KG 450: Zukunftsfähigkeit der IT-Infrastruktur

1. Einordnung der Zukunftsfähigkeit im Kontext der TGA

Zukunftsfähigkeit bei IT-Infrastruktur bedeutet im Gebäudekontext, dass technische Systeme nicht nur den aktuellen Bedarf erfüllen, sondern auch auf steigende Datenmengen, veränderte Nutzungen, neue Kommunikationsstandards, höhere Verfügbarkeitsanforderungen und wachsende Sicherheitsanforderungen vorbereitet sind. Gemeint ist damit keine abstrakte Innovationsfähigkeit, sondern die konkrete technische, organisatorische und wirtschaftliche Eignung einer Infrastruktur, über einen langen Lebenszyklus hinweg anpassbar und betriebssicher zu bleiben.

Innerhalb der Kostensystematik nach DIN 276 ist die gebäudebezogene IT-Infrastruktur regelmäßig der Kostengruppe 450 zuzuordnen. Hierzu zählen insbesondere strukturierte Verkabelung, Datenverteilernetze, Kommunikationsinfrastruktur, Netzverteiler, Server- und Technikräume sowie weitere fernmelde- und informationstechnische Anlagen. Diese Zuordnung ist für Kostenplanung, Ausschreibung und Verantwortungsabgrenzung wesentlich, weil Zukunftsfähigkeit nicht nur eine technische, sondern auch eine investive und vertragliche Fragestellung ist.

Zu den wichtigsten Schnittstellen gehört die KG 440. Eine IT-Infrastruktur ist nur dann langfristig belastbar, wenn Stromversorgung, Unterverteilungen, Schutzkonzepte, USV-Anbindungen, Erdung und Potentialausgleich von Beginn an auf steigende IT-Lasten vorbereitet werden. Ebenso besteht eine enge Verbindung zur KG 480. Gebäudeautomation, Energiemonitoring, Zutrittskontrolle und viele Smart-Building-Funktionen nutzen IP-basierte Übertragungswege und sind damit auf eine leistungsfähige informationstechnische Basis angewiesen.

Der Zusammenhang mit Digitalisierung und Smart Building ist unmittelbar. Mit wachsender digitaler Gebäudenutzung steigen die Anforderungen an Bandbreite, Verfügbarkeit, Datenqualität und Schnittstellenoffenheit. Zukunftsfähige IT-Infrastruktur ist daher nicht ergänzende Komforttechnik, sondern Bestandteil der Grundfunktion moderner Gebäude.

2. Skalierbarkeit der Netzwerkinfrastruktur

Die technische Grundlage für Skalierbarkeit ist eine strukturierte Verkabelung mit Leistungsreserven. Ziel ist eine Infrastruktur, die nicht nur heutige Anwendungen wie Bürokommunikation und WLAN trägt, sondern auch spätere Anforderungen aus Gebäudeautomation, Sicherheitstechnik, Medienversorgung, Smart Metering und datenintensiven Betriebsprozessen. Die Planung darf sich deshalb nicht allein an der Erstnutzung orientieren.

Ein zentrales Element ist der Glasfaser-Backbone. Während im Horizontalbereich weiterhin kupferbasierte Lösungen wirtschaftlich und technisch sinnvoll sein können, ist im Primär- und Sekundärbereich Glasfaser regelmäßig die robustere Wahl. Sie bietet hohe Bandbreiten, große Reichweiten, geringe elektromagnetische Empfindlichkeit und ausreichende Reserven für spätere Kapazitätssteigerungen. Für größere Liegenschaften oder technisch anspruchsvolle

Gebäude ist ein glasfaserbasierter Backbone daher ein wesentlicher Baustein der Zukunftsfähigkeit.

Modulare Verteilersysteme erhöhen die Anpassungsfähigkeit. Hauptverteiler, Etagenverteiler und Netzwerkschränke sollten so geplant werden, dass zusätzliche Patchfelder, Glasfaserabschlüsse, Rangierkapazitäten und aktive Komponenten nachgerüstet werden können, ohne dass die Grundstruktur verändert werden muss. Das betrifft nicht nur die Zahl der Höheneinheiten, sondern auch Tiefe, Kabelführung, Belüftung und Zugänglichkeit.

Reservekapazitäten in Kabeltrassen sind ein weiterer Kernpunkt. Eine auf den Erstbedarf dimensionierte Trassenplanung führt in der Praxis schnell zu Engpässen. Nachinstallationen werden dann baulich aufwendig, störanfällig und kostenintensiv. Zukunftsfähige Planung sieht daher freie Querschnitte, zusätzliche Leitungswege, Reserveschächte und ausreichend dimensionierte Durchdringungen vor. Gleiches gilt für Steigzonen und Trassen in Technikzentralen.

Auch Server- und Technikräume müssen erweiterbar geplant werden. Entscheidend sind nicht nur die aktuelle Rack-Anzahl, sondern Erweiterungsflächen, Kühl- und Stromreserven, Zugangssituationen sowie die Möglichkeit, zusätzliche Verteiler- oder Sicherheitstechnik aufzunehmen. Wer diese Räume ausschließlich auf den momentanen Bedarf auslegt, erzeugt frühzeitig strukturelle Grenzen.

Technisch bedeutet Skalierbarkeit somit: standardisierte Netzstruktur, leistungsfähiger Backbone, modulare Verteiler, freie Trassenreserven und ausbaufähige Technikflächen. Ohne diese Grundsätze bleibt Zukunftsfähigkeit auf organisatorische Improvisation beschränkt.

3. Leistungs- und Energieplanung mit Reserven

Zukunftsfähigkeit der IT-Infrastruktur setzt eine Elektroplanung voraus, die mit Lastzuwächsen rechnen kann. Die Dimensionierung der Anschlussleistung darf sich nicht allein an der aktuellen Ausstattung orientieren, sondern muss spätere Verdichtung, zusätzliche aktive Netzkomponenten, Servertechnik, Sicherheitsanlagen und Kommunikationssysteme berücksichtigen. Je stärker ein Gebäude digitalisiert wird, desto enger wird die Verbindung zwischen IT-Last und elektrotechnischer Grundauslegung.

Reserven in Unterverteilungen sind deshalb technisch sinnvoll. Erforderlich sind freie Abgänge, Reserveplätze, ausreichend dimensionierte Sammelschienen, Platz für nachrüstbare Schalt- und Schutzgeräte sowie klare Trennungen zwischen allgemeinen Stromkreisen und kritischen IT-Versorgungen. Werden Unterverteilungen ohne Ausbaureserven konzipiert, sind spätere Anpassungen mit erheblichem Eingriff in den laufenden Betrieb verbunden.

USV-Reserven sind besonders für zentrale Netz- und Serverstrukturen relevant. Eine USV muss nicht nur den Erstbedarf tragen, sondern auch absehbare Laststeigerungen und Reservezeiten berücksichtigen. Zu knapp ausgelegte Anlagen sind zwar investiv günstiger, verlieren aber mit jeder Erweiterung an Betriebswert. Zukunftsfähige Planung verlangt daher eine nachvollziehbare Lastbilanz mit Zuschlägen für Wachstum, Umschaltstrategien und gegebenenfalls zusätzliche Kommunikations- oder Sicherheitsfunktionen.

Redundanzkonzepte wie N+1 oder 2N sind nicht pauschal erforderlich, aber dort geboten, wo Ausfallfolgen erheblich sind. Die technische Bewertung hängt von der Kritikalität der Nutzung ab. Ein Verwaltungsgebäude mit allgemeiner Büronutzung stellt andere Anforderungen als ein Gesundheitsbau, ein Rechenzentrumsbereich oder ein Leitstand. Zukunftsfähigkeit bedeutet hier, Redundanz nicht nachträglich improvisieren zu müssen, sondern Trassen, Flächen, Einspeisepunkte und Schaltanlagen so vorzubereiten, dass spätere Erhöhungen des Verfügbarkeitsniveaus möglich bleiben.

Ersatzstromfähigkeit ist ebenfalls frühzeitig zu bewerten. Wo kritische IT-Funktionen über längere Stromausfälle hinweg betrieben werden müssen, reicht eine reine USV-Versorgung nicht aus. Dann ist zu prüfen, ob Ersatzstrom vorgesehen werden muss und welche Systemteile daran anzuschließen sind. Diese Entscheidung betrifft nicht nur die Elektrotechnik, sondern auch die IT-Architektur und das Betriebskonzept.

Der Zusammenhang zwischen IT-Last und Elektroplanung ist damit direkt. Digitale Gebäudefunktion erhöht elektrische Lasten, verschärft Anforderungen an Verfügbarkeit und macht Reserven zum integralen Bestandteil der Energieplanung.

4. Thermische und bauliche Vorsorge

Mit steigender IT-Leistungsdichte steigt die thermische Belastung. Nahezu jede zusätzlich aufgenommene elektrische Leistung wird als Wärme an den Raum abgegeben. Zukunftsfähige IT-Infrastruktur setzt daher voraus, dass bereits in frühen Planungsphasen steigende Leistungsdichten berücksichtigt werden. Dies betrifft insbesondere Serverräume, Technikräume, Netzwerkschränke und lokal verdichtete aktive Infrastruktur.

Kühllastreserven sind deshalb kein Komfortmerkmal, sondern betriebliche Vorsorge. Werden Räume nur auf die initiale Ausstattung dimensioniert, entstehen bei späteren Erweiterungen lokale Überhitzung, vorzeitige Alterung von Komponenten und ungeplante Nachrüstkosten. Die Kühllastberechnung muss daher Erweiterungsszenarien, Reserveflächen und den möglichen Austausch gegen leistungsdichtere IT-Komponenten berücksichtigen.

Flexible Klimatisierungskonzepte sind solchen starren Lösungen überlegen, die nur auf einen einzigen Ausbaustand ausgelegt sind. Erforderlich sind Systeme, die sich in Teillasten stabil betreiben lassen, aber zugleich spätere Laststeigerungen aufnehmen können. Dazu zählen zonierte Kühlung, modulare Gerätekonzepte, nachrüstbare Kühlregister oder reservierte Aufstellflächen. Dabei ist nicht die maximale Technikdichte in jedem Fall wirtschaftlich, wohl aber die Fähigkeit, Lasten schrittweise erhöhen zu können.

Raumhöhen, Doppelböden und Kühlzonen haben unmittelbaren Einfluss auf die Zukunftsfähigkeit. Ausreichende Raumhöhen erleichtern Kabelführung, Luftführung und spätere Nachrüstung. Doppelböden können je nach Nutzung vorteilhaft sein, insbesondere wenn Luftführung, Stromversorgung und Dateninfrastruktur flexibel geführt werden sollen. Kühlzonen oder definierte Warm- und Kaltbereiche verbessern die Beherrschbarkeit höherer Lasten. Diese Aspekte sind früh architektonisch zu berücksichtigen, weil sie später nur mit hohem Aufwand veränderbar sind.

Auch Brandschutzreserven sind erforderlich. Zusätzliche Leitungswege, Nachbelegungen in Trassen und spätere Durchdringungen dürfen nicht dazu führen, dass Brandabschnitte unkontrolliert geschwächt werden. Zukunftsfähigkeit bedeutet daher auch, brandschutztechnisch geordnete Reserven in Schächten, Abschottungen und Technikräumen vorzusehen.

Die Schnittstelle zur Kälte- und Lüftungsplanung ist damit offensichtlich. Eine zukunftsfähige IT-Infrastruktur kann nicht isoliert durch Daten- und Elektroplanung entstehen, sondern nur im Zusammenspiel mit thermischer und baulicher Vorsorge.

5. Technologische Offenheit

Technologische Offenheit ist eine wesentliche Voraussetzung langfristiger Nutzbarkeit. Gemeint ist die Fähigkeit einer Infrastruktur, unterschiedliche Anwendungen, Protokolle und Systementwicklungen aufzunehmen, ohne bei jeder Veränderung grundlegende Teile ersetzen zu müssen. Dies beginnt bei standardisierten Schnittstellen und setzt sich in der Wahl offener Kommunikationsarchitekturen fort.

IP-basierte Systeme spielen hierbei eine zentrale Rolle. Sie erleichtern die Integration unterschiedlicher Anwendungen in ein gemeinsames Übertragungsnetz und schaffen eine einheitliche Grundlage für Kommunikation, Management und Monitoring. Dies bedeutet nicht, dass alle Systeme vereinheitlicht werden müssen, wohl aber, dass proprietäre Sonderwege möglichst vermieden werden sollten, wenn keine zwingenden fachlichen Gründe dagegen sprechen.

Interoperabilität ist aus planerischer Sicht höher zu bewerten als kurzfristige Funktionsvorteile einzelner Insellösungen. Systeme, die sich nur untereinander oder nur mit spezifischen Zusatzkomponenten verbinden lassen, schränken Erweiterbarkeit und Betreiberfreiheit ein. Zukunftsfähigkeit verlangt deshalb technische Lösungen, die dokumentierbar, integrierbar und mit vertretbarem Aufwand austauschbar bleiben.

Die Vermeidung proprietärer Insellösungen ist auch wirtschaftlich relevant. Je enger ein Gebäude an einzelne herstellerspezifische Architekturen gebunden wird, desto größer werden Abhängigkeiten im Betrieb, bei Ersatzbeschaffung und bei späteren Erweiterungen. Technisch ist deshalb zu bevorzugen, was standardisiert, nachvollziehbar und in bestehende Infrastrukturkonzepte integrierbar ist.

Update- und Erweiterungsfähigkeit betrifft nicht nur Software, sondern auch physische Infrastruktur. Netzverteiler, Glasfaserreserven, zusätzliche Ports, modulare Spannungsversorgung und erweiterbare Kühlkonzepte sind Ausdruck technologischer Offenheit auf Hardware-Ebene. Aus technischer Sicht ist daher nicht die starre Vollausstattung entscheidend, sondern die Fähigkeit, Systeme geordnet weiterzuentwickeln.

6. Cyber-Sicherheit und Betriebssicherheit

Zukunftsfähige IT-Infrastruktur muss nicht nur leistungsfähig, sondern auch sicher und beherrschbar sein. Netzwerksegmentierung ist hierfür ein Grundprinzip. Kritische Gebäudefunktionen, Nutzerkommunikation, Sicherheitsanlagen und betriebliche Managementsysteme sollten nicht unstrukturiert in einem gemeinsamen Netz geführt werden.

Segmentierung reduziert Störungsreichweiten, erschwert unbefugte Zugriffe und vereinfacht die betriebliche Kontrolle.

Zugriffskontrolle betrifft sowohl die logische als auch die physische Ebene. Serverräume, Netzverteiler und Schnittstellen zu externen Netzen müssen gegen unberechtigten Zugriff geschützt werden. Parallel dazu sind Rollen- und Rechtekonzepte erforderlich, damit Änderungen, Wartung und Fernzugriffe nachvollziehbar und begrenzt bleiben. Betriebssicherheit ist ohne geregelte Zugriffshoheit nicht erreichbar.

Monitoring ist ein weiteres Schlüsselelement. Zukunftsfähigkeit bedeutet, Zustände frühzeitig erkennen zu können. Dazu gehören Lastentwicklungen, Temperaturverläufe, Portbelegungen, Verfügbarkeitsmeldungen, Spannungszustände, Kommunikationsausfälle und sicherheitsrelevante Ereignisse. Ohne Monitoring wird eine Infrastruktur erst dann sichtbar, wenn sie bereits gestört ist.

Redundante Kommunikationswege sind dort erforderlich, wo Gebäudefunktionen von der Verfügbarkeit digitaler Netze abhängen. Dies kann interne Backbone-Strecken, Provideranbindungen oder Verbindungen zwischen Technikzentralen betreffen. Redundanz ist dabei nicht Selbstzweck, sondern Mittel zur Begrenzung von Ausfallfolgen.

Dokumentation und Wartung sind organisatorische Voraussetzungen technischer Betriebssicherheit. Eine Infrastruktur ist nur dann langfristig beherrschbar, wenn Leitungswege, Verteiler, Patchbeziehungen, Schutzkonzepte, Softwarestände, IP-Strukturen und Schnittstellen eindeutig dokumentiert sind. Fehlende Dokumentation ist in der Praxis eine der häufigsten Ursachen für Störungen, Fehlersuche mit hohem Aufwand und unsichere Erweiterungen.

Der Zusammenhang zwischen IT-Sicherheit und Gebäudefunktion ist inzwischen unmittelbar. Fällt die IT-Infrastruktur aus oder wird sie kompromittiert, sind häufig nicht nur Kommunikationsdienste betroffen, sondern auch Zutritt, Überwachung, Automationsfunktionen, Energiemonitoring und betriebliche Steuerungsprozesse.

7. Wirtschaftliche Betrachtung

Zukunftsfähigkeit ist wirtschaftlich nur sinnvoll, wenn Reservekapazitäten begründet und gezielt eingesetzt werden. Maßstab ist die Lebenszyklusbetrachtung. Eine Infrastruktur mit zu geringen Reserven ist in der Erstinvestition günstiger, verursacht jedoch häufig hohe Nachrüstkosten, Betriebsunterbrechungen und verkürzte Nutzungszyklen. Umgekehrt kann eine unbegründete Vollausstattung zu unnötiger Kapitalbindung führen.

Investitionssicherheit entsteht durch technische Entscheidungen, die spätere Nutzungsänderungen mit vertretbarem Aufwand zulassen. Dies betrifft insbesondere Trassenreserven, modulare Verteiler, leistungsfähige Backbone-Strukturen, Reserveflächen in Technikräumen und ausreichend dimensionierte Energie- und Kälteinfrastruktur.

Die Vermeidung späterer Nachrüstkosten ist ein zentrales Argument für strategische Reserven. Nachträglich eingezogene Trassen, erweiterte Stromverteilungen oder umgebaute Serverräume sind in Bestandsgebäuden regelmäßig erheblich teurer als eine vorausschauende Erstplanung. Wirtschaftlich ist daher nicht nur der Anschaffungspreis zu betrachten, sondern der Aufwand über den gesamten Nutzungszeitraum.

Anpassungsfähigkeit bei Nutzungsänderungen erhöht den Gebäudewert. Gebäude, deren IT-Infrastruktur flexibel auf neue Mieter, andere Arbeitsplatzkonzepte, höhere Sicherheitsanforderungen oder datenintensive Anwendungen reagieren kann, lassen sich langfristig wirtschaftlicher betreiben und vermarkten.

Die wirtschaftliche Bewertung von Reservekapazitäten erfordert jedoch Maß und Ziel. Zukunftsfähigkeit bedeutet nicht pauschale Überdimensionierung, sondern eine strategisch begründete Reserve. Technisch sinnvoll sind Reserven dort, wo spätere Erweiterung wahrscheinlich, betriebskritisch oder im Nachgang besonders teuer wäre.

8. Neubau vs. Bestand

Im Neubau kann Zukunftsfähigkeit integrativ geplant werden. Architektur, Elektrotechnik, IT-Infrastruktur, Kälte, Lüftung, Brandschutz und Gebäudeautomation lassen sich von Beginn an aufeinander abstimmen. Trassen, Schächte, Technikräume, Kühlzonen und Redundanzwege können geordnet vorgesehen werden. Das ist der wirtschaftlich und technisch günstigste Fall.

Im Bestand besteht die Herausforderung darin, bestehende Infrastruktur zu modernisieren, ohne den laufenden Betrieb unverhältnismäßig zu beeinträchtigen. Häufig fehlen freie Trassen, dokumentierte Reserven, zusätzliche Stromkapazitäten oder geeignete Technikflächen. Deshalb sind schrittweise Erweiterungen oft der einzig praktikable Weg. Voraussetzung ist eine saubere Bestandsaufnahme.

Wirtschaftliche und technische Grenzen müssen dabei offen benannt werden. Nicht jede Altstruktur lässt sich auf heutiges Niveau anheben. Manchmal ist eine Teilmodernisierung ausreichend, in anderen Fällen ist eine grundlegende Neuordnung wirtschaftlich sinnvoller als fortgesetzte Nachrüstung im Bestand.

9. Typische Praxisfragen

Welche Reserven sind technisch sinnvoll?

Sinnvoll sind Reserven bei Trassen, Verteilerkapazitäten, Anschlussleistung, USV-Auslegung, Kühllast, Glasfaserfasern und Technikflächen. Die Größenordnung richtet sich nach Nutzung, Erweiterungswahrscheinlichkeit und Nachrüstaufwand.

Wie wird Skalierbarkeit konkret geplant?

Durch hierarchische Netzstruktur, modulare Verteiler, freie Trassenquerschnitte, ausbaufähige Technikräume und definierte Reserveanschlüsse in Strom- und Datennetzen. Skalierbarkeit ist eine planerische Strukturentscheidung, keine spätere Zusatzmaßnahme.

Wann ist Glasfaser im Gebäude erforderlich?

Glasfaser ist insbesondere im Backbone, bei größeren Distanzen, hohen Bandbreiten, elektromagnetisch sensiblen Umgebungen und bei erhöhten Zukunftsanforderungen erforderlich oder technisch zweckmäßig.

Welche Rolle spielt Redundanz?

Redundanz erhöht Verfügbarkeit und begrenzt Ausfallfolgen. Sie ist vor allem bei kritischen Gebäudefunktionen, zentralen Serverstrukturen, wichtigen Kommunikationswegen und sicherheitsrelevanten Anwendungen erforderlich.

Wie wird die Stromversorgung langfristig abgesichert?

Durch realistische Lastprognosen, Reserven in Verteilungen, abgestufte USV- und Ersatzstromkonzepte, sauberen Potentialausgleich sowie vorbereitete Erweiterungsoptionen für zusätzliche Verbraucher und höhere Leistungsdichten.

Welche Haftungsrisiken bestehen bei unzureichender Vorsorge?

Unzureichende Vorsorge kann zu Ausfällen, Nachrüstzwängen, Terminverzug, Mehrkosten und Funktionsmängeln führen. Bei sicherheits- oder betriebsrelevanten Anwendungen entstehen daraus erhebliche technische und vertragliche Haftungsrisiken.

10. Typische Planungsfehler

Ein häufiger Fehler ist die Unterschätzung zukünftiger Bandbreiten. Wird die Infrastruktur ausschließlich für den aktuellen Bedarf ausgelegt, fehlen später Reserven für datenintensive Anwendungen, zusätzliche WLAN-Dichte oder netzbasierte Gebäudefunktionen.

Ebenso kritisch sind fehlende Leistungsreserven in Stromversorgung und USV. Solche Defizite bleiben oft lange unbemerkt und treten erst bei Erweiterungen oder Lastspitzen zutage. Die Folge sind teure Umbauten im Betrieb.

Unzureichende Klimatisierung ist ein klassischer Fehler bei Server- und Technikräumen. Steigende Leistungsdichten werden häufig unterschätzt, sodass Erweiterungen thermisch nicht mehr beherrschbar sind.

Nicht abgestimmte Schnittstellen zwischen IT, Elektrotechnik, Kälte, Brandschutz und Gebäudeautomation führen zu funktionalen Lücken, unklaren Verantwortlichkeiten und ineffizienten Nachbesserungen. Besonders problematisch ist dies bei Technikräumen und zentralen Verteilerstrukturen.

Kurzfristige Kostenoptimierung ohne Lebenszyklusbetrachtung ist wirtschaftlich regelmäßig nachteilig. Werden Reserven konsequent herausoptimiert, verschieben sich Kosten lediglich in spätere Projektphasen oder in den Betrieb, dann meist unter ungünstigeren Randbedingungen.

11. Technisches Fazit

Die Zukunftsfähigkeit der IT-Infrastruktur wird nicht durch einzelne Hochleistungs-Komponenten sichergestellt, sondern durch eine vorausschauende Gesamtplanung. Maßgeblich sind skalierbare Netzstrukturen, Leistungs- und Kältereserven, technologische Offenheit, klare Schnittstellen sowie geordnete Sicherheits- und Betriebskonzepte.

Frühzeitige integrale Planung ist dafür zwingend. IT-Infrastruktur, Elektrotechnik, Gebäudeautomation, Kälte, Lüftung, Brandschutz und Architektur wirken unmittelbar zusammen. Werden diese Zusammenhänge erst spät betrachtet, entstehen strukturelle Defizite, die später nur mit hohem Aufwand korrigiert werden können.

Skalierbarkeit und Redundanz sind dabei keine optionalen Komfortmerkmale, sondern zentrale Parameter für langfristige Gebäudefunktion. Je stärker Gebäude digitalisiert und technisch vernetzt sind, desto unmittelbarer wird der Zusammenhang zwischen IT-Infrastruktur und Betriebsfähigkeit.

Langfristige strategische Planung bedeutet deshalb, Reserven technisch begründet vorzusehen, Schnittstellen offen und standardisiert zu halten und den gesamten Lebenszyklus der Infrastruktur in die Entscheidung einzubeziehen.

Hinweis:

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