Leitfaden Cybersicherheit in der Gebäudeautomation

BIG-EU
WG-FM 100
Version 01

Stand 09/24

Die BACnet Interest Group Europe (BIG-EU) ist ein Anwender- und Industrieverband, der den erfolgreichen Einsatz des BACnet-Protokolls in der Gebäudeautomation (GA) durch Interoperabilitätstests, Fortbildungsprogramme und Werbeaktivitäten in Europa fördert.

Die BIG-EU wurde am 14. Mai 1998 in Frankfurt am Main von zunächst 17 Mitgliedsfirmen gegründet. Heute hat die BIG-EU über 120 Mitglieder aus ganz Europa sowie Australien und Nordamerika.

Der BACnet-Standard wurde von der ASHRAE (American Society of Heating, Refrigeration and Air-Conditioning Engineers) entwickelt, aktuell gepflegt und öffentlich zugänglich gemacht, damit die Hersteller interoperable Produkte für die GA entwickeln können. Die BIG-EU ergänzt die Arbeit des ASHRAE-Normenausschusses um europäische Anforderungen.

Zu den Mitgliedern der BIG-EU gehören Gebäudeeigentümer, beratende Ingenieure und Gebäudebetreiber sowie Unternehmen, die sich mit dem Entwurf, der Herstellung, der Installation, der Inbetriebnahme und der Wartung von Gebäudeautomationsanlagen befassen, welche das herstellerneutrale Datenübertragungsprotokoll BACnet für die Kommunikation nutzen.

WG Facility Management

Ziel des Leitfaden WG-FM 100 – Version 01 der Arbeitsgruppe Facility Management (FM) ist es, Rahmenbedingungen für den sicheren Betrieb einer Liegenschaft zu definieren. Dabei orientiert sich dieser Leitfaden an den Lebenszyklusphasen im FM, wie diese bereits im deutschsprachigen Raum etabliert sind. Dazu gehört die „GEFMA 100“-Richtlinie (www.gefma.de/service/shop) und die Berücksichtigung einzelner Leistungsbilder der Honorarordnung für Architekten und Ingenieure (HOAI – www.hoai.de/hoai/leistungsphasen).

Inhalt des Leitfadens „Cybersicherheit in der Gebäudeautomation“

Abb. 1: Übersicht der Leistungsphasen nach HOAI

Im folgenden Leitfaden verwendete Abkürzungen:

AG	Auftraggeber
AMEV	Arbeitskreis Maschinen- und Elektrotechnik staatlicher und kommunaler Verwaltungen
ASHRAE	American Society of Heating, Refrigerating and Air-Conditioning Engineers
BACnet	Building Automation and Control Network
BACnet/SC	BACnet Secure Connect
B-BC	Building Controller (Geräteprofil)
BBMD	BACnet Broadcast Management Device
BetrSichV	Betriebssicherheitsverordnung
BMS	Building Management System
BSI	Bundesamt für Sicherheit in der Informationstechnik
CER	Critical Entities Resilience (EU-Richtlinie „Critical Entities Resilience Directive“)
CRA	Cyber Resilience Act
DDC	Direct Digital Control
DIN	Deutsches Institut für Normung
DSGVO	Datenschutz-Grundverordnung
EN	Europäische Norm
FM	Facility Management
FND	Firmenneutrales Datenübertragungsprotokoll
GA	Gebäudeautomation
GEFMA	German Facility Management Association
GEG	Gebäudeenergiegesetz
HOAI	Honorarordnung für Architekten und Ingenieure
IBM	Inbetriebnahmemanagement
IEC	Internationale Elektrotechnische Kommission (engl.: International Electrotechnical Commission)
INF.13	Baustein im IT-Grundschutz des BSI
INF.14	Baustein im IT-Grundschutz des BSI
INF.5	Baustein im IT-Grundschutz des BSI
IP	Internet Protocol
ISO	Internationale Organisation für Normung (engl.: International Organization for Standardization)
IT	Informationstechnologie (engl.: Information Technology)
KRITIS	Kritische Infrastrukturen
LP	Leistungsphase (nach HOAI)
MBE	Management- und Bedieneinrichtung
NET.1.2	Baustein im IT-Grundschutz des BSI
NIS 2	Netzwerk- und Informationssicherheit (2. EU-Direktive „Network and Information Security Directive“)
NIS2UmsuCG	NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz
OT	Operative Technologie (engl.: Operational Technology)
RMP	Risiko-Management-Prozess
SLA	Service Level Agreement
TGA	Technische Gebäudeausrüstung
TÜV	Technischer Überwachungsverein
VDI	Verein Deutscher Ingenieure e. V.
VDMA	Verband Deutscher Maschinen- und Anlagenbau

Einleitung

Die zunehmenden technologischen Entwicklungen in der Gebäudetechnik bis hin zu Smart Buildings und die schnelle Marktdurchdringung der Gebäudetechnik mit der allgemeinen Informationstechnik führt auch zu einem zunehmend höheren Cybersicherheitsrisiko.

Durch fehlendes Know-how (keine IT-Kernkompetenz) im Baumanagement, bei den Gebäudeplanungen und bei Betreibern im Gebäudekontext, durch Fachkräftemangel bei Integratoren und Inbetriebnehmern und der potentiell großen Auswirkungen erfolgreicher Cyberangriffe auf die Infrastruktur von Gebäuden ist eine gemeinsame IT/OT-Sicherheit nicht nur für Betreiber kritischer Infrastruktur und Bundesbehörden relevant, sondern muss zum Standard des Gebäudebetriebs werden; denn die Angreifer suchen und finden oft den schwächsten Punkt. Hierfür gibt es einige prominente Beispiele für den Umweg über die Gebäudetechnik.

Die Gesetzgeber haben dieses Gefahrenpotential erkannt und sowohl auf europäischer als auch auf nationaler Ebene entsprechende Cybersicherheitsvorgaben gemacht:

- auf europäischer Ebene
  NIS-2-Direktive (EU 2022/2555),
  Cyber Resilience Act (CRA – EU 2022/0272),

- auf nationaler Ebene (am Beispiel Deutschland)
  NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG).

In dem immer moderneren und digitalisierten Umfeld sowie aufgrund zunehmender internationaler politischer Spannungen wächst daher die Sorge über massive negative wirtschaftliche Auswirkungen im beruflichen Umfeld – u. a. bei Kompromittierung technischer Anlagen in eigener Verantwortung. Dazu gehören:

- wirtschaftlicher Schaden durch Verlust der Reputation – etwa durch negative öffentliche Wahrnehmung mit Pressemitteilungen oder Soziale Medien,
- finanzieller Schaden durch eingeschränkte Verfügbarkeit der firmeninternen Möglichkeiten, dazu gehören Erpressungsversuche oder negative Einflussnahmen in Produktionsprozessen.

Darüber hinaus wurden hohen Geldbußen, teilweise sogar mit persönlicher Haftung der Geschäftsleitung (wie z. B. beim „Cyber Resilience Act“ der EU), angekündigt.

Mit diesem Leitfaden soll ein Mehrwert durch Empfehlungen zu Standardisierungen u. a. von Prozessen, Infrastrukturen, Services und geeigneten Organisation (Rollen), erreicht werden (Security by Design von Beginn an). Denn ein Ausfall der Informationstechnik (IT) führt für die Gebäudetechnik mit seinen Operativen Technologien (OT) dazu, dass Betreiberpflichten nicht mehr oder nur mit enormem Aufwand wahrgenommen werden können.

Der Kreis der Betreiber von kritischen Infrastrukturen wird zunehmend und zukünftig mehr Unternehmensbereiche beinhalten. Resultierend daraus wachsen die Anforderungen von verschiedensten nationalen Verbänden und Organisationen, um die IT/OT-Sicherheit herzustellen [bspw. 1, 2]. Eine verlässliche und belastbare IT/OT-Infrastruktur aufzubauen und in Betrieb zu halten, ist eine Disziplin für Fachleute aus IT und Gebäudeautomation. Daher ist die Anwendung der Maßnahmen zur Erreichung einer IT/OT-Sicherheit nicht nur beim Betreiben kritischer Infrastruktur und bei Bundesbehörden relevant, sondern sollte ein integraler Ansatz zum Standard des Gebäudebetriebs werden.

[1]: AMEV-Gebäudeautomation 2023

[2]: VDMA-Einheitsblatt 24774

Dieser Leitfaden dient der Darstellung derzeit gültiger Anforderungen an die IT/OT-Sicherheit von Gebäuden. Verpflichtende Anforderungen gibt es für Betreiber kritischer Infrastrukturen (KRITIS) und Bundesbehörden. Angesprochen sind jedoch alle Beteiligten im Lebenszyklus des Planens, Errichtens und Betreibens der technischen Gebäudeausrüstung. Mit diesem Leitfaden sollen keine IT/OT-Sicherheitskonzepte entworfen werden. Es wird ein Überblick zu erforderlichen Tätigkeiten je Bauphasen mit entsprechenden Hinweisen zu bereits etablierten Hilfsmitteln gegeben.

Abgrenzung: Dieser Leitfaden berücksichtigt nicht die etablierten Prozesse für Funktionen in der Gebäudeautomation, sondern konzentriert sich auf die zusätzlichen Anforderungen und Aufgaben im IT/OT-RMP für die GA. Schnittstellen zu den im Nachgang erwähnten Use Cases für Smart Buildings und Gebäudemanagementsystemen sind aktuell nicht berücksichtigt und bei Bedarf separat zu betrachten.

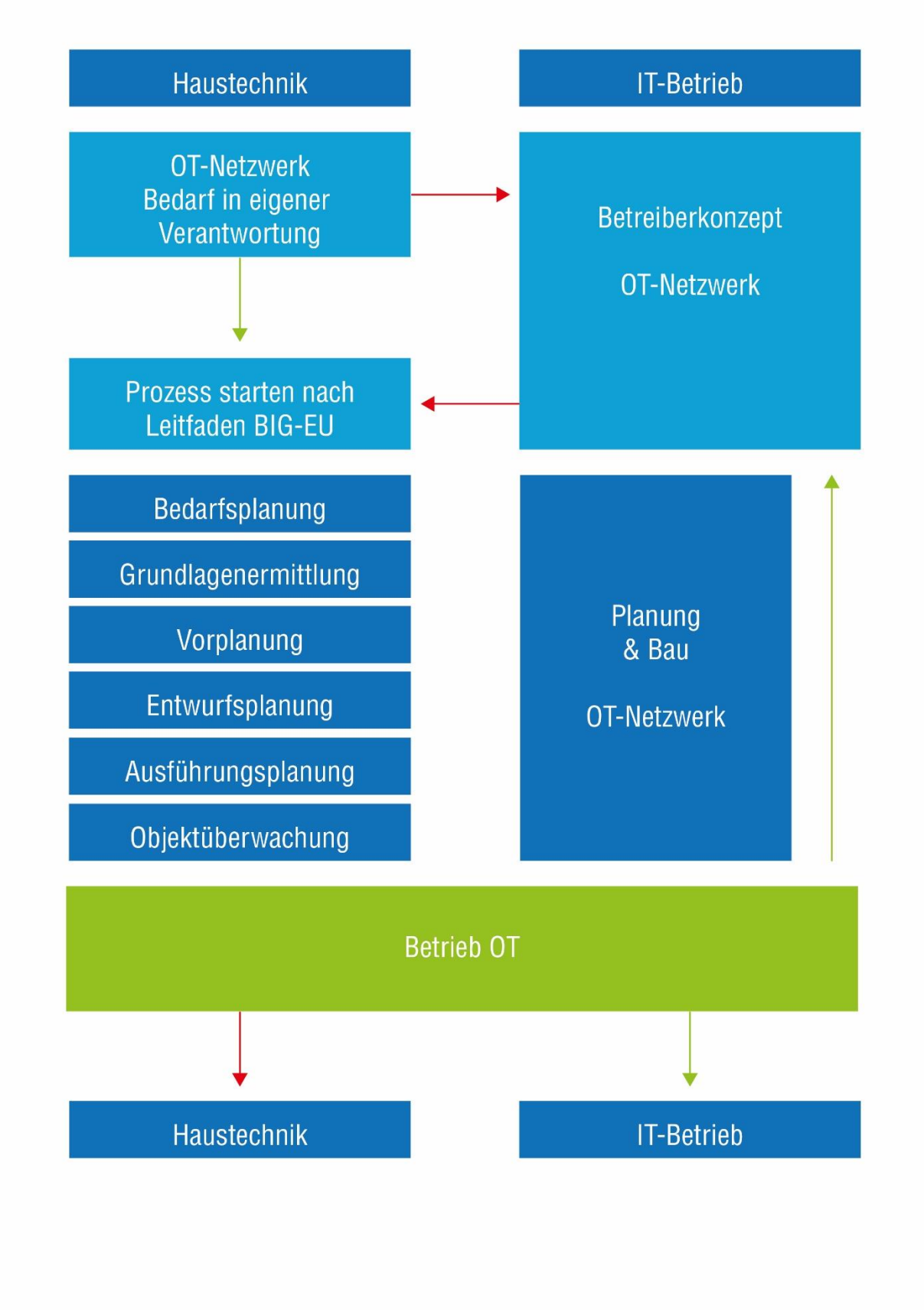

Abb. 2: Darstellung der verschiedenen Prozessschritte

Gemäß dem Flussdiagramm müssen während des Bauprozesses einer Gebäudeautomation, angelehnt an die Bau- bzw. Leistungsphasen der in Deutschland etablierten HOAI, eine Vielzahl von gesetzlichen Anforderungen berücksichtigt werden.
Bei der Vielzahl von Vorschriften ist es für interessierte Anwender schwer zu erkennen, wann im Planungs- und Bauprozess welche Empfehlungen, Normen oder Vorschriften herangezogen werden müssen.
Übersicht für eine individuelle Umsetzung der IT/OT-Sicherheitsanforderungen:

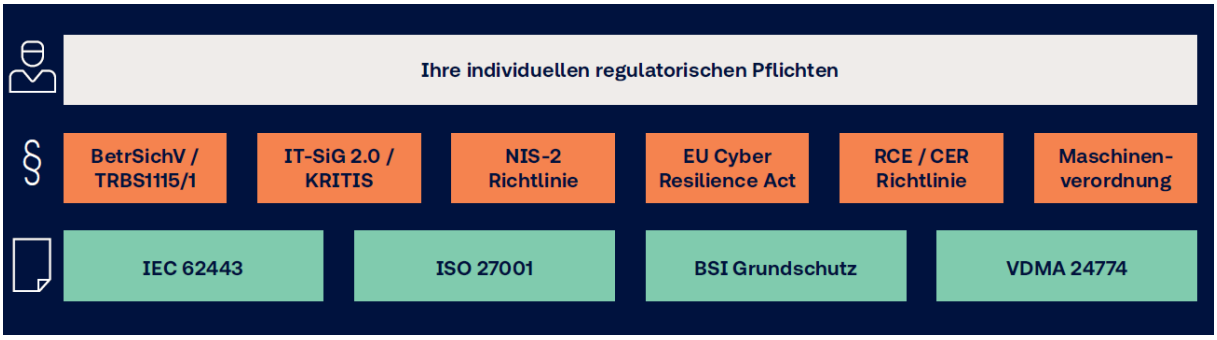

Abb. 3: Leitfaden GA TÜV SÜD Stand 02/24

Die Bewertung und der Einsatz der jeweils geforderten Sicherheitsanforderungen in dem Unternehmensumfeld übernehmen verschiedene Verantwortliche in ihren Rollen.

Die Benennung der Starter-Rollen orientiert sich aus der Empfehlung des BSI und der „INF.14 Gebäudeautomation“:

Rolle 1: Haustechnik

Rolle 2: Planer

Rolle 3: Administrator

Rolle 4: IT-Betrieb

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Haustechnik
Weitere Zuständigkeiten	Planer, Administrator, IT-Betrieb

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt.

Abb. 4: BSI – INF.14

Je nach individuellen Anforderungen/individueller Ausprägung der haustechnischen IT/OT-Systeme und -Services werden diese vier übergeordneten Rollen im IT/OT-Risikomanagementprozess (IT/OT-RMP) während dem Planungs- und Bauprozess spezifisch ergänzt bzw. umbenannt – gemäß Vorschlägen in dem Leitfaden definierten und folgenden Rollenkarten.

Auch hier gibt es weitere Umsetzungshinweise der INF.14, welche weitere Rollen vordefiniert.

Das Inbetriebnahmemanagement muss dabei auch die Rollen für die Bedien- und Managementfunktionen der GA berücksichtigen, die mit grundsätzlich unterschiedlichen Aufgaben und Anforderungen auf die GA zugreifen können. Diese Rollen sind

- Gebäudenutzer bzw. Nachfrageorganisationen, z. B. Mieter,
- interne oder externe Betreiberorganisationen (z. B. Haustechnik), die die operative Betriebsführung von GA und TGA-Anlagen sicherstellen,
- externe Dienstleister (z. B. für Instandhaltung oder Wartung), denen Zugriff auf einzelne Anlagen eingeräumt werden muss,
- Facility-Manager, die z. B. im Rahmen des kaufmännischen Managements oder zur Optimierung der Lebenszykluskosten Zugriff auf Managementfunktionen benötigen,
- Systemadministratoren, denen die Systempflege obliegt, z. B. für Backup und Restore, Systemparameter, Benutzerunterstützung und
- Errichter, die z. B. neue Firmware einspielen.

Abb. 5: Umsetzungshinweis INF.14

Der IT/OT-Risikomanagementprozess (IT/OT-RMP) definiert für alle Lebenszyklusphasen erforderliche Aufgaben und Rollen, welche für die jeweiligen Use Cases der Bedarfsplanung mehrfach vergeben und durchlaufen werden. Dem Systemeigner kommt hierbei eine übergeordnete Rolle der Gesamtverantwortung zu und er ist Bedarfsträger. Innerhalb der Gesamtverantwortung sind die zusätzlichen Rollen der Produktverantwortung und dem Sicherheitsmanagement, um Unternehmen für alle Use Cases in der Organisation zu definieren. Use Cases sind im weiteren Sinn der Bedarfsplanung auch moderne Anwendungsfälle digitaler Building-Management-Systeme (BMS) und Smart-Building-Plattformen. Diese sind in den Bauplanungsprozess als Anforderung für Building-IT-Systeme zu berücksichtigen, als Beispiel:

- Facility Management / Predictive Maintenance
- Schließmanagement / Indoor-Navigation / Raumbelegung
- Parkraummanagement / E-Mobility

Diese Systeme nutzen Informationen aus den GA-Systemen. Deren Schnittstellen sind bereits bei der Bedarfsplanung zu berücksichtigen.

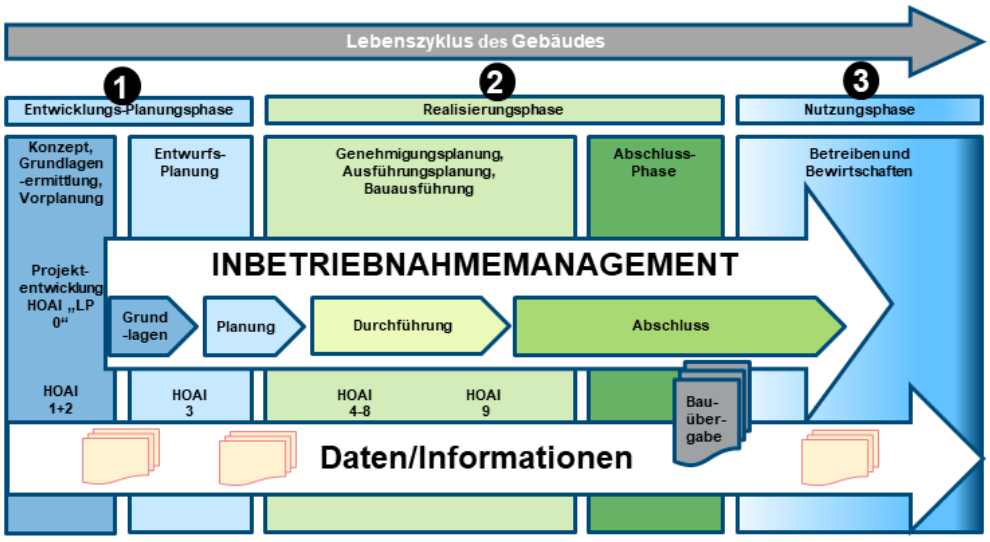

Abb. 6: Beispiel zu IT/OT-Sicherheit als integraler Ansatz bei der Deutschen Bundesbank

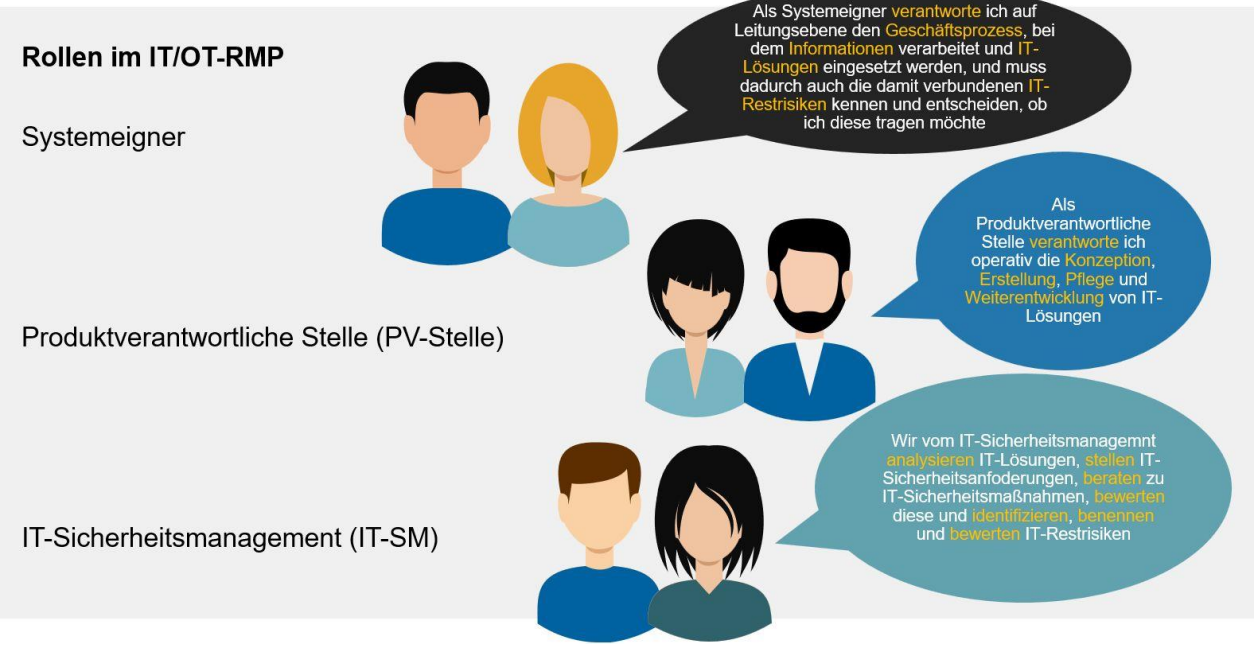

Abb. 7: Beispiel zum IT/OT-RMP der Deutschen Bundesbank

In dem folgenden Leitfaden sind „Rollen-Karten“ als Module passend zu einer Bedarfsanalyse und angelehnt an den jeweiligen Leistungsphasen der HOAI visualisiert.

Diese in der „INF.14 Gebäudeautomation“ definierten vier Rollen bilden das Grundgerüst und dienen zur ersten Orientierung im Umfeld der IT/OT-Sicherheit in der Gebäudeautomation. Genauer spezifizierte Rollenanforderungen sind in eckigen Klammern [xx] ergänzt.

Diese Anordnung der zur Verfügung gestellten „Karten“ ergibt eine Übersicht, in welcher Leistungsphase des Bauprozesses sich verantwortliche Stellen mit entsprechender Expertise um welche Themen kümmern müssen, damit die Umsetzung und Sicherheit durch die geforderten OT-Netzwerkstruktur erfolgreich in das anstehende Projekt implementiert werden. Bei Bedarf können die folgenden Karten an die definierten Rollen 1–4 übergeben werden.

Übersicht der zur Verfügung gestellten Karten:

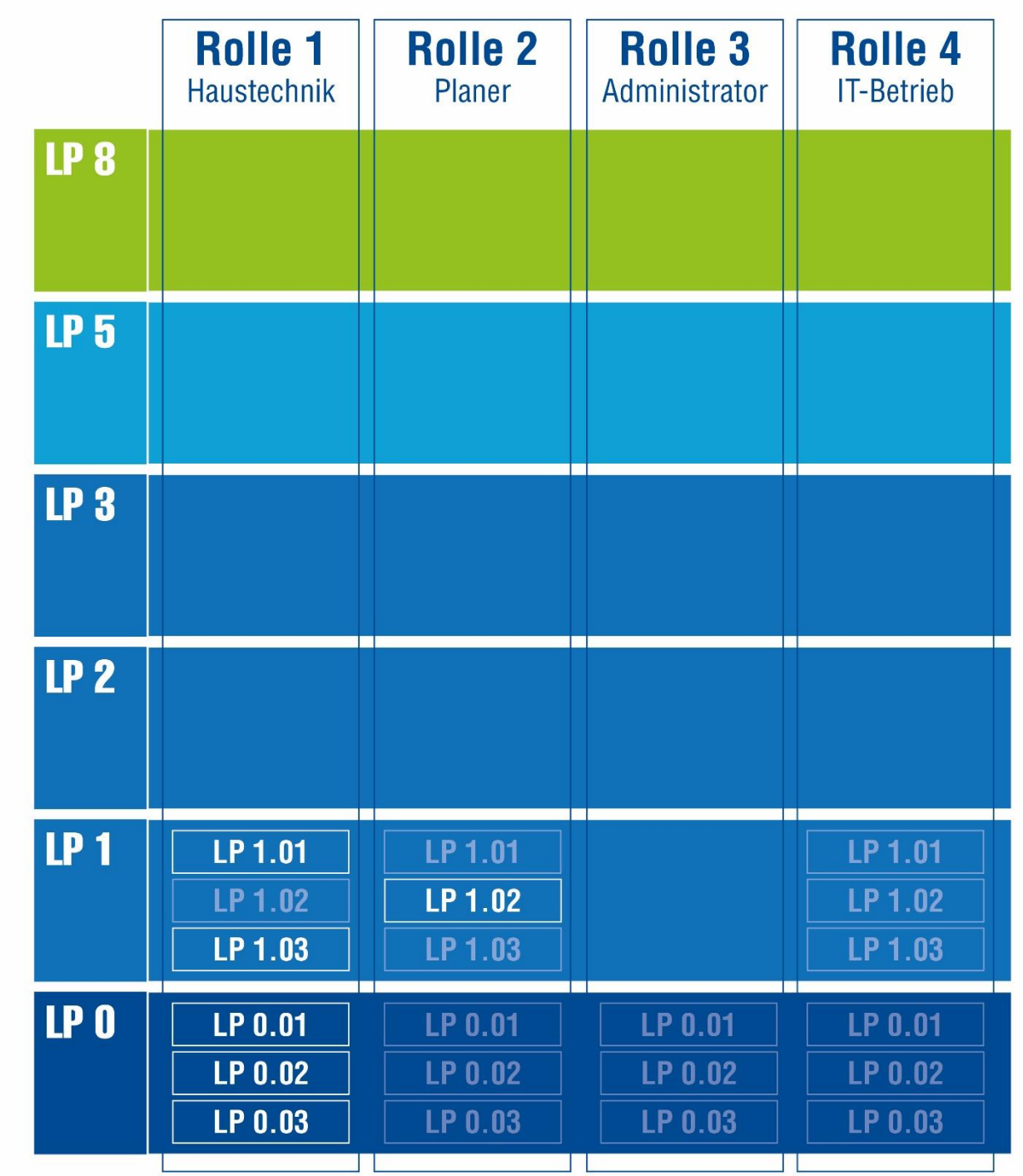

Abb. 8: Übersicht der Rollenkarten

LP 0: Bedarfsplanung – Betriebskonzept

Die Bedarfsplanung einschließlich der IT/OT-RMP-Betriebskonzepte spielen eine elementare Rolle für den effizienten, wirtschaftlichen und sicheren Gebäudebetrieb. Ebenso wird durch die qualitative Ausführung der Gebäudeautomation, welche auf der Grundlage einer bedarfsgerechten Planung erfolgt, die Basis für die Zukunftsfähigkeit eines Gebäudes geschaffen. Intelligente und vernetzte Systeme steigern dabei den Nutzerkomfort sowie den Wert einer Immobilie.

Passend zu den zur Anwendung kommenden Systeme und Kommunikationsprotokolle sowie zur Gebäudenutzung müssen wirksame IT/OT-RMP als Security-Maßnahmen getroffen werden. Die Starter-Rollen des IT/OT-RMP sind in den gesamten Planungs- und Integrationsprozess zur Errichtung der GA zu involvieren. Der Integrationsplaner, der ebenso für die GA, IT und OT zuständig ist, benötigt Informationen zu den konkreten Anforderungen an den Gebäudebetrieb sowie zu dessen Umsetzung. Zugleich muss die Umsetzung der Maßnahmen durch beteiligte Bauherren während des gesamten Planungs-, Integrations- und Inbetriebnahmeprozesses überwacht werden. Hierbei sollten Bauherren durch ein planungs- und baubegleitendes Qualitätscontrolling sicherstellen, dass die Anforderungen korrekt erfüllt werden und keine Schnittstellen- sowie Sicherheitsprobleme entstehen. Gibt es in dem Umfeld keine Expertise, kann diese Dienstleistung im Rahmen eines Inbetriebnahmemanagement (IBM) extern eingekauft werden.

Für den künftigen Betrieb der technischen Anlagen über eine integrierte Gebäudeautomation sind in der Phase der Bedarfsanalyse und des Betriebskonzeptes wichtige Grundlagen im Bereich der Netzwerksicherheit zu betrachten.

Dazu gehören:

- Spezifikation des Untersuchungsgegenstandes und Festlegung des Schutzbedarfs,
- Ermittlung der IT-Sicherheitsanforderungen und deren Schutzziele,
- Festlegung von Maßnahmen zur Identifikation und Bewertung von technischen Restrisiken,
- Berichterstattung und Genehmigung von Restrisiken.

Zudem stellen sich weitere Fragen zum Schutz der Informationen und der eingesetzten IT- und OT-Komponenten:

- Vertraulichkeit (Confidentiality),
- Integrität (Integrity),
- Verfügbarkeit (Availability),
- werden personenbezogene Daten erhoben bzw. verarbeitet? (DSGVO).

Die hier gewonnenen Kriterien und Erkenntnisse fließen dann in die weitere Realisierung des Bauprozesses nach der HOAI ein.

LP 0.01 Kartenthema: Gesetzliche/verpflichtende Anforderungen

Schlagworte:
#Gesetze GA #Verpflichtung GA #IT-Sicherheit in der GA #IT-Security #GEG

Kurzbeschreibung:
Der Gesetzgeber erhebt zunehmend Anforderungen an den energetisch optimierten Betrieb von Gebäuden durch Automation. Zudem sollen die gesetzlichen und verpflichtenden Anforderungen einen sicheren Gebäudebetrieb (IT-Sicherheit) sicherstellen.
Um den gesetzlichen und verpflichtenden Anforderungen bei der Errichtung von GA gerecht zu werden, ist daher eine Kenntnis über die Vielzahl an Gesetzen und Normen notwendig. Dieses Modul soll die wichtigsten Gesetze und Normen aufzeigen sowie deren Zusammenhänge erläutern.

Verweise:
Gebäudeenergiegesetz (GEG)

DIN V 18599-11 – Energetische Bewertung von Gebäuden

DIN EN ISO 52120-1:2019-12 – Energieeffizienz von Gebäuden

INF.14 Gebäudeautomation

KRITIS/NIS2-Richtlinie/BSI Grundschutz-Kompendium zu branchenspezifischen Standards und Anforderungen

Zielstellung:
Ziel dieses Moduls ist es, die bestehenden gesetzlichen Anforderungen zur Errichtung von Gebäudeautomationssystemen aufzuzeigen. Hierbei sind die Anforderungen an die Effizienz der Technische Gebäudeausrüstung (TGA), insbesondere der GA, geregelt und stellen dadurch einen energetisch effizienten Gebäudebetrieb sicher. Zudem soll die Informationssicherheit als integraler Bestandteil bei der Planung, Realisierung und dem Betrieb von GA dauerhaft etabliert werden.

Rolle:
Rolle 1 [Systemeigner/Bedarfsträger/Bauherr]

mit Zuarbeit von
Rolle 2 [integrale Beratung intern/extern]
Rolle 3 [GA-Systemadministrator]
Rolle 4 [IT-Security-Organisation/Manager]

LP 0.02 (gemäß Checkliste Anhang A)

Kartenthema: Normative Anforderungen

Schlagworte:
#GA Normen #Empfehlungen #VDI3814 #Richtlinien

Kurzbeschreibung:
Die Gebäudeautomation (GA) hat sich zunehmend als Leitdisziplin für den nachhaltigen Betrieb von Gebäuden und Immobilienportfolios über den gesamten Lebenszyklus entwickelt. Da die Voraussetzungen hierfür bereits beim Planen und Errichten (Neubau, Umbau, Erweiterung, Sanierung) geschaffen werden, ist es elementar wichtig, die GA bereits in den Planungs- und Bauprozessen mit den dazu geltenden Normen und Empfehlungen zu berücksichtigen. Dieses Modul soll die wichtigsten Normen und Empfehlung aufzeigen.

Verweise:
Technisches Regelwerk VDI 3814 – Gebäudeautomation (GA)

DIN EN ISO 16484-5:2023-02 – Systeme der Gebäudeautomation – Teil 5 (BACnet)

AMEV-Gebäudeautomation
AMEV-BACnet BACnet 2017
BACtwin in öffentlichen Gebäuden

VDMA 24774 - IT-Sicherheit in der Gebäudeautomation

VDI 6041:2017-07 Facility-Management – Technisches Monitoring von Gebäuden und gebäudetechnischen Anlagen

Facility Management; Inbetriebnahmemanagement für Gebäude; Methoden und Vorgehensweisen für gebäudetechnische Anlagen

Zielstellung:
Ziel dieses Moduls ist es, die bestehenden Normen und Empfehlungen zur Errichtung von Gebäudeautomationssystemen aufzuzeigen. Die Anwendung der Richtlinienreihe, Normen und Empfehlungen soll dazu führen, dass die Nachhaltigkeit von Gebäuden und Immobilienportfolios sichergestellt und verbessert wird. Hierbei trägt der Bauherr, besonders bei der Definition seiner Anforderungen, eine wichtige und entscheidende Rolle.

Die Anwendung der Richtlinienreihe, Normen und Empfehlungen ist ein wichtiger Bestandteil bei der Planung, Realisierung und dem Betrieb von GA.

Rolle:
Rolle 1 [Anlagenverantwortliche TGA]

mit Zuarbeit von
Rolle 2 [integrale Beratung intern/extern]
Rolle 3 [GA-Systemadministrator]
Rolle 4 [IT-Security-Organisation/Manager]

LP 0.03 (gemäß Checkliste Anhang A)

Kartenthema: Bedarfsplanung, Betreiberkonzept und Lastenheft

Schlagworte:
#Bauherr/Nutzer #Objektplaner/Architekt #Fachplaner TGA #Hersteller GA Komponenten #Ausführende Gewerke #Betreiber

Kurzbeschreibung:
Die Schritte der Bedarfsplanung sollen sicherstellen, dass die Aufgabenstellung des Auftraggebers (AG) umfänglich erfasst und vollständig beschrieben wird. Die im Rahmen der Bedarfsplanung zu erstellenden Dokumente – wie Betreiberkonzepte und Lastenhefte – liegen im Verantwortlichkeitsbereich des AG (besondere Leistung nach HOAI) und sind durch diesen kontinuierlich zu pflegen. Diese Dokumente stellen die wesentliche Grundlage für die Planung der GA dar und sind durch alle Verwender verpflichtend zu beachten.

Verweise:
Technisches Regelwerk VDI 3814 – Blatt 2.1 – Gebäudeautomation (GA) – Planung – Bedarfsplanung, Betreiberkonzept und Lastenheft

VDI MT 3814 Blatt 6 – 2020-01 – Beuth.de – Gebäudeautomation (GA) – Qualifizierung, Rollen und Kompetenzen

AMEV-Inbetriebnahmemanagement 2023-10

Zielstellung:
Die rechtzeitige Fertigstellung von Bedarfsplanung, Betreiberkonzept und Lastenheft ist entscheidend für die Gebäudeautomation. Dies verbessert den Bauprozess durch:

- **Frühe Planungssicherheit:** Klarheit über Ziele und Umfang durch rechtzeitige Bedarfsplanung,
- **Risikominimierung:** Identifikation und Bewältigung potenzieller Probleme durch frühzeitiges Betreiberkonzept und Lastenheft,
- **effiziente Ressourcenallokation:** bessere Zuweisung von Materialien, Arbeitskräften und Finanzen durch rechtzeitige Dokumente,
- **bessere Ausschreibungen:** präzise Ausschreibungen dank frühzeitigem Lastenheft für Auswahl von Auftragnehmern und Lieferanten,
- **beschleunigte Umsetzung:** schnellere Projektumsetzung mit klaren Vorgaben aus Betreiberkonzept und Lastenheft,
- **bessere Koordination der Gewerke:** verbesserte Abstimmung zwischen verschiedenen Gewerken durch rechtzeitige Dokumente,
- **Kosteneffizienz:** leichtere Budgetierung und Kostenkontrolle für Projektabschluss innerhalb des Budgets,
- **Kunden- und Nutzerzufriedenheit:** Erfüllung der Bedürfnisse der Nutzer durch rechtzeitig erstelltes Betreiberkonzept für höhere Zufriedenheit.

Rolle:
Rolle 1 [Anlagenverantwortliche TGA]

mit Zuarbeit von
Rolle 2 [integrale Beratung intern/extern]
Rolle 3 [GA-Systemadministrator]
Rolle 4 [IT-Security-Organisation/Manager]

LP 1: Grundlagenermittlung – Projektvorbereitung

Kick-off IT/OT-Risikomanagementprozess (RMP)

1. Mitwirken bei der Koordination mit dem IT-Sicherheitsmanagement des AG durch den Integrationsplaner TGA und Definition der Randbedingungen für die Durchführung des IT-Sicherheitsmanagements für den weiteren Projektverlauf.

2. Ermittlung der relevanten Randbedingungen und Vorgaben insbesondere aus den Bausteinen BSI (u. a. „INF.13 Technisches Gebäudemanagement“ und „INF.14 Gebäudeautomation“) sowie weiterer Vorgaben aus den Abteilungen.

   Beratung durch IT-Sicherheitsmanagement und klare Rollenverteilung.

LP 1.01 (gemäß Checkliste Anhang A)

Kartenthema: IT-Infrastruktur

Schlagworte:
#Netztopologie, #Bestandssituation, #gesetzliche IT-Vorgaben, #Zielvorstellung
#IT-Dienstleister, #IT-Betreiberverantwortung, #IT-Schnittstellen, #IT-SLA

Kurzbeschreibung:

- **Beschreibung und Darstellung der Bestandssituation im IT-Netzwerk**
  Für die Projektvorbereitung ist in Bestandsinstallationen eine ausführliche und korrekte Grundlagenermittlung unbedingt durchzuführen, damit die aktuelle Situation in Bezug auf die neu zu planende und gemäß den gesetzlichen Richtlinien anzupassende Zielvorstellung deutlich wird. Mit Hilfe einer logischen oder ortsbezogenen Netzwerktopologie kann sich das Planungsteam schnell einen Überblick der vorhandenen IT-Infrastruktur machen und diese im weiteren Planungsprozess mit weitergehenden Informationen präzisieren. Für Neu- und Bestandsprojekte gibt eine Zukunfts-Netzwerk-Topologie allen Projektbeteiligen und Entscheidern eine strukturierte Darstellung der Zielstellung.
- **Wer betreibt die IT-Infrastruktur (intern/extern)**
  Gibt es mehrere interne oder externe Dienstleister, wer sind die Ansprechpartner und Wissensträger? Wer hat die Betreiberverantwortung bis zu welchen Schnittstellen?

Verweise:
BSI, NET.1.2 – Netzmanagement

Technisches Regelwerk VDI 3814 – Blatt 2.2: Gebäudeautomation (GA) – Planung – Planungsinhalte, Systemintegration und Schnittstellen

Zielstellung:
Die rechtzeitige Fertigstellung von Bedarfsplanung, Betreiberkonzept und Lastenheft ist entscheidend für die Gebäudeautomation. Dies verbessert den Bauprozess durch:

- Definition der Zuständigkeit bzw. der Betreiberverantwortung,
- Beschreibung Bestandssituation der IT-Infrastruktur mit Hilfe einer Topologie,
- Wer ist in der Betreiberverantwortung, damit die IT-Infrastruktur stabil funktioniert?
- Wer sind die Ansprechpartner und Wissensträger (intern/extern) beim Betreiber?
- Wie lauten die Betreiberverträge (auch Service-Level-Agreement (SLA) genannt)?
- Wo liegen die Schnittstellen in der IT-Infrastruktur?

All dies gilt es in der Projektvorbereitung herauszufinden.

Rolle:
Rolle 1 [IT-Abteilung]

mit Zuarbeit von
Rolle 2 [integrale Beratung intern/extern]
Rolle 4 [IT-Security-Organisation/Manager]

LP 1.02 (gemäß Checkliste Anhang A)

Kartenthema: OT-Infrastruktur

Schlagworte:
#GA-Bestandserfassung, #DDC, #Automationseinrichtung, #B-BC, #BBMD

Kurzbeschreibung:

- **Erfassung der GA-Devices (Protokoll-Schnittstelle, IP-Adresse, BACnet-Revision)**
  Für die Projektvorbereitung sind die vorhandenen GA-Devices (DDC-Controller) und OT-Infrastrukturkomponenten (BBMDs, Gateways, Bus-Repeater etc.) mit ihren technischen Attributen aufzunehmen. In Bestandsinstallationen ist eine ausführliche und korrekte Grundlagenermittlung unbedingt durchzuführen, damit die aktuelle Situation in Bezug auf die neu zu planende und gemäß den gesetzlichen Richtlinien anzupassende Zielvorstellung deutlich wird.
  Mit Hilfe einer logischen oder ortsbezogenen Netzwerktopologie kann sich das Planungsteam schnell einen Überblick der vorhandenen OT-Infrastruktur machen und diese im weiteren Planungsprozess mit weitergehenden Informationen präzisieren sowie cybersicher ausführen. Für Neu- und Bestandsprojekte gibt eine Zukunfts-Netzwerk-Topologie allen Projektbeteiligen und Entscheidern eine strukturierte Darstellung der Zielstellung.
- **Zugriffsberechtigungen zu MBE, Technikzentralen (Admin, Techniker, Hausmeister, externe Dienstleister)**
  Gibt es mehrere interne oder externe Dienstleister, wer sind die Ansprechpartner und Wissensträger? Wer hat die Betreiberverantwortung bis zu welchen Schnittstellen?

Verweise:
INF.5: Raum sowie Schrank für technische Infrastruktur

INF.14 Gebäudeautomation

Technisches Regelwerk VDI 3814 – Blätter 1/2.1/2.2/2.3/4.2

B-PAT-Beschreibung
B-PAT Template Table

Zielstellung:

- Definition der Zuständigkeit bzw. Betreiberverantwortung,
- Beschreibung Bestandssituation der OT-Infrastruktur mit Hilfe einer Topologie,
- Wer ist in der Betreiberverantwortung, damit die OT-Infrastruktur stabil funktioniert?
- Wer sind die Ansprechpartner und Wissensträger (intern/extern) beim GA-Betreiber?
- Wie lauten die Betreiberverträge (auch Service-Level-Agreement (SLA) genannt)?
- Wo liegen die Schnittstellen in der OT-Infrastruktur?

All dies gilt es in der Projektvorbereitung herauszufinden.

Rolle:
Rolle 2 [integrale Beratung intern/extern]

mit Zuarbeit von
Rolle 1 [Anlagenverantwortliche TGA]
Rolle 4 [IT-Security-Organisation/Manager]

LP 1.03 (gemäß Checkliste Anhang A)

Kartenthema: Betreiberkonzept

Schlagworte:
#GA-Betreiberkonzept, #Lastenheft GA

Kurzbeschreibung:

- **Beschreibung der Randbedingungen für das Betreiben von Gebäudeautomation (GA) in Liegenschaft/Projektfläche/bewirtschaftetem Gebäudebestand**
  Für eine sinnvolle Systemintegration in der Gebäudeautomation ist es im Vorfeld der Planung notwendig, Ausführung und Nutzung der Anforderungen an das technische System für den neu zu gestaltenden Anwendungsfall (Projekt/Modernisierung/ Sanierung) zu definieren.
  Dabei ist es von hohem Nutzen, die Ziele des Betreibens von betriebstechnischen Anlagen im Planungsprozess zu kennen.
- Damit zeitlich oder örtlich unterschiedliche GA-Planungen auch zu vergleichbaren und gleich zu nutzenden Ergebnissen führen, ist ein Standard, das sog. Lastenheft GA der Liegenschaft, zu definieren.

Verweise:
VDI/GEFMA 3810 Blatt 5: Betreiben von Gebäuden und Instandhalten von gebäudetechnischen Anlagen – Gebäudeautomation

Technisches Regelwerk VDI 3814 – Blatt 2.1 – Gebäudeautomation (GA) – Planung – Bedarfsplanung, Betreiberkonzept und Lastenheft

Zielstellung:

- **Anforderungen des AG/Bauherrn aufnehmen und priorisiert beschreiben**
  Welche Gewerke werden mit Gebäudeautomation betrieben und welche Management-Bedien-Funktionen werden für das Betreiben der Liegenschaft benötigt.
  (Visualisierung/Registrierung/Bedienung/Archivierung)
- **Definition der Prozesse, Prozessbeteiligten und der Verantwortung in der Nutzung von GA**
  Welche Abläufe und Meldeketten gibt es schon bzw. werden in Zukunft zusätzlich benötigt?
- **Abgrenzung interner/externer Prozesse**
  Welche Dienstleister/Wartungsnehmer handeln auf welcher Grundlage zu welchen Reaktionszeiten? Wo ist dies schriftlich niedergelegt (z. B. in einem sog. Service-Level-Agreement (SLA)/Dienstleistungsvertrag)?
- **Sichereres und wirtschaftliches Betreiben von GA mit IT-Netzwerken**
  über die gesamte Liegenschaft trotz wechselnder GA-Auftragnehmer/GA-Systemintegratoren/GA-Errichterfirmen

Rolle:
Rolle 1 [GA-Betrieb/Systemeigner]

mit Zuarbeit von
Rolle 2 [GA-Fachplaner]
Rolle 4 [IT-Betrieb]

LP 2–9: Hinweis – Folgeversionen in Arbeit

Der aktuelle Stand des Leitfadens orientiert sich an etablierten Methoden aus Deutschland. Mit der Betrachtung der Bedarfsplanung – Betriebskonzept (LP 0) und Grundlagenermittlung – Projektvorbereitung (LP 1) soll nicht suggerieren, dass in den darauffolgenden Leistungsphasen die Inhalte des Leitfadens nicht weiter berücksichtigt werden sollten.

Die weitere Zusammenstellung der notwendigen Empfehlungen, Richtlinien und Prozesse sind in Arbeit und werden in darauffolgenden Versionen des Leitfadens integriert.

Danksagung

Der Präsident der BACnet Interest Group Europe (BIG-EU) Thomas Kurowski bedankt sich für die aktive Umsetzung dieser Version des Leitfadens bei allen Beteiligten der Arbeitsgruppe WG-FM – angeleitet von den Vorsitzenden Patrick Lützel (TÜV SÜD Industrie Service GmbH) und Rüdiger Schröder (Fraport AG).

Ebenfalls gebührt allen Personen ein Dank, die durch konstruktive Rückmeldungen beim Public Review zu dieser Version beigetragen haben.

Abbildungsverzeichnis

Anhang A: Checkliste zur Cybersicherheit in der Gebäudeautomation

Nummer	Anforderung	berücksichtigt
LP 0: Bedarfsanalyse – Betriebskonzept		
LP 0.01	Gesetzliche/verpflichtende Anforderungen	ja/nein
LP 0.02	Normative Anforderungen	ja/nein
LP 0.03	Bedarfsplanung, Betreiberkonzept und Lastenheft	ja/nein
LP 1: Grundlagenermittlung		
LP 1.01	IT-Infrastruktur	ja/nein
LP 1.02	OT-Infrastruktur	ja/nein
LP 1.03	Betreiberkonzept	ja/nein