Leitfaden Cybersicherheit in der Gebäudeautomation

BIG-EU
WG-FM 100
Version 02

Stand 09/26

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. Eingebettet in das Leistungsspektrum der „GEFMA 100“- Lebenszyklusphasen (www.gefma.de/service/shop) und die Berücksichtigung einzelner Leistungsbilder und Integration in die Honorarordnung für Architekten und Ingenieure (HOAI – www.hoai.de/hoai/leistungsphasen).

Inhalt des Leitfadens „Cybersicherheit in der Gebäudeautomation“

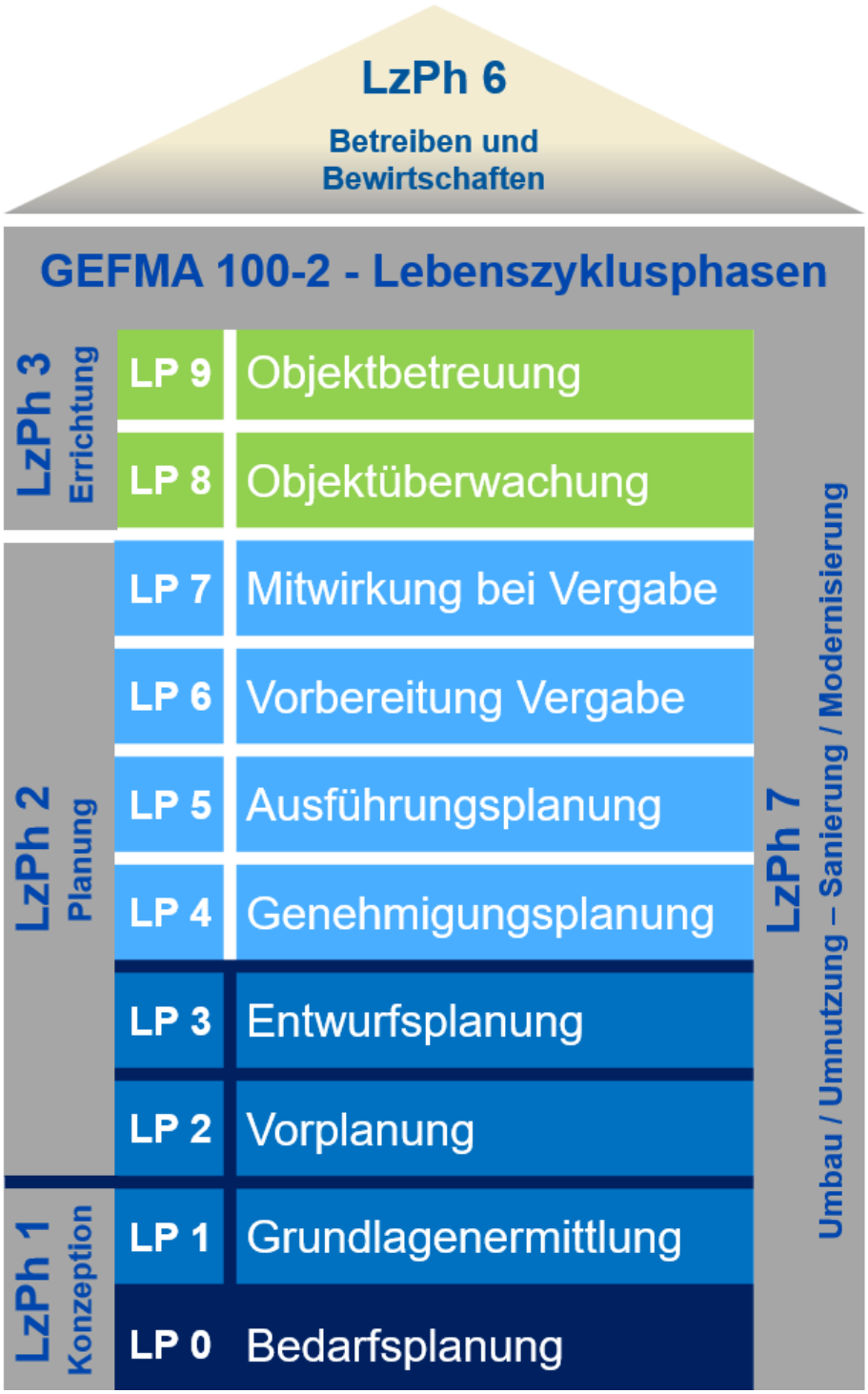


Abb. 1: Einordnung der Leistungsphasen in Anlehnung der HOAI in die Lebenszyklusphasen (LzPh) der GEFMA 100-2

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
BCM	Business Continuity Management
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
CySi	Cybersicherheit
DDC	Direct Digital Control (nicht mehr gebräuchlich)
DIN	Deutsches Institut für Normung
DSGVO	Datenschutz-Grundverordnung
EN	Europäische Norm
EST	Enrollment over Secure Transport (automatisierter Erhalt und Erneuerung von digitalen Zertifikaten durch eine PKI)
FM	Facility Management
FND	Firmenneutrales Datenübertragungsprotokoll
GA	Gebäudeautomation
GEFMA	German Facility Management Association
GModG	Gebäudemodernisierungsgesetz, ehem. Gebäudeenergiegesetz (GEG)
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)
IT/OT-RMP	IT/OT-Risiko-Management-Prozess (gemäß der Richtlinie / siehe auch RMP)
KRITIS	Kritische Infrastrukturen
LP	Leistungsphase (nach HOAI)
LzPh	Lebenszyklusphasen (nach GEFMA)
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)
PKI	Public-Key-Infrastruktur (digitaler Ausweis zur Erstellung von CA-Zertifikaten)
RMP	Risiko-Management-Prozess (gemäß BSI bzw. VDI/VDE 2182)
SLA	Service Level Agreement
TGA	Technische Gebäudeausrüstung
VDMA	Verband Deutscher Maschinen- und Anlagenbau
VDI	Verein Deutscher Ingenieure e. V.
ZÜS	Zugelassene Überwachungsstelle - In Deutschland Prüforganisationen wie z.B. TÜV, DEKRA

Einleitung

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

BACnet wurde vor rund 30 Jahren als offenes Kommunikationsprotokoll entwickelt, um die verschiedenen technischen Gewerke einer Liegenschaft herstellerneutral miteinander zu vernetzen. Der offene Charakter dieser „Sprache“ galt lange Zeit als großer Vorteil, birgt heute jedoch auch erhebliche Risiken für Cyberangriffe. Um diesem Risiko zu begegnen, wurde der BACnet-Standard 2016 erstmals um die Möglichkeit verschlüsselter Kommunikation erweitert. Mit dem Addendum 135-2016bj wurde 2019 die Spezifikation BACnet/SC („Secure Connect“) offiziell in den BACnet-Standard aufgenommen und als Teil des ANSI/ASHRAE Standard 135-2016 veröffentlicht. Damit wurde eine sichere, TLS-verschlüsselte Kommunikation im BACnet-Protokoll etabliert. Doch was nützt BACnet/SC, wenn die zugrunde liegende Netzinfrastruktur weiterhin Sicherheitslücken aufweist?

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.

Regulatorik

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** (vorbehaltlich am Beispiel Deutschland)
  Umsetzung der NIS-2-Direktive in nationales Recht mit dem Gesetz zur „NIS-2-Richtlinie“ am 06.Dezember 2025, sowie dem KRITIS-Dachgesetz auf Grundlage der DIN SPEC 14027

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

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

Für alle betroffenen Unternehmen ist eine direkte persönliche Haftung für Mitglieder der Leitungsorgane (Management Bodies) bei Schäden eingeführt, die durch die Pflichtverletzung der handelnden Personen entstehen. Darüber hinaus sind signifikante Geldstrafen vorgesehen, die sich prozentual von dem jeweiligen weltweiten Jahresumsatz des betroffenen Unternehmens orientieren (wie z. B. beim „Cyber Resilience Act“ der EU - Kapitel 7, Artikel 64.2 sowie NIS-2-Richtlinie, Art. 34).

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 ein sicherer Betrieb nicht mehr oder nur mit enormem Aufwand wahrgenommen werden kann.

Der Kreis der Betreiber von besonders wichtigen (bwE) und wichtigen (wE) Einrichtungen 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, 3]. 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]: AMEV-LAN 2021

[3]: VDMA-Einheitsblatt 24774

HINWEIS: Es ist also im eigenen Interesse einer verantwortlichen Führungskraft auf Ebene C-Level im betroffenen Unternehmensumfeld, auch die Resilienz seines beruflichen Umfeldes inkl. der informationstechnischen (IT) sowie operativen (OT) Systeme zu stärken sowie verantwortlichen Mitarbeitern notwendige Maßnahmen für finanzielle Freiräume zu gewährleisten. Der dazu etablierte Prozess wird Risiko-Management-Prozess (RMP) genannt und ist auch in der VDI/VDE 2182 beschrieben.

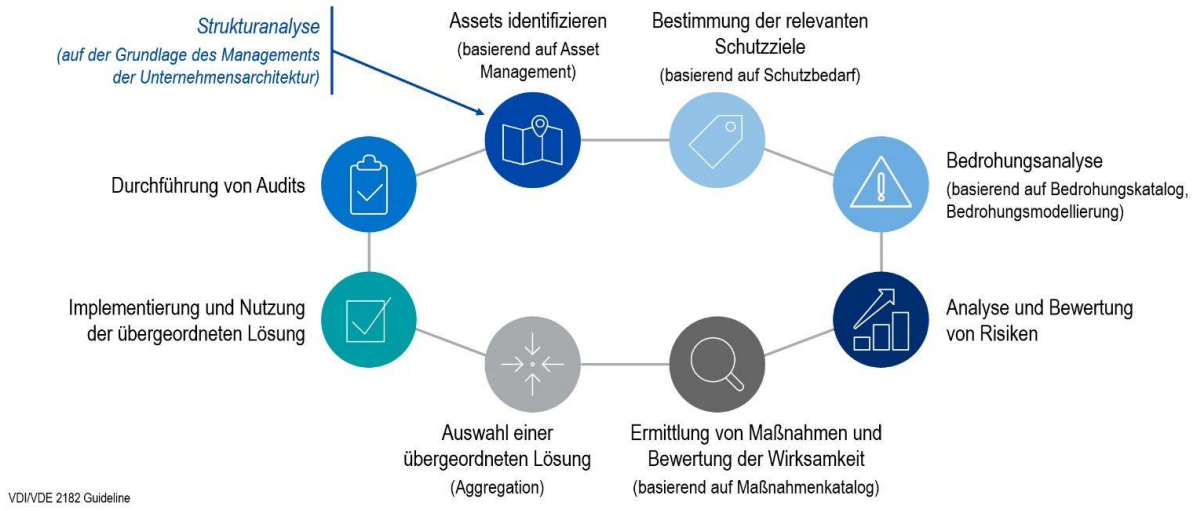


Abb. 2: VDI / VDE 2182 Guideline

Ist diese grundlegende Bereitschaft zur Einführung eines RMP nicht gegeben, sind darauf aufbauende Aktivitäten, wie z.B. eine daraus resultierende Teilanalyse des Systems der Gebäudeautomation (GA-S) anhand des Leitfadens nicht von Erfolg gekrönt.

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 Leistungsphasen 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.

Einstieg in die Praxis

Einleitend als Grundlage zu dem folgenden Schaubild (Abb. 2).
Sie stehen vor der Herausforderung:

- Sie werden im Umfeld der **Haustechnik** mit der Realisierung einer gebäudetechnischen Anlage betraut.
- Nach Stand und Regel der Technik verfügt das dazu notwendige Automationssystem mittlerweile über eine digitale Kommunikationsmöglichkeit. Sie nehmen zur Klärung des Sachverhaltes Kontakt mit Ihrem unternehmenseigenen **IT-Betrieb** auf.
- Der IT-Betrieb verfügt derzeit über kein anzuwendendes Betreiber Konzept für operative Technologien (OT) in einem **OT-Netzwerk.**

Was sollten Sie nun in die Wege leiten?
Folgend werden Prozessschritte empfohlen, die u.a. Ihre interne Struktur zur Unternehmensorganisation hinterfragen.
Ein denkbares Zielbild ist die Übernahme des **OT-Betriebes** durch den **IT-Betrieb**.

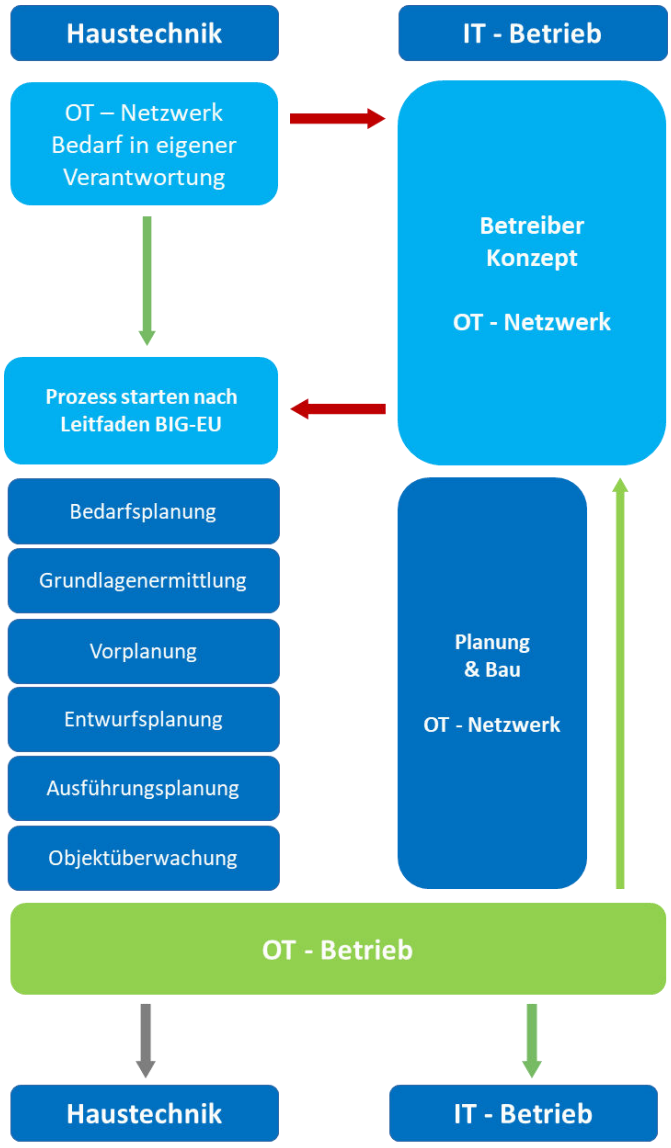


Abb. 3: Darstellung der verschiedenen Prozessschritte

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:

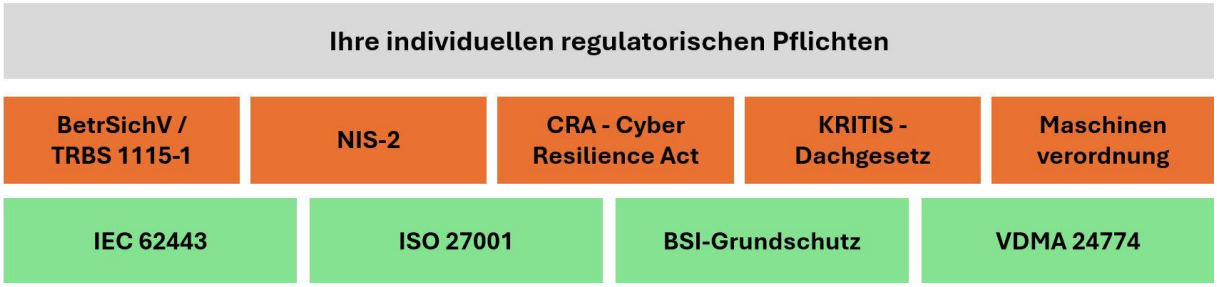


Abb. 4: Auf Basis Leitfaden GA TÜV SÜD Stand 02/24 (aktualisiert 09/26)

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-Grundschutzes mit dem Baustein „INF.14 Gebäudeautomation“ und wird in den jeweiligen Rollenkarten konkretisiert:

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. 5: BSI / IT-Grundschutz – INF.14

Je nach individuellen Anforderungen bzw. individueller Ausprägung der haustechnischen IT/OT-Systeme und -Services werden diese vier übergeordneten Rollen im IT/OT- Risiko-Management-Prozess (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. 6: Umsetzungshinweis INF.14

IT/OT: Organisation, Prozesse und Rollen

Der IT/OT-Risiko-Management-Prozess (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 für alle Use Cases des Unternehmens 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.

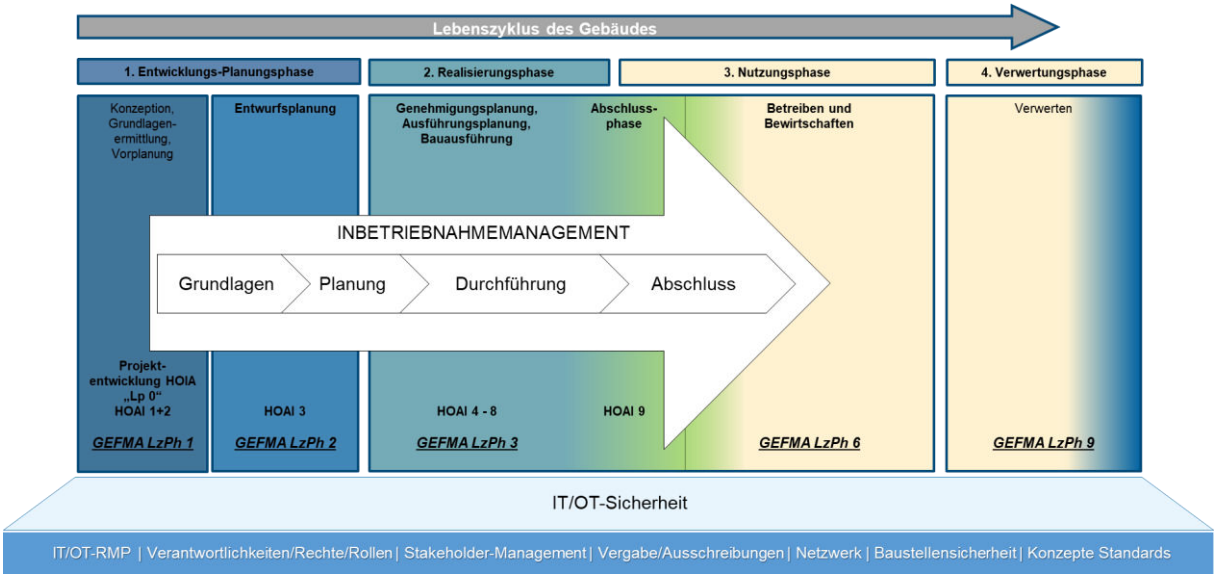


Abb. 7: Beispiel zu IT/OT-Sicherheit als integraler Ansatz bei der Deutschen Bundesbank

Der Prozess zur Risikoanalyse und -behandlung nach BSI-Standard 200-3, nachfolgend Risiko-Management-Prozess (RMP) genannt, umfasst die systematische Identifikation, Bewertung, Behandlung und Überwachung von Risiken für schützenswerte Daten, Systeme und Ressourcen in IT- und OT-Infrastrukturen, deren Verfügbarkeit, Integrität und Vertraulichkeit für den Betrieb essenziell sind.

Durch gezielte Fragestellung nach dem Wer, Wo, Was, Wie wird die Prozesslogik durchlaufen.

	Fragestellung	**Ziel/Zweck**	**Beschreibung**
Wer	Wer verantwortet und ist beteiligt?	Verantwortung und Steuerung, Prozessbeteiligung	Benennung von Verantwortlichkeiten und Rollen, bspw. die Systemeignerschaft. Die Umsetzung des IT/OT-RMPs erfolgt in Zusammenarbeit mit den jeweiligen Fachverantwortlichen und IT-Verantwortlichen.
Wo	welcher Bereich wird betrachtet?	Abgrenzung des Betrachtungsbereichs	Klar definierter Geltungsbereich (Informationsverbund), der alle relevanten Geschäftsprozesse, IT-Systeme, Anwendungen, Daten und Räumlichkeiten umfasst. Die Abgrenzung erfolgt zu Beginn und ist Grundlage für alle weiteren Schritte des Prozesses.
Was	Um was handelt es sich konkret?	Betrachtungsgegenstände und Sicherheitsanforderungen	Für jeden Betrachtungsgegenstand sind Schutzbedarfe hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit zu erstellen, um die erforderlichen Sicherheitsanforderungen festzulegen.
Wie	Wie ist die Reihenfolge und Vorgehensweise?	Identifikation, Bewertung und Behandlung von Risiken	Identifikation von Gefährdungen, Abgleich mit Grundschutzmaßnahmen, ggf. vertiefte Risikoanalyse und Umsetzung zusätzlicher Maßnahmen sowie kontinuierliche Überprüfung.

Tabelle 1: Aus den Quellen BSI IT Grundschutz, BSI-Standard 200-2: IT-Grundschutz-Methodik, BSI-Standard 200-3: Risikoanalyse und IT-Grundschutz-Kompendium

Darum empfehlen wir für die Bestimmung der zu betrachtende Gegenstände eines GA-System (GA-S) mit den dazugehörigen Werten (Assets), in Anlehnung an die VDI 3814 Blatt 1, die Clusterbildung anhand der funktionalen Struktur. Auf der Basis kann eine notwendige Cybersicherheit in der Anlagenautomation (AA), z.B. Wärmeerzeuger, der Raumautomation (RA) sowie dem Managementsystem (GA-M) mit Anbindungen anderer Systeme zu Nutzung von diversen Anwendungsfällen (Use-Cases) bestimmt werden.

Dabei dürfen auch die dazu jeweils verwendeten Bedien- und Anzeigeeinrichtungen (BAE) nicht von der Betrachtung ausgeschlossen werden.

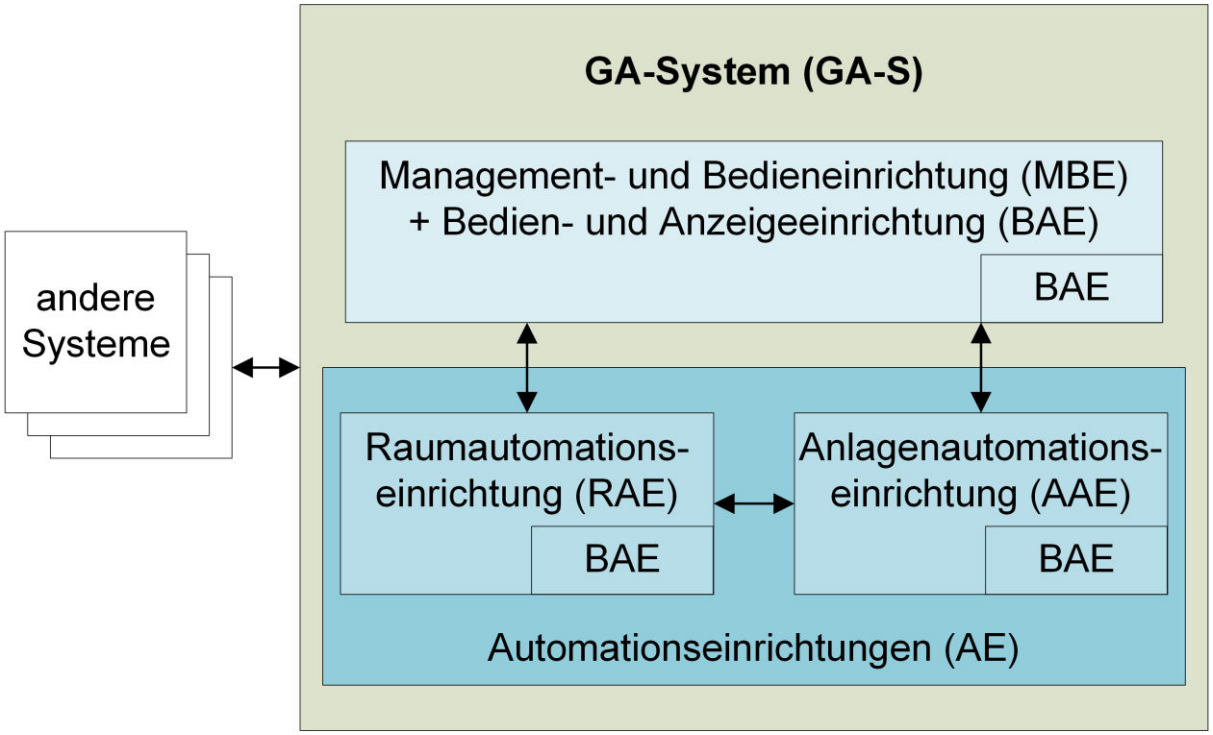


Abb. 8: Darstellung aus der VDI 3814

Betrachtungsgegenstände finden sich auf allen Ebenen der Automatisierungspyramide, die Darstellung wurde in Aufgabenbereiche für Gebäude an die aktuellen Anforderungen seitens AMEV erweitert und ergänzt.

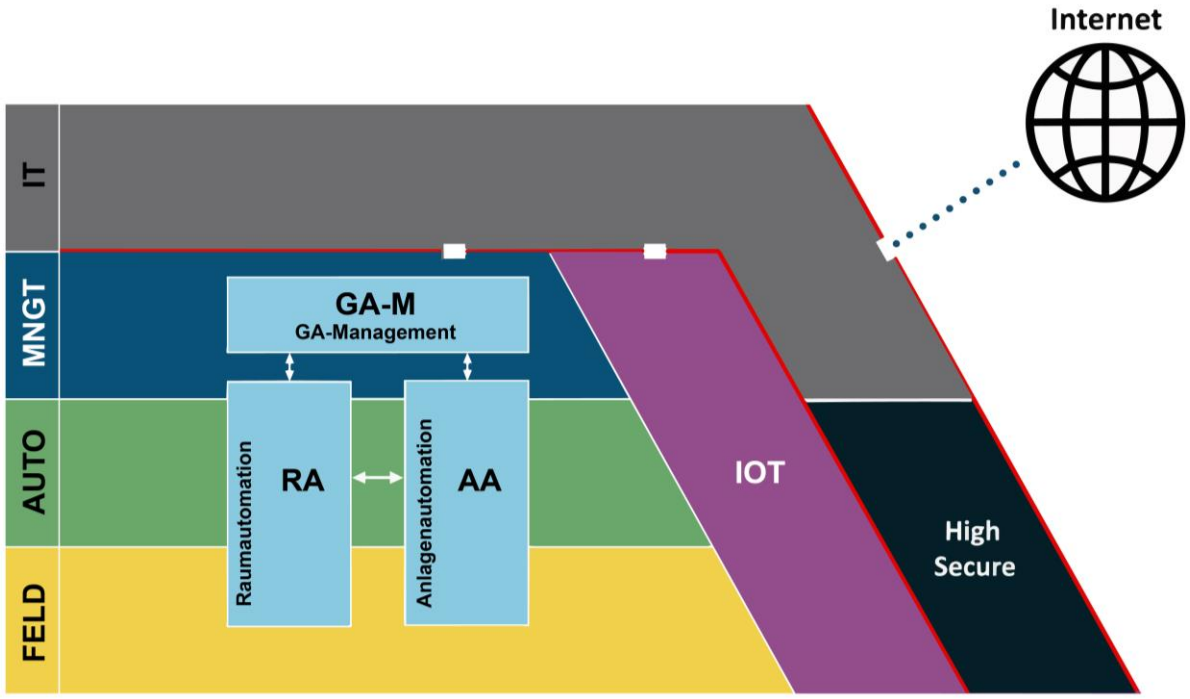


Abb. 9: Automationspyramide nach AMEV-Empfehlung 169 / Gebäudeautomation

Informationstechnologie (IT): Unter anderem sind Komponenten zu betrachten, die innerhalb der GA zu den operativen Technologien (OT) gehören und gemanagt werden. Darunter zählen Zentrale IT/OT-Firewall / DMZ-Router, Managed Core- & Distribution-Switche, Zentrale Netzwerkdienste (DHCP / DNS / NTP)

Managementebene (MNGT): U.a. Managementbedienebene (BMS / SCADA), Energiemanagementsysteme (EMS), Fernzugriff / Remote Access (VPN-Gateway)

Automationsebene (AUTO): U.a. Automationseinrichtung (veraltet DDC / VDI 3814 Blatt 1), Automationsschwerpunkt (ASP), Gateways

Feldebene (FELD): U.a. Pumpen, Ventile, Beschattung

Eine exemplarische Auflistung zur Herangehensweise an die erwähnten typischen Betrachtungsgegenstände finden sich in Anhang B – Beispiele Betrachtungsgegenstände.

Ein Betrachtungsgegenstand enthält in der Regel kommunikative Schnittstellen zum Steuern, Konfigurieren oder Auslesen und ist gemäß seinem funktionalen Einsatz in der für ihn bestimmten Schutzzone zu behandeln.

Schutzzonen in Unternehmen (gemäß dem BSI IT-Grundschutz) orientieren sich nach der Kritikalität des jeweiligen Prozesses, in denen die jeweiligen Assets im technischen Facility Management zugeordnet sind.

Es empfiehlt sich innerhalb eines OT-Netzes je nach Schutzbedarf eine entsprechende Standardisierung abzuleiten.

Der Leitfaden gibt in den folgenden „Rollen-Karten“ eine Anleitung zur Projektabwicklung angelehnt an die Lebenszyklusphasen 1-3 sowie 7 der GEFMA 100-2, bzw. den jeweiligen Leistungsphasen der HOAI.

Die Karten orientieren sich nach den definierten vier Rollen in der „INF.14 Gebäudeautomation“.

Diese ergeben eine Übersicht, in welcher Leistungsphase des Planungs- und 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.

Genauer spezifizierte Rollenanforderungen sind in eckigen Klammern [xx] ergänzt.

Zur vereinfachten Anwendung der Rollenkarten wurden Diese mit der Expertise und Erfahrung beteiligter Anwender um „Best Practice – Karten“ ergänzt.

Übersicht der zur Verfügung gestellten Karten:

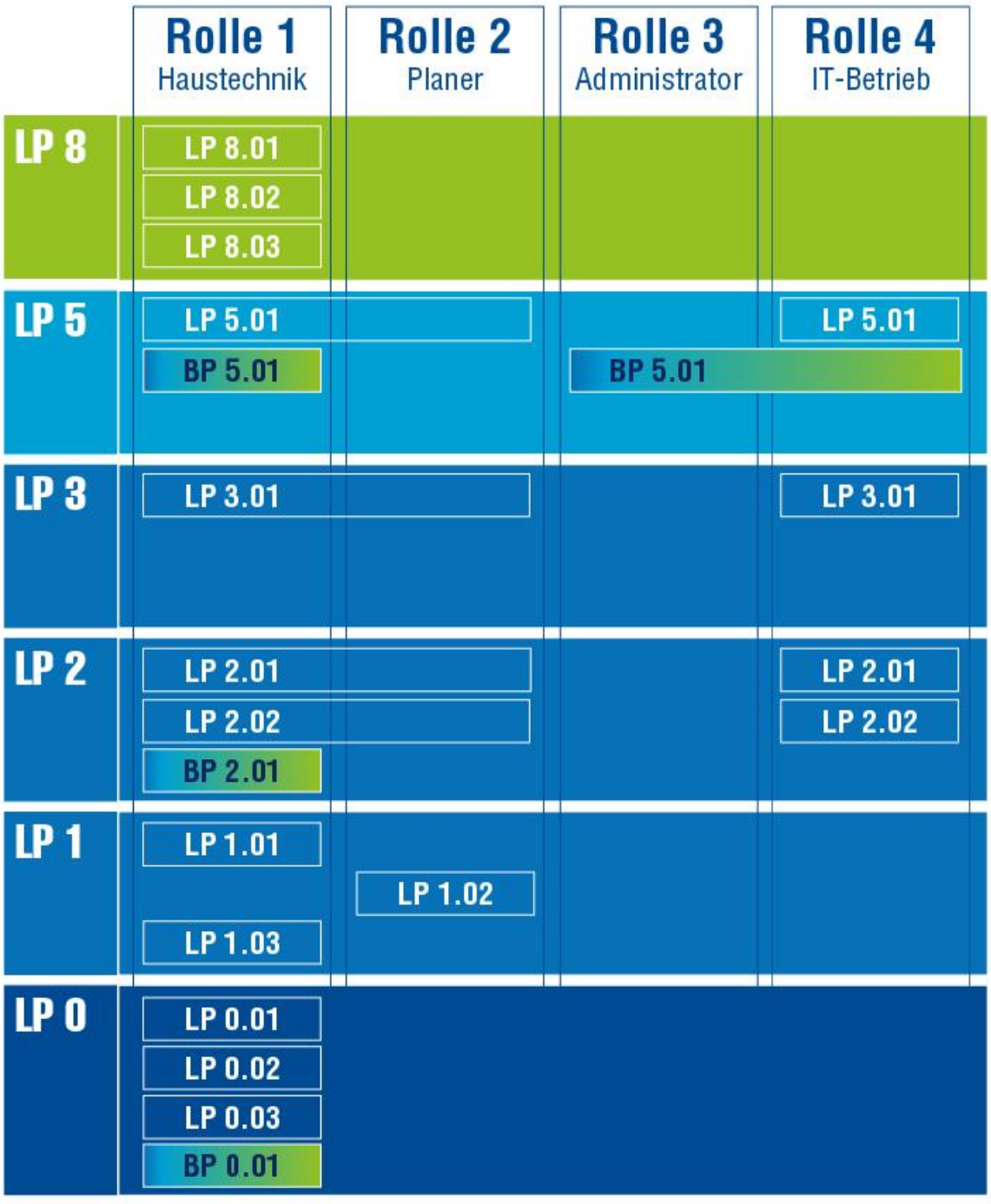


Abb. 10: Übersicht der Rollenkarten

LP 0: Bedarfsplanung (Betriebskonzept)

Die Bedarfsplanung einschließlich der IT/OT-RMP-Betriebskonzepte spielen eine elementare Rolle für den effizienten, wirtschaftlichen und sicheren Gebäudebetrieb. Mit Blick auf den iterativen Planungsprozess ist bis in die LP 3 die Bedarfsplanung fortzuschreiben (Vergleiche DIN 18205 - Bedarfsplanung im Bauwesen). 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),

Bei der Planung und Errichtung von GA-S sind Bezüge zu personenbezogenen Daten zwingend zu vermeiden, ansonsten sind die Anforderungen der DSGVO zu beachten. 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 #GModG

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:
- Gebäudemodernisierungsgesetz (GModG)
- DIN / TS 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
- VDI 6039: 2011 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]

BP 0.01 (Best Practice) (gemäß Checkliste Anhang A)

Kartenthema: Informations-Sicherheitsmanagement & Analyse der Betroffenheit

Schlagworte:
#Überblick #Betroffenheit #Scope #Kernprozesse #Risiko #ZÜS #Management-Verantwortung #Informationssicherheitsbeauftragte #Top-Down #Ressourcen #Sicherheitsziele #Sicherheitsstrategie

Kurzbeschreibung:
Zu Beginn jeder Maßnahme sollte jeder Verantwortliche seine Betroffenheit und Betreiberpflichten zu den verschiedenen Regulierungen analysieren. Daraus ergibt sich der Scope sowie die Notwendigkeit, Risiken und deren Auswirkungen im eigenen beruflichen Umfeld zu erkennen und zu minimieren. Grundvoraussetzung für die Durchführung des Risiko-Management-Prozesses (RMP) ist die Übernahme der Gesamtverantwortung für die Informationssicherheit durch die Geschäfts- bzw. Institutsleitung. Diese übergeordnete Rolle muss den gesamten RMP initiieren, steuern und kontrollieren. Diese Verantwortung muss von allen Beteiligten deutlich erkennbar sein.

Verweise:
- TÜV Verband: Whitepaper Cybersicherheit in der TGA vernetzter Gebäude
- ISACA: Cyber-Sicherheits-Check OT (Seite 1 - 33)
- TÜV-Verband: Beschlüsse der EK ZÜS
- BSI: Entscheidungsbaum der NIS-2-Betroffenheitsprüfung
- BSI: IT Grundschutz ISMS.1

Zielstellung:
In jeder Institution
muss das Bewusstsein entwickelt werden, dass die systematischen Sicherheitsprozesse im Rahmen eines RMP von oben nach unten (Top-Down) durch alle hierarchischen Instanzen getragen werden müssen. Das Initial MUSS durch die Geschäfts- bzw. Institutsleitung erfolgen, welche die strategischen Ziele festlegt, um den Sicherheitsmanagementprozess mit allen Beteiligten erfolgreich umzusetzen. Zudem müssen ausreichende Ressourcen zur Verfügung gestellt werden, die für die Umsetzung der Sicherheitsmaßnahmen benötigt werden.

Folgende Fragestellungen sind geklärt und tabellarisch gelistet:
• Welche Richtlinien, Empfehlungen und gesetzliche Vorgaben kommen bei mir zum Zuge?
• Habe ich schützenswerte Kernprozesse (Kronjuwelen)?
• Habe ich eine direkte oder auch indirekte Gefahrenlage u.a. als Kollateralschaden?
• Wer ist der „Kümmerer“ meines Netzes für operative Technologien (OT)?

Rolle:
Management u.a. Leitung Institution, COO, ISB und BCM

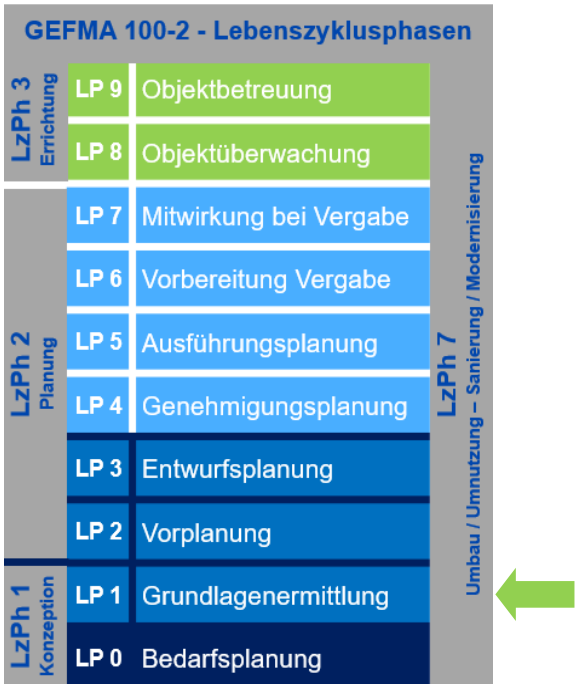
Mit Zuarbeit:
Rolle 1 [Investor / Auftraggeber]
Rolle 1 [GA-Betrieb/Systemeigner]

LP 1: Grundlagenermittlung (Projektvorbereitung)

Im Abschnitt LP 0 wird mit Blick auf den iterativen Planungsprozess bis in die LP 3 der Bedarfsplanungsprozess beschrieben. Diese Aufgaben sind weitgehend dem künftigen Nutzer und Betreiber (Rolle 1) zuzuordnen.

In den folgenden Abschnitten LP 1-3 werden die besonderen Leistungen der Fachplaner (Rolle 2) zum IT/OT RMP parallel zu den Grundleistungen der HOAI für TGA der Anlagengruppe 1-8 schrittweise beschrieben. Die Zugehörigen Karten geben dazu im Rollenkontext (Rollen 1-4) konkrete Aufgabenverteilungen und -beschreibungen.

Im Fokus der LP 1 liegt dabei zunächst die Vorstellung und Abstimmungen zur Besetzung der Rollenverteilung, die Betroffenheitsanalyse, der Festlegung des Planungs- / Projektumfang, die Einarbeitung in IT/OT Unternehmensstandards bzw. IT-Governance. Hier ist ein Abgleich mit nationalen Vornormen, insbesondere aktuelle Anforderungen aus der Europäischen Union (EU) vorzunehmen.



<u>Was ist zu tun:</u> Kick-off IT/OT-Risiko-Management-Prozess (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.

   Zielstellung: Klare Zuordnung der Verantwortungsbereiche, Aufgaben und 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
- Technisches Regelwerk VDI 3814 – Blatt 4.2: Gebäudeautomation (GA) – Methoden und Arbeitsmittel für Planung, Ausführung und Übergabe (inkl. Checklisten)

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 [OT-Betrieb

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:

- BSI: INF.5: Raum sowie Schrank für technische Infrastruktur
- BSI: INF.14 Gebäudeautomation
- Technisches Regelwerk VDI 3814 – Blätter 1/2.1/2.2/2.3/4.2
- BACnet Interest Group Europe (BIG-EU): BACnet - Project Adress Table (B-PAT)

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-Dienstleister

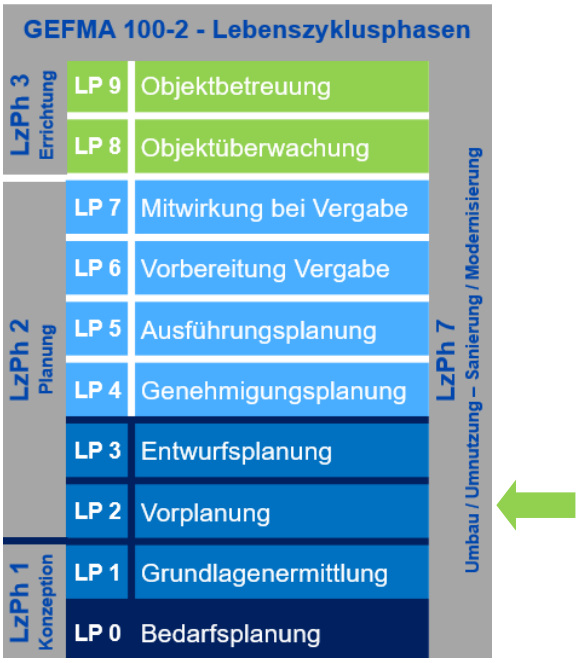
Rolle:
Rolle 1 [GA-Betrieb/Systemeigner]

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

LP 2: Vorplanung

In der LP 1 lag der Fokus auf Vorstellung und Abstimmungen zur Besetzung der Rollenverteilung, die Betroffenheitsanalyse, der Festlegung des Planungs- / Projektumfang, Einarbeitung in IT/OT Unternehmensstandards / IT-Governance. Hier ist ein Abgleich mit nationalen Vornormen, insbesondere aktuelle Anforderungen aus der Europäischen Union (EU) vorzunehmen.

Der fachliche Beginn des IT/OT RMP erfolgt ab der LP 2. Zunächst steht die Identifizierung der Untersuchungsgegenstände und der Abgleich zur Bedarfsplanung sowie Schutzbedarfs-, Schwachstellen- und Strukturanalyse für alle GA-relevanten Systeme und Netze an.



<u>Was ist zu tun:</u> Initiierung und Mitwirken beim IT/OT RMP

- Die **Konzeption**, Erstellung, Entwicklung von IT-Lösungen gemäß IT/OT Unternehmensstandards
- Koordinierung des IT/OT-RMP durch den Integrationsplaner
- Erarbeitung von Vorgaben für andere Fachplaner TGA

Verantwortung: GA/Integrationsplaner
Beratung durch IT/OT Sicherheitsmanagement

LP 2.01 (gemäß Checkliste Anhang A)

Kartenthema: Strukturanalyse

Schlagworte:
#Informationsverbund, #IT-Systeme, #OT-Systeme, #Anwendungen, #Netzplan, #Räume, #Gruppenbildung

Kurzbeschreibung:
Systematische Erfassung, Inventarisierung und Dokumentation aller Bestandteile des Informationsverbundes – einschließlich Anwendungen, IT- und OT-Systemen, Netzinfrastrukturen sowie Räumlichkeiten im Zusammenspiel mit den Geschäftsprozessen als unverzichtbare Grundlage für die nachfolgende Schutzbedarfsfeststellung.

Verweise:
- BSI-Standard 200-2 (Kapitel 8.1: IT-Strukturanalyse)
- DIN EN ISO/IEC 27001
- VDI/VDE 2182 Blatt 1

Zielstellung:
Vollständige und strukturierte Modellierung und Inventarisierung aller relevanten Komponenten des Informationsverbundes (Hardware, Software, Netze, Räume, Gebäude und Schnittstellen).

Kernfragen zur Klärung:
1. Welche Anwendungen, IT/OT-Systeme, Netze und Räume gehören zum definierten Informationsverbund?
2. Wie sind die Systeme untereinander vernetzt und welche externen/internen Schnittstellen liegen vor?
3. Können gleichartige Systeme oder Anwendungen (Betrachtungsgegenstände) zur Komplexitätsreduktion sinnvoll zusammengefasst werden (Gruppenbildung)?

Rolle:
Rolle 1 [Systemeigner / Bauherr] - Bereitstellung der Systemdokumentation, Abgrenzung des Informationsverbundes, strukturierte Asset-Aufnahme und Gruppenbildung OT

Rolle 2 [Planer]: - Netzwerkpläne, Topologien, Raumpläne und Anwendungsbeziehungen sowie Unterstützung bei der Gruppenbildung

Rolle 4 [IT-Betrieb / Informationssicherheitsbeauftragter] - Gruppenbildung IT

LP 2.02 (gemäß Checkliste Anhang A)

Kartenthema: Schutzbedarfsfeststellung

Schlagworte:
#Schutzbedarfsfeststellung, #Schutzziele, #Verfügbarkeit, #Integrität, #Vertrauligkeit, #Schadensszenarien, #Kernabsicherung, #kritische Assets (Kronjuwelen)

Kurzbeschreibung:
Systematische Ermittlung und Zuordnung des Schutzbedarfs (z.B. normal, hoch, sehr hoch) für die identifizierten Geschäftsprozesse, in Verbindung mit den dabei verarbeiteten Informationen und den eingesetzten GA-Komponenten und Netzen in den drei Grundwerten Verfügbarkeit, Integrität und Vertraulichkeit, anhand realistischer Schadensszenarien.

Verweise:
- BSI-Standard 200-2 (Kapitel 8.2: Schutzbedarfsfeststellung)
- BSI INF.14
- DIN EN ISO/IEC 27005
- VDI/VDE 2182 Blatt 1

Zielstellung:
Klassifizierung aller GA-Subsysteme, um den notwendigen Aufwand für spätere Sicherheitsmaßnahmen (LPH 3/5) wirtschaftlich und risikogerecht zu dimensionieren.

Kernfragen zur Klärung:
1. Welche konkreten Auswirkungen (z.B. finanzielle Schäden, Personenschäden, Reputationsverlust) entstehen bei einem Ausfall oder einer Manipulation der GA-Komponenten?
2. Welches Schutzziel besitzt im konkreten Gewerk (z.B. Kälteerzeugung vs. Einzelraumregelung) die höchste Priorität?
3. Liegen kumulierte Effekte vor (z.B. Verknüpfung mehrerer eigentlich unkritischer Systeme zu einer kritischen Gesamtkette)?

Rolle:
Rolle 1 [Systemeigner/Bauherr] – Definition der Akzeptanzkriterien für Schäden & finale Freigabe der Einstufung

Rolle 2 [Planer / Integrationsplaner TGA] – Identifikation der technischen Abhängigkeiten und funktionale Beschreibung der Schadensfolgen

Rolle 4 [IT-Betrieb / Informationssicherheitsbeauftragter] – Methodische Führung der Feststellung, Plausibilitätsprüfung & Dokumentation nach BSI-Vorgaben

BP 2.01 (Best Practice) (gemäß Checkliste Anhang A)

Kartenthema: Kommunikation GA-Bestand

Schlagworte:
#GA-Netzwerk #BACnet/IP #TCP/IP #BACnet/SC-Router #BACnet/SC Hub #BACnet-Node #BBMD

Kurzbeschreibung:
Die BACnet-Kommunikation bestehender GA-Netzwerke kann durch den Einsatz von BACnet/SC sicher verschlüsselt (TLS 1.3) werden. Hierzu wird mindestens ein BACnet/SC-Hub benötigt. Die Hub-Funktion kann Bestandteil eines BACnet-Routers sein, sie kann jedoch ebenso in jedem anderen BACnet/SC-fähigen Gerät implementiert werden. Ein BACnet-Router ist nur erforderlich, wenn BACnet/SC mit anderen BACnet-Datalinks, beispielsweise BACnet/IP oder BACnet MS/TP, verbunden werden soll. In reinen BACnet/SC-Netzwerken ist kein Router erforderlich. Der Einsatz von BACnet Broadcast Management Devices (BBMD) entfällt. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) arbeitet derzeit daran, BACnet/SC als sicheres Übertragungsprotokoll in seine Empfehlungen für die Gebäudeautomation aufzunehmen.

Verweise:
BSI: IT Grundschutz INF14.M12 Nutzung sicherer Übertragungsprotokolle für die GA

Zielstellung:
Für GA-Betreiber mehrere Gebäude oder Liegenschaften soll eine Lösung angeboten werden, die Kommunikation über das sichere Protokoll BACnet/SC für gegebene IT.Infrastrukturen (Backbone) zu ertüchtigen, ohne den Bestand zu ersetzen. Daraus ergeben sich folgende Vorteile:

- Geringerer Planungsaufwand und geringere Planungskosten
- Geringerer Investitionsaufwand
- Durch die Kommunikation über TCP/IP entfallen die BBMD aus BACnet-Netzwerken. Dadurch entstehen einfache Netzwerkstrukturen.

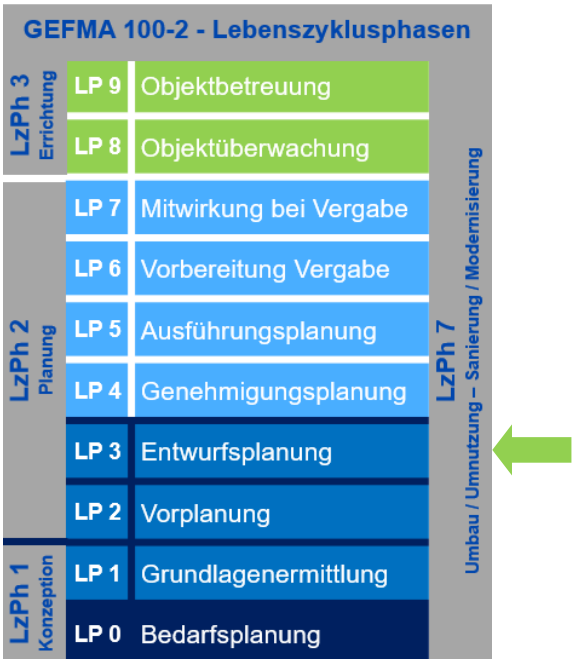
Rolle:

Rolle 1 [GA-Betrieb/Systemeigner]

LP 3: Entwurfsplanung

Nach der Identifizierung der Untersuchungsgegenstände sowie der Schutzbedarfs- und Schwachstellenanalyse in der LP 2 werden in der LP3 bereits:

- Netzwerk- und Systemarchitektur konzipiert
- Rollen- und Berechtigungskonzepte geschrieben
- vorgesehene Untersuchungsgegenstände verifiziert (siehe auch Anhang B – Beispiele Betrachtungsgegenstände)
- die Schutzbedarfsmaßnahmen in das GA-Gesamtkonzept integriert



<u>Was ist zu tun:</u> Festlegung des Schutzbedarfs anhand des IT/OT-RMP

- Der **Systemeigner** legt anhand der **Anforderungen** an den Schutzbedarf fest, wie schützenswert die jeweiligen **Informationen/Funktionen/Assets** in Bezug auf deren Verfügbarkeit, Integrität und Vertraulichkeit sind.
- Basierend auf dieser Einstufung wird im Rahmen des IT/OT-Risikomanagementprozesses bewertet, ob die **Informationen/Funktionen/Assets** sicher verarbeitet/(produzieren) werden können, bzw. das Vorhaben sicher umgesetzt werden kann.

Verantwortung: Systemeigner und IT/OT-Sicherheitsmanagement

LP 3.01 (gemäß Checkliste Anhang A)

Kartenthema: Schutzbedarfsfestlegung

Schlagworte:
#Modellierung, #Informationsverbund, #Strukturanalyse, #GA-Komponenten, #Netzplan, #Zielobjekte, #Gewerkeabgrenzung, #Asset

Kurzbeschreibung:
Strukturierte Erfassung und Modellierung aller Assets, Komponenten, Systeme, Netze und Schnittstellen der Gebäudeautomation (GA) in ein konsistentes Modell (Informationsverbund) mithilfe der vorhandenen Bausteine aus dem BSI-Grundschutzkompendium als essenzielle Basis für die anschließende Risikoanalyse und Maßnahmenzuordnung.

Verweise:
- BSI-Standard 200-2 (Kapitel 8.3: Modellierung des Informationsverbunds)
- BSI IT-Grundschutz-Bausteine
- DIN EN ISO/IEC 27001 / ISO 27005
- VDI/VDE 2182 Blatt 1 (IT-Sicherheit in der Industriellen Automation)

Zielstellung:
Vollständige und überschneidungsfreie Abbildung der GA-Topologie (Feldebene, Automationsebene, Managementebene) und deren logischer/physikalischer Verbindungen, um Sicherheitszonen sachgerecht abzugrenzen und Schutzbedarfe präzise den jeweiligen Zielobjekten zuzuordnen.

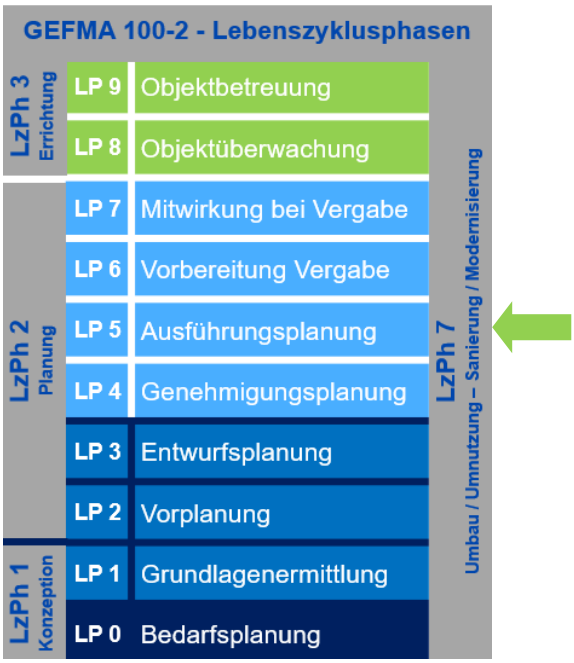
Kernfragen zur Klärung:
1. Welche GA-Komponenten (Automationseinrichtungen, Sensoren/Aktoren, BACnet-Router, BMS-Server, IoT-Gateways) gehören exakt zum gemeinsamen Betrachtungsbereich?
2. Wie verlaufen die Schnittstellen und Kommunikationsbeziehungen zwischen GA-Netzen (OT) und dem übergeordneten Korporativ-Netzwerk (IT) bzw. externen Dienstleister-Zugängen?
3. Lassen sich gleichartige Komponenten (z. B. Raumbediengeräte gleicher Baureihe) zu repräsentativen Gruppen/Zielobjekten zusammenfassen, um die Modellierung effizient zu gestalten?

Rolle:
Rolle 1 [Systemeigner/Bauherr]
Rolle 2 [Planer / Integrationsplaner TGA]
Rolle 4 [IT-Betrieb / Informationssicherheitsbeauftragter]

LP 5: Ausführungsplanung

Das Bau Soll und somit alle IT/OT Anforderungen sind mit der Entwurfsplanung der LP 3 abgeschlossen. Hierbei gilt ein „Redaktionsschluss“

In der anstehenden Ausführungsplanung erfolgt die Ausarbeitung für eine ausschreibungsreife in der Regel produktneutrale Baubeschreibung. In der IT/OT Sicherheit können Aufgrund des Schutzbedarfes im Rahmen von Präqualifizierungen konkrete Produkte einschließlich Vorgaben zur Härtung festgelegt werden.



<u>Was ist zu tun:</u> Ermittlung der IT/OT-Sicherheitsanforderungen und Bewertung der potenziellen IT/OT-Risiken.

- **Gemeinsame Gestaltung, mit allen fachlich an der Planung Beteiligten**, mit Ziel einer sicheren und gesicherten Kommunikation zwischen den Systemen/Anlagen, technischen Einrichtungen für alle Gewerke und deren IT/OT-Asset.
- Untersuchung und Festlegung der erforderlichen Lösungen
- Dokumentation zur Lösung der avisierten Architektur (LAD),
- Fortschreibung/ Weiterentwicklung von IT/OT-Lösungen (ggf. Standardisierung).

Verantwortung: IT-Sicherheitsmanagement und Produktionsverantwortliche Stelle

LP 5.01
(gemäß Checkliste Anhang A)

Kartenthema:
IT/OT-Netzwerktopologie, Segmentierung, Spezifikation (Festlegung der Schutzmaßnahmen)

Schlagworte:
#Netzwerksegmentierung, #BACnet_SC, #Systemhärtung, #Firewallregeln, #Fernwartungskonzept

Kurzbeschreibung:
Erstellung ausführungsreifer Pläne, Schemata und technischer Vorgaben zur physischen und logischen IT/OT-Sicherheit der Gebäudeautomation. Übersetzung der Schutzbedarfsfestlegung und des Grundschutz-Sicherheitskonzepts (LPH 3/4) in konkrete Spezifikationen (wie z.B. Systemhärtung) und Festlegung von Prüf- und Abnahmekriterien aller Betrachtungsgegenstände.

Verweise:
- BSI-Standard 200-2, INF.14, INF.13, IND.1, OPS.1.2.5,
- DIN EN ISO/IEC 27001
- IEC 62443-3-3
- VDI 3814
- VDI/VDE 2182 Blatt 1

Zielstellung:
Vollständige und strukturierte Modellierung und Dokumentation aller relevanten Komponenten des Informationsverbundes (Hardware, Software, Netze, Räume, Gebäude und Schnittstellen).

Kernfragen zur Klärung:
1. Welche Anwendungen, IT/OT-Systeme, Netze und Räume gehören zum definierten Informationsverbund?
2. Wie sind die Systeme untereinander vernetzt und welche externen/internen Schnittstellen liegen vor?

Rolle:
Rolle 1 [Systemeigner / Bauherr]
Rolle 2 [Planer]
Rolle 4 [IT-Betrieb / Informationssicherheitsbeauftragter]

BP 5.01 (Best Practice) (gemäß Checkliste Anhang A)

Kartenthema: Zertifikate & Verschlüsselung

Schlagworte:
#Vertrauenswürdige CA #Zertifikatsmanagement #X509-Zertifikate#PKI

Kurzbeschreibung:
Planung Sicherheitskonzept für cybersicheren Betrieb und Inbetriebnahme. Beinhaltet u.a.:

- Erstellung-, Verteilung- und Verwaltung digitaler X.509v3 Zertifikate und sonstiger weiterer Anmeldedaten mit möglichst einheitlichem Verfahren über alle OT-Geräte hinweg
- Festlegung der Workflows für eine eigenhoheitliche, zentrale Handhabung dieser Zertifikate (typischerweise über eine kundenseitige PKI) im gesamten Lebenszyklus und Festlegung der Verantwortlichkeiten.

Für effiziente und sichere Abläufe müssen die entsprechenden Zertifikatsprozesse zumindest in der Betriebsphase vollautomatisiert ablaufen. Handbetrieb ist maximal für das initiale "bootstrapping" der Vertrauensbeziehungen im Projekt zulässig, sollte aber auch dort konzeptionell möglichst auf ein Minimum beschränkt werden.

Hinweis:
Das Bundesamt für Bauwesen und Raumordnung (BBR) erstellt aktuell im Rahmen seines Forschungsprojektes "BACnet Secure Connect - Weiterentwicklung und Handling für kritische Infrastruktur" in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und der BIG-EU einen entsprechenden Leitfaden, der für BACnet/SC Handreichung bieten wird.
Inhaltlich wird dieser Leitfaden voraussichtlich folgende Durchführungsmöglichkeiten für den Zertifikatsaustausch unterstützen:

- Verwendung der BACnet-Mechanismen aus Rev. 24. Dies entweder über eine direkte Unterstützung einer BACnet-fähigen CA oder durch Verwendung eines entsprechenden BACnet-fähigen Protokollgateways
- Verwendung des EST-Protokolls gemäß RFC 7030. Dies für eine direkte Anbindung an einen EST-Server der IT-seitigen PKI. Generell nutzbar nicht nur für BACnet/SC Zertifikate; für EST-unterstützende BACnet-Geräte unabhängig von der BACnet Revision

Steht keine eigene PKI zur Verfügung, können für die initiale Erstellung von sicheren Zertifikaten auch kostenfreie Tools genutzt werden. Die BACnet International (BI) stellt dazu einen BACCARI-Server als BACnet-fähige CA zur Verfügung. Hinweis: CA-Software wird seitens CRA als "Class I"-Produkte eingestuft und benötigt somit zukünftig eine explizite Zertifizierung zur Verwendung.

Verweise:

- VDMA EB 24186:2024 / VDMA 24774:2023-03
- Public-Key-Infrastruktur (PKI)
- BACnet International (BI): BACCARI-Server
- Bundesamt für Bauwesen und Raumordnung (BBR): „Leitfaden für den Betrieb und Zertifikats-Workflow mit BACnet/SC“ (in Erarbeitung)

Zielstellung:

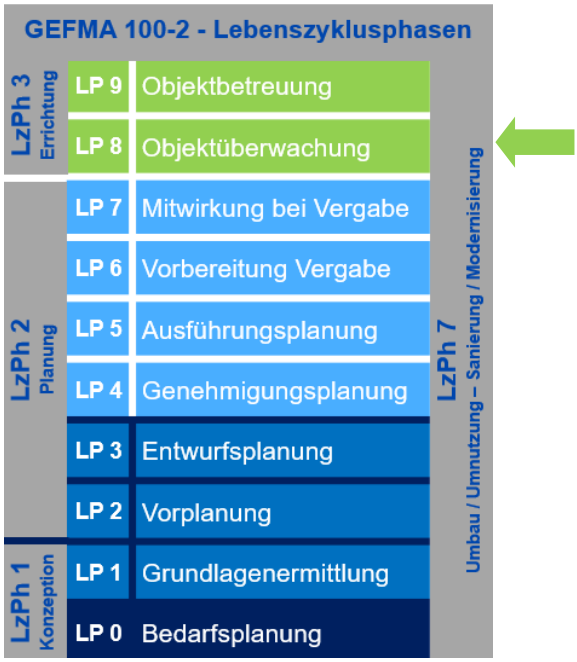
- Der regelmäßige Austausch von Zertifikaten muss in die Betriebsprozesse des Systemeigners mit aufgenommen werden.
- Eine sichere Kommunikation entsteht u.a. auch durch die Nutzung sicherer Zertifikate mit einer sinnvoll begrenzten Gültigkeitsdauer. Zertifikate mit einer unbegrenzten Gültigkeitsdauer oder Zertifikate mit einer abgelaufenen Gültigkeit stehen im Widerspruch zu einer sicheren Kommunikation.

Rolle:
Rolle 1 [GA-Betrieb/Systemeigner]
Rolle 3 [GA-Administrator]
Rolle 4 [IT-Betrieb]

LP 8: Objektüberwachung

Nach der Ausschreibung ist die Ausführungsplanung als Werks- und Montageplanung vom Systemintegrator fortzuschreibend und durch den Planer auf Übereistimmung mit dem Planung Soll bzw. den Vorgaben der IT/OT-Sicherheit und Abstimmung im IT/OT-RMP aus den vorangegangenen Phasen freizugeben.

Danach folgt die Überwachung der Bauausführungen.



<u>Was ist zu tun:</u> Die Überwachung der Bauausführung, die Inbetriebnahme und Abnahme

LP 8.01 (gemäß Checkliste Anhang A)

Kartenthema: Inbetriebnahmemanagement

Schlagworte:
#Inbetriebnahmemanagement, #Schnittstellenmanagement, #Notfallplanung #Prüfplan

Kurzbeschreibung:
Aufgrund der steigenden Komplexität der Anlagen in den Gebäuden muss die Inbetriebnahme gewerkeübergreifend erfolgen. Dabei müssen Wechselwirkungen und Abhängigkeiten zwischen den technischen Anlagen, GA-Komponenten berücksichtigt werden. Anhand eines Prüfplans werden die Inbetriebnahmereihenfolge und die jeweiligen Prüfungen sowie die Reihenfolge der Anbindung an das GA-System festgelegt. Nach Abschluss der Inbetriebnahmephase und der Überführung der Anlagen in den bestimmungsgemäßen Betrieb, müssen Zugänge, Konten für den Zugriff von Dritten während der Inbetriebnahme gelöscht werden.

Verweise:
- BSI IT-Grundschutz
- AMEV TMon
- VDI 6039

Zielstellung:
Das Inbetriebnahmemanagement soll sicherstellen, dass alle Systeme und Prozesse fehlerfrei und effizient funktionieren, um diese in den bestimmungsgemäßen Betrieb zu überführen. Es dient darüber hinaus zur Qualitätssicherung und sorgt dafür, dass die Sicherheitsmaßnahmen unter Einhaltung der Service- und Wartungspläne wirksam bleiben.

Rolle:
Rolle 1 [OT-Betrieb / Dienstleister & Errichter]

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

LP 8.02
(gemäß Checkliste Anhang A)

Kartenthema:
Funktionstests

Schlagworte:
#Penetrationstests, #Validierung, #Testprotokolle

Kurzbeschreibung:
Durchführung erstmaliger und regelmäßiger Funktionstests zur Validierung der Sicherheitsmaßnahmen. Die Testergebnisse werden dokumentiert, um die Funktionsfähigkeit und Sicherheit der Systeme nachzuweisen.

Verweise:
- BSI IT-Grundschutz
- VDMA 24774

Zielstellung:
Die Funktionstests gewährleisten, dass alle Sicherheitsmaßnahmen korrekt implementiert sind und die Systeme zuverlässig funktionieren. Die Dokumentation der Tests schafft Nachvollziehbarkeit und Transparenz.

Rolle:
Rolle 1 [GA-Betrieb/Systemeigner]

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

LP 8.03
(gemäß Checkliste Anhang A)

Kartenthema:
Backup & Restore

Schlagworte:
#Backups, #Datenverschlüsselung, #Restore-Tests

Kurzbeschreibung:
Erstmalige und regelmäßige Sicherung der Systemdaten und deren Verschlüsselung, um die Verfügbarkeit und Integrität der Daten sicherzustellen. Backups werden überprüft und getestet, um ihre Wiederherstellbarkeit zu gewährleisten.

Verweise:
- BSI IT-Grundschutz
- VDMA 24774

Zielstellung:
Durch regelmäßige Backups und Integritätsprüfungen wird sichergestellt, dass wichtige Daten bei einem Ausfall oder Angriff schnell und zuverlässig wiederhergestellt werden können.

Rolle:
Rolle 1 [GA-Betrieb/Systemeigner]

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

Auf einen Blick

Die im Leitfaden vorgeschlagenen Schritte zu mehr Cybersicherheit in der Gebäudeautomation finden sie, für einen besseren Überblick, stichpunktartig auf einem Plakat zusammengefasst. Dieses können sie sich hier herunterladen und bei Bedarf im DIN A2 Format zur Verfügung stellen.

Abbildungsverzeichnis

Glossar

Asset (Technisches Facility Management):
Ein Asset ist eine bauliche oder technische Anlage, Ausrüstung oder Einrichtung, die im Rahmen des Facility Managements betrieben, gewartet oder verwaltet wird, z. B. Gebäude, Aufzüge, Gebäudeautomationssysteme, Heizungs-, Klima-, Lüftungs- und Sanitäranlagen oder Sicherheitssysteme.

Act: Europäische **Verordnungen** wirken direkt auf alle EU-Mitgliedstaaten. Verordnungen sind Rechtsakte, die in allen ihren Teilen verbindlich sind. Sie gelten bei Inkrafttreten automatisch und in einheitlicher Weise in allen EU-Ländern, ohne dass sie in einzelstaatliches Recht umgesetzt werden müssen.

Directive: Europäische **Richtlinien** sind von den EU-Mitgliedstaaten in nationales Recht umzusetzen. Richtlinien geben den EU-Ländern ein bestimmtes Ziel vor, stellen ihnen jedoch frei, wie sie dieses verwirklichen. Die Umsetzung in nationales Recht muss innerhalb der Frist erfolgen, die in der Richtlinie festgelegt wurde (normalerweise zwei Jahre).

SHT ist der Überbegriff für alle technischen Schutzmaßnahmen (umfasst Safety & Security) | Brandmeldeanlage, Zutrittskontrolle, Videoüberwachung, Not-Aus-Schalter | VdS, DIN, EN, TRBS, ... |

Safety ist die funktionale Sicherheit (Schutz vor unbeabsichtigten Gefahren, technische Defekten oder Bedienfehler) | Not-Aus, Schutzgitter, Überdruckventil | TRBS 1115-1, EN ISO 13849, ... |

Security (als Gegenstück zu Safety) meint den Schutz vor absichtlichen Angriffen (z. B. Einbruch, Sabotage).

Hinweis: Folgeversionen in Arbeit

Die Neuausgabe des Leitfadens ist eine Weiterentwicklung von Rollenkarten und Best Practice - Karten mit dem Schwerpunkt in den Leistungsphasen 2 – 5 und orientiert sich an etablierten Methoden aus Deutschland. In der nächsten Ausgabe sind Ergänzungen für die Leistungsphase 8 und dem Regelbetrieb geplant.

Relevante neu veröffentlichte Zusammenstellungen notwendiger Empfehlungen, Richtlinien und Prozesse sind fortlaufend in Arbeit und werden in aktualisierten 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) u.a. mit Zuarbeit umfangreicher Expertise durch die Deutsche Bundesbank, der TU Braunschweig und der Deutschen Flugsicherung

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

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
BP 0.01	**Informations-Sicherheitsmanagement & Analyse der Betroffenheit**	**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
LP 2: Vorplanung			
LP 2.01	Strukturanalyse	ja	nein
LP 2.02	Schutzbedarfsfeststellung	ja	nein
BP 2.01	**Kommunikation GA-Bestand**	**ja**	**nein**
LP 3: Entwurfsplanung			
LP 3.01	Schutzbedarfsfeststellung	ja	nein
LP 5: Ausführungsplanung			
LP 5.01	IT/OT-Netzwerktopologie, Segmentierung, Spezifikation	ja	nein
BP 5.01	**Zertifikate & Verschlüsselung**	**ja**	**nein**
LP 8: Objektüberwachung			
LP 8.01	Inbetriebnahmemanagement	ja	nein
LP 8.02	Funktionstests	ja	nein
LP 8.03	Backup & Restore	ja	nein

Anhang B: Beispiele Betrachtungsgegenstände

Betrachtungsgegenstand	Funktionen	Schnittstellen	Datenflüsse	Sicherheitsrisiken
Informationstechnologie (IT)				
Zentrale IT/OT-Firewall / DMZ-Router	Strikte Segmentierung zwischen Office-IT, Internet und GA-OT; Deep Packet Inspection (DPI) für GA-Protokolle	RJ45/SFP+ (Ethernet), IPsec-Tunnel, Management-Konsole (HTTPS/SSH)	Filterung des gesamten Nord-Süd-Verkehrs (z.B. MBE-Zugriffe, Externe Cloud-Dienste); Blockieren unerlaubter Quer-Kommunikation	Fehlkonfigurationen („Any-Any"-Regeln); Denial-of-Service (DoS), der den Durchsatz lähmt; Ausnutzung von Firmware-Schwachstellen
Managed Core- & Distribution-Switche	Zentrales Routing innerhalb des GA-Backbones, Durchsetzung von VLANs, Port-Security (802.1X), Loop-Protection	Ethernet (Kupfer/Glasfaser), SNMPv3, SSH	Weiterleitung und Priorisierung (QoS) von IP-basierten GA-Datenströmen (BACnet/IP, OPC UA) zwischen den Etagen-Verteilern	Unberechtigtes Aufschalten fremder Geräte an freien Ports; MAC-Flooding; Man-in-the-Middle-Angriffe durch ARP-Spoofing
Zentrale Netzwerk-dienste (DHCP / DNS / NTP)	Automatische IP-Vergabe, Namensauflösung im GA-Netz und Bereitstellung einer synchronen Systemzeit (essentiell für Logfiles/Alarme)	UDP-Ports 53 (DNS), 67/68 (DHCP), 123 (NTP)	Verteilung von Netzwerkkonfigurationen an GA-Komponenten; Beantwortung von Zeit- und Namensanfragen aller IP-Teilnehmer	DNS-Spoofing/Poisoning leitet Datenströme um; NTP-Manipulation verfälscht Zeitstempel von Sicherheits-Logs (Verschleierung von Angriffen); IP-Adress-Erschöpfung (DHCP Starvation)

Betrachtungsgegenstand	Funktionen	Schnittstellen	Datenflüsse	Sicherheitsrisiken
Managementebene (MNGT)				
Management bedienebene (BMS / SCADA)	Zentrales Bedienen und Beobachten, Anlagenübergreifendes Monitoring, Alarm- und Ereignismanagement (Meldung, Quittierung), Erstellung von Trends und Berichten, zentrale Zeitschaltprogrammierung, Benutzer- und Zugriffsverwaltung	Ethernet, Web-Schnittstellen (HTTPS), BACnet/IP, OPC UA, SMTP	Senden von Konfigurationen und Zeitschaltprogrammen an Automationsebene; Empfang von Prozessdaten und Alarmen	Einfallstor für Ransomware über ungesicherte Web-Clients/Office-Netz-Kopplungen; Brute-Force auf Administratoren-Logins; unverschlüsselte Protokolle
Energie Management Systeme (EMS)	Kontinuierliche Verbrauchserfassung, Zählerdatenmanagement, automatische Berichterstellung (KPIs), Lastgang- und Effizienzanalysen, Grenzwertüberwachung für Energieströme, Bereitstellung von Optimierungsvorgaben	REST-API, SQL-Datenbanken, MQTT, AMQP	Export von Verbrauchsdaten an interne IT-Systeme oder externe Cloud-Anbieter	Manipulation historischer Daten führt zu Fehlinterpretationen der Energieeffizienz oder gezieltem Greenwashing
Fernzugriff / Remote Access (VPN-Gateway)	Bereitstellung und Absicherung von Ende-zu-Ende-Verbindungen, Protokollierung von Zugriffen, sichere Benutzerauthentifizierung, Routing und Trennung des externen Datenverkehrs vom lokalen Netzwerk	IPsec / TLS-VPN, LTE/5G-Router, MFA-Schnittstellen	Direkte Tunnelung von externen Systemen (Dienstleister) in die Automations- oder Feldebene zur Fernprogrammierung	Supply-Chain-Angriffe über kompromittierte Laptops externer Techniker; dauerhaft offene und unüberwachte VPN-Verbindungen

Betrachtungsgegenstand	Funktionen	Schnittstellen	Datenflüsse	Sicherheitsrisiken
Automationsebene (AUTO)				
Automations-einrichtung (veraltet DDC), (VDI 3814 Blatt 1)	Steuern, Regeln, Überwachen, Störungsmanagement, Betriebsdatenerfassung.	Physische Schnittstellen (Sensoren/Aktoren), Kommunikative Schnittstellen (Ethernet/GA-Netzwerk (BACnet), Funknetzwerke, Feldbus-Netzwerke), Bediener/Mensch	Intern: Messwerte, Stell- und Steuerbefehle. Extern: Übertragung von Prozessdaten an MBE; Störungsmanagement an MBE; Empfang von Steuerbefehlen und Zeitschalteinträgen von MBE	Manipulation lokaler Regelstrategien führt zu Anlagenausfall, Fehlbedienungen oder Übersteuern von Regelprozessen
Automations-schwerpunkt (ASP)	Physische Aufnahme und Schutz von Automationskomponenten, Spannungsversorgung und Absicherung interner Baugruppen, Strukturierung und Bündelung lokaler Systembusse und Netzwerk-Uplinks	Interne Systembusse, Switch-Uplinks, serielle Kopplungen.	Bündelung und Weiterleitung lokaler Datenströme der angeschlossenen DDC-Komponenten zum Backbone-Netzwerk	Physisches Sabotagerisiko bei unverschlossenen Schaltschränken; Abgreifen des internen Datenverkehrs direkt vor Ort
Gateways	Protokollumsetzung und -übersetzung, Datentyp-Anpassung, Entkopplung unterschiedlicher Bussysteme, Sicherstellung der Interoperabilität zwischen verschiedenen Herstellern und Gewerken.	RS-485 (seriell), RJ45 (Ethernet), KNX-TP, Modbus RTU/TCP, BACnet	Bidirektionale Übersetzung im laufenden Datenfluss (z.B. Modbus-Registerwerte in BACnet-Objekte)	Häufig fehlende Sicherheitsfeatures ('Protokoll-Broker' ohne Filterwirkung); Schwachstellen veralteter Protokolle werden in IP-Netze übertragen

Betrachtungsgegenstand	Funktionen	Schnittstellen	Datenflüsse	Sicherheitsrisiken
Feldebene (FELD)				
Pumpen	Hydraulischer Transport flüssiger Medien, Druckhaltung, volumenstromabhängige Leistungsanpassung (Drehzahlregelung), Energieeffiziente Medienförderung in Heiz- und Kühlkreisläufen	Analoge Signale (0-10V), digitale IOs, Modbus RTU, Profibus	Empfang von Drehzahlvorgaben und Start-/Stopp-Befehlen; Rückmeldung von Betriebsstunden und Störberichten	Trockenlauf oder Kavitation durch manipulierte Steuerbefehle; Sabotage der Medienversorgung in kritischen Gebäuden (z.B. Krankenhäuser)
Ventile	Stetige oder schaltende Querschnittsänderung zur präzisen Volumenstromregelung von gasförmigen oder flüssigen Medien, hydraulischer Abgleich, physische Absperrung von Rohrleitungen im Regelkreis	0-10V, 4-20mA, Modbus RTU, BACnet	Erhalt stetiger Stellsignale (0-100%) vom DDC-Regler; Rückmeldung der tatsächlichen Ventilposition	Gezieltes Schließen von Sicherheitsventilen oder Blockieren im voll geöffneten Zustand führt zu thermischen/hydraulischen Instabilitäten oder Energieverschwendung
Beschattung	Mechanische Positionierung von Jalousien, Rollläden oder Markisen, tageslichtabhängige Lamellennachführung (Blendschutz), Reduzierung des solaren Wärmeeintrags, Umsetzung von Sicherheitsfahrbefehlen (Wind-/Frostalarm)	SMI (Smarte Motoren), KNX, Relaiskontakte	Empfang von Zentralbefehlen zur Fassadensteuerung (z.B. Windalarm); Senden von Lamellenwinkel-Vorgaben	Sabotage des Windalarms führt zur Zerstörung von Jalousien bei Sturm; Manipulation der Verschattung zur künstlichen Erhöhung der Kühllast