondern technische Voraussetzung für wirtschaftliche, sichere und anpassungsfähige Gebäudeinfrastruktur.

11. Abschlusshinweis

Als TGA-Ingenieurbüro mit Sitz in Köln begleitet MT Ingenieure Projekte von der Grundlagenermittlung bis zur Ausführungsplanung über alle Gewerke hinweg.