DEUTSCHE BUNDESBANK
EUROSYSTEM

Sicherheit in der GA aus Sicht des Betreibers

33. GLT-Anwendertagung 2019

LEUPHANA UNIVERSITÄT LÜNEBURG

Jochem Gombert, Deutsche Bundesbank

Sicherheit in der GA aus Sicht des Betreibers
Agenda

1. Das Zentrale Baumanagement / Aufgaben im Bauen und Betreiben
2. Überblick IT-relevante Anlagen
3. Globale Entwicklung in der Gebäudeautomation
4. Unterschiedliche Kulturen IT / OT
5. Beispiele / Lösungswege / neue Kulturen
   - Neue Filiale
   - Sicherheitsvorfall Fernwartung
   - Security Awareness Workshops
   - Anwendungsneutrale Netze, Netzwerkarchitektur
6. Resümee

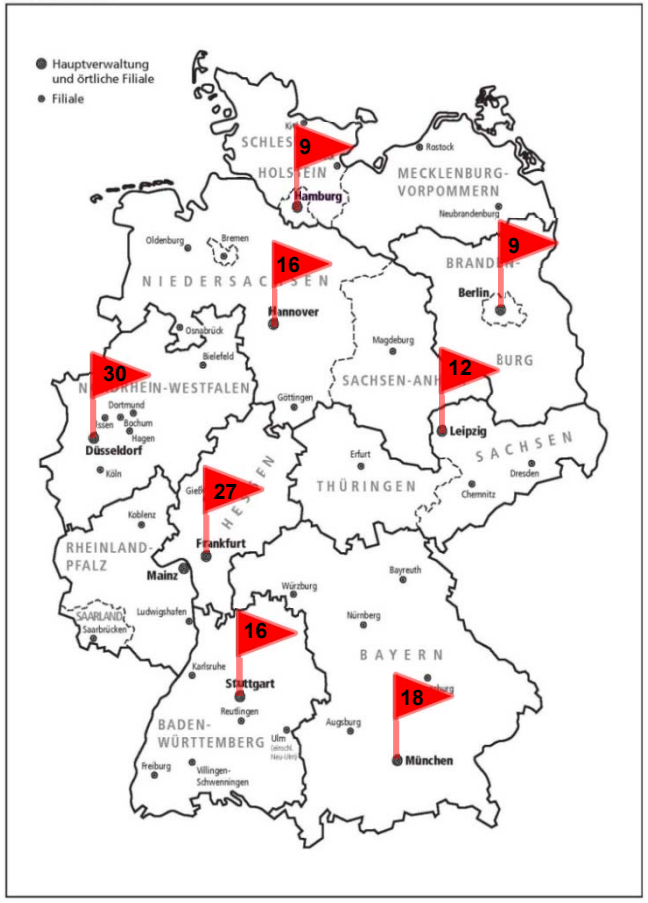
Zentrales Baumanagement

Aufgaben und Organisation

Das **Zentrale Baumanagement (ZBM)** ist für die Planung und Durchführung von Bauangelegenheiten der Bank zuständig.

Architekten und Ingenieure der Fachrichtungen Elektro- und Sicherheitstechnik sowie Versorgungstechnik führen Maßnahmen von der **ersten Planungsüberlegung** bis zur **Übergabe** und Abrechnung für die Gebäude der Bank durch.

Das ZBM übernimmt die Fachaufsicht über den **Betrieb der Gebäude** der Bundesbank und unterstützt die Betreiber in allen Liegenschaften.



8 Projektbüros / Anzahl Projekte

Berlin, Düsseldorf, Hamburg, Hannover, Leipzig, München und Rhein-Main sowie Stuttgart

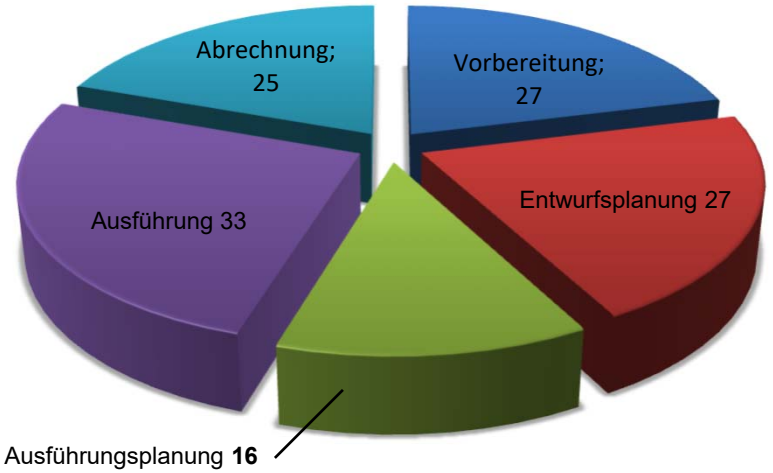
Zentrales Baumanagement
Bauprojekte

Einzelprojekte (Auswahl)

Dortmund, Neue Filiale
In Ausführung
Fertigstellung 2019

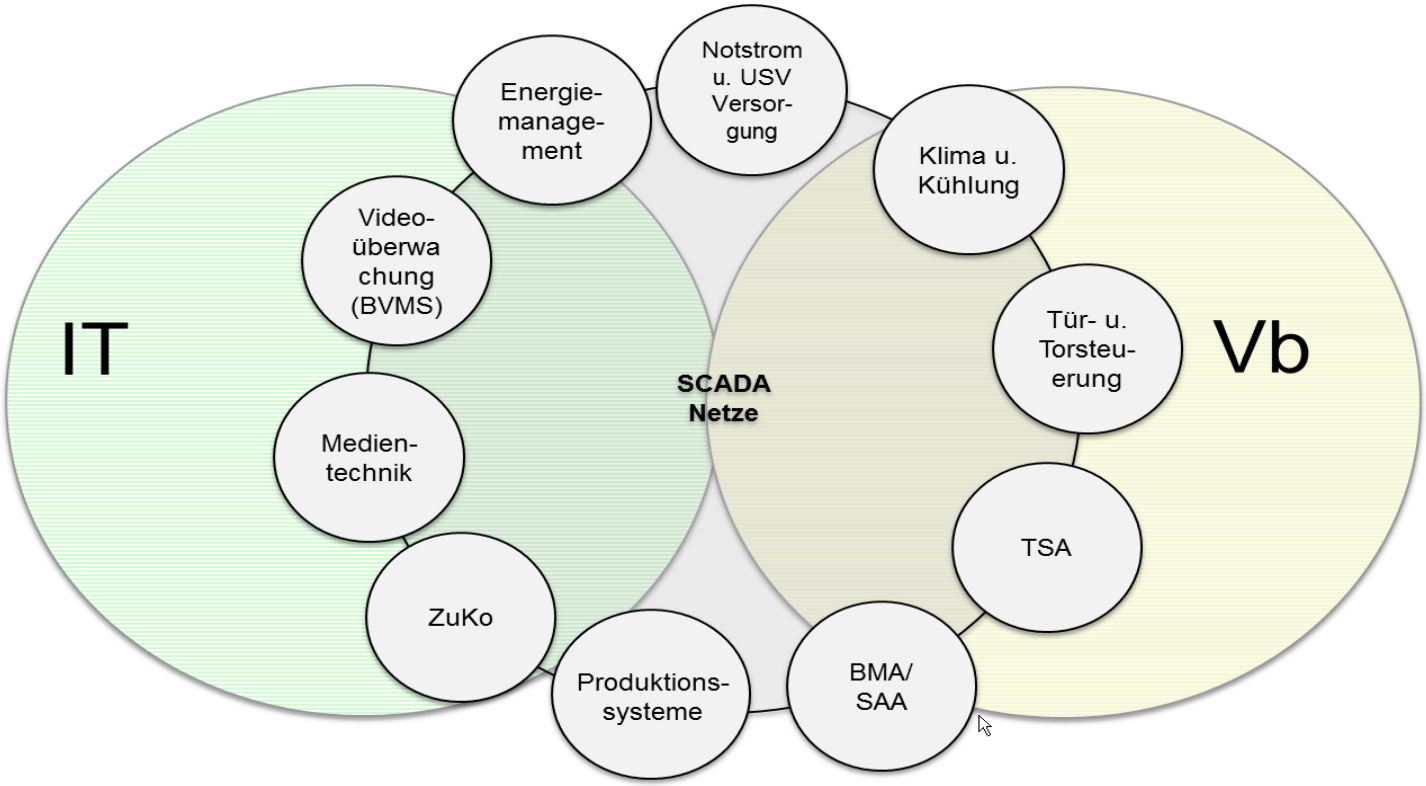
Hauptverwaltung in Rheinland-Pfalz und dem Saarland, MAGMA (Mainz Gesamtmaßnahme)
In Ausführung
Fertigstellung 2021

Bearbeitungsphasen



Sicherheit in der GA aus Sicht des Betreibers

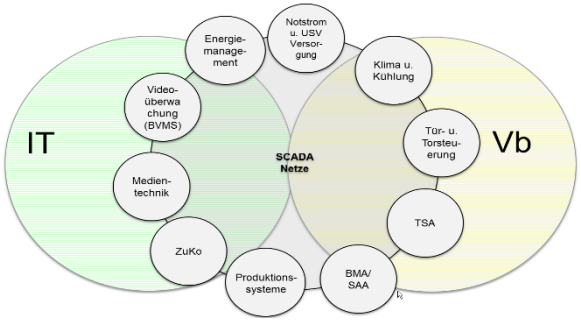
Schnittstellen zwischen den Gewerken und Verständnis für GA-Netze



ZuKo	Zutrittskontrollsysteme	**BMA**	Brandmeldeanlagen
TSA	Tresorsicherungsanlagen	**SAA**	Sprachalarmierungsanlagen
USV	Unterbrechungsfreie Stromversorgung		

Sicherheit in der GA aus Sicht des Betreibers

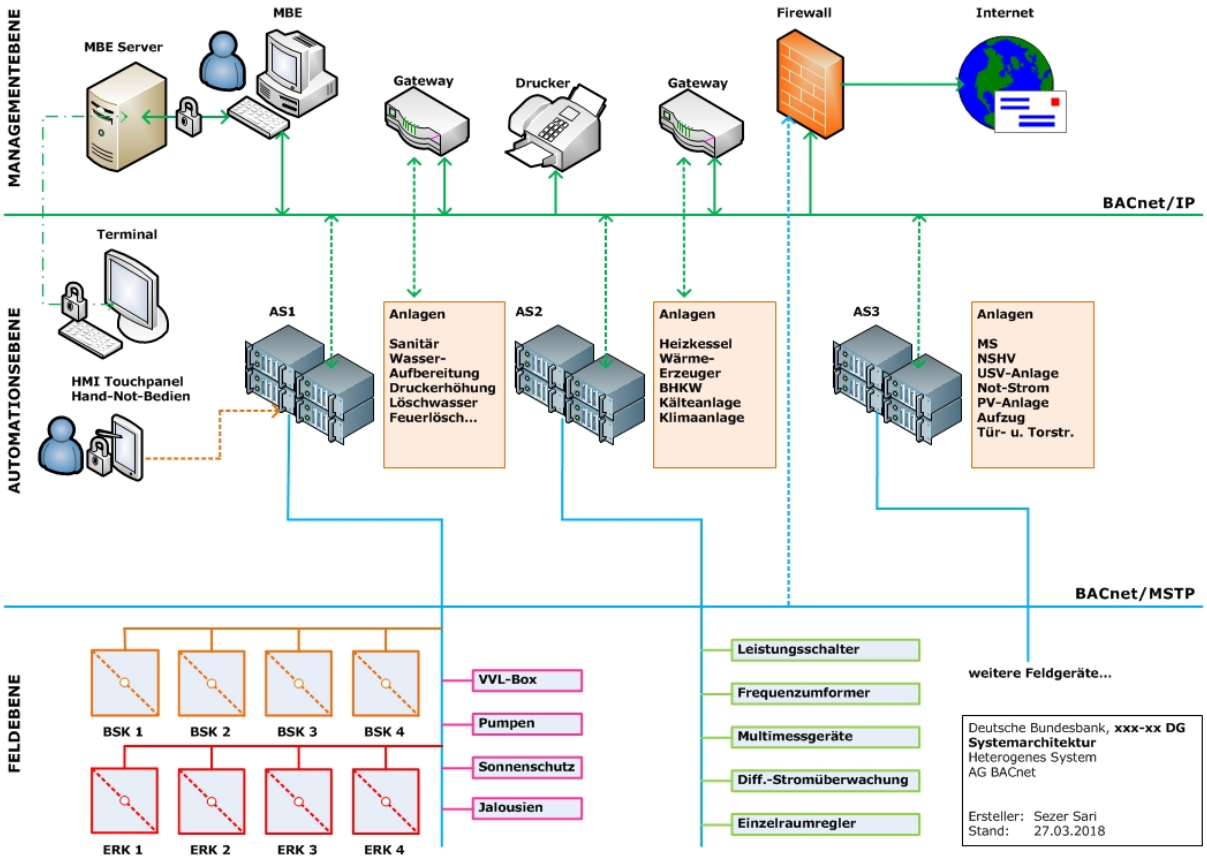
Vielfalt und Komplexität



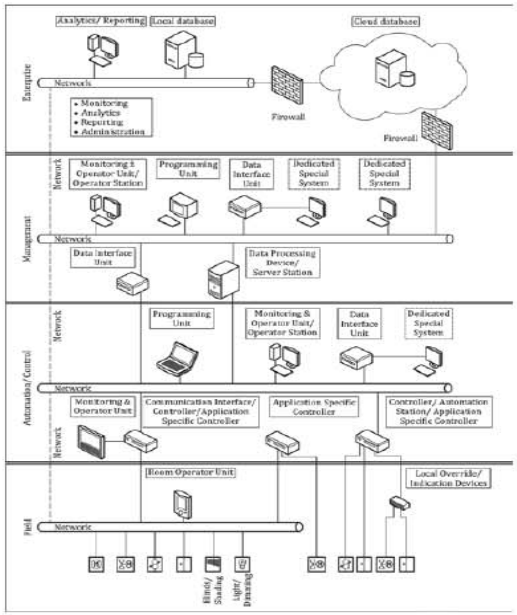
Die zunehmende Digitalisierungen betrifft neben der **IT** den **Betreiber** von Technischen Anlagen den **Objektschutz** und die **Organisation**, da diese Systeme u. a. einen wesentlichen Aspekt des Perimeterschutzes (z. B. Zugangskontrolle) ausmachen.

Wie kann nun der Betreiber in seinem Unternehmen dazu beitragen Fehler zu vermeiden und Schutzziele zu erreichen?

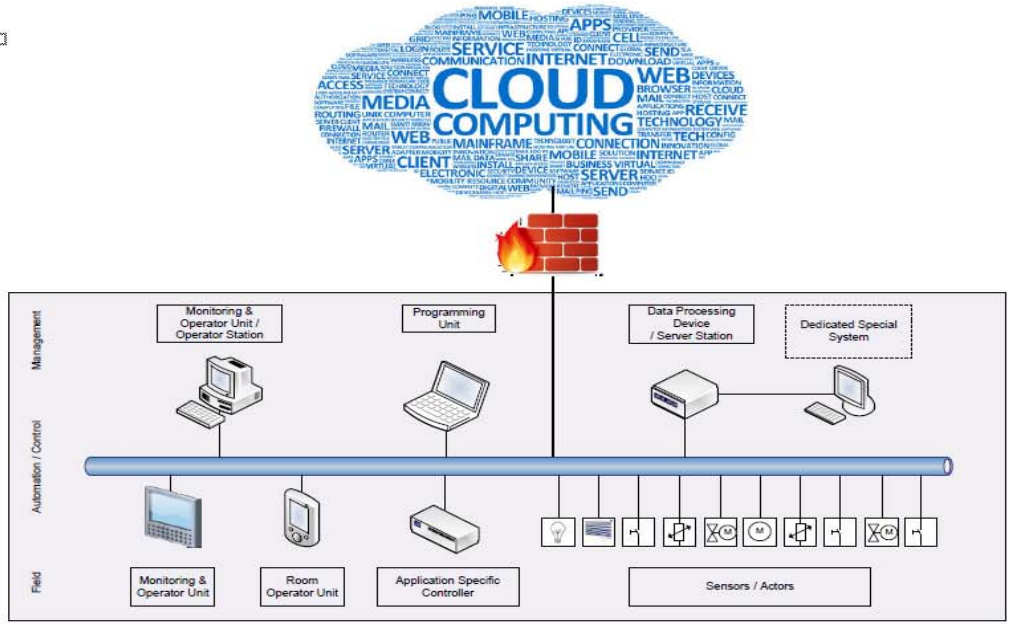
Sicherheit in der GA aus Sicht des Betreibers
Heutige Systemarchitektur GA



Globale Trends in der digitalen Bauwirtschaft



Gebäudeautomations-Ebenen
(DIN EN ISO 16484-2)

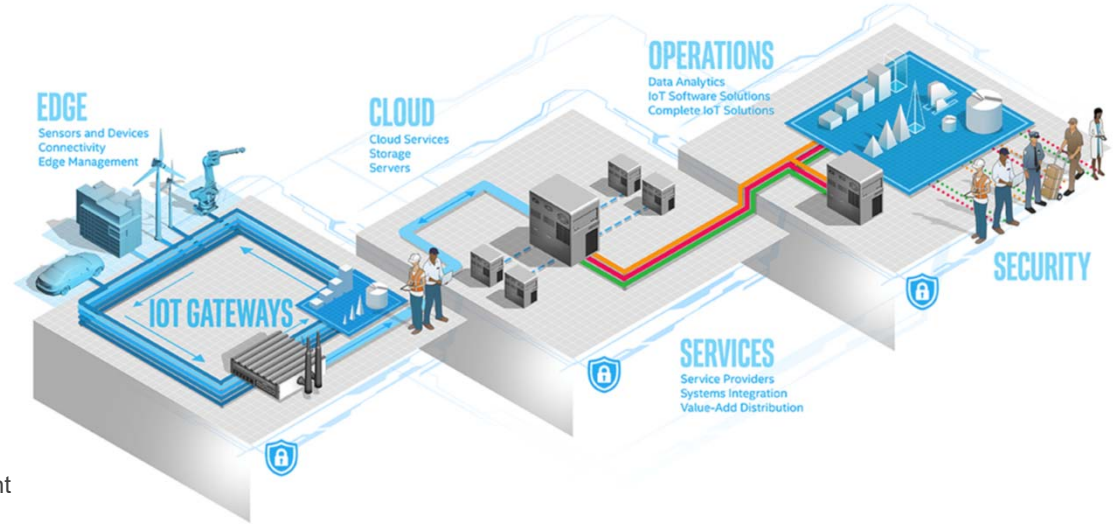


IoT

Sicherheit in der GA aus Sicht des Betreibers
Technologischen Entwicklung

Der Auslöser für die wachsende Bedrohung und die Aktualität des Themas IT-Sicherheit in der Gebäudeautomation liegt in der technologischen Entwicklung

Wir befinden uns auf dem Weg ins IoT; das bedeutet dass in Zukunft noch mehr netzwerkfähige Geräte einen direkten Zugang zum Internet erhalten werden.



Sicherheit in der GA aus Sicht des Betreibers
Unterschiedliche Kulturen

IT	Betreiber	Nutzer
• Wie kann ich Sicherheit und Performance der Systeme gewährleisten?	• Wie kann ich die Gewerke intelligent steuern?	• Wie genieße ich mehr Komfort, Sicherheit und Produktivität

Auswirkungen auf die Tätigkeiten

Durch die Digitalisierung werden zukünftig vermehrt informationstechnische Anlagen in der Gebäudetechnik verbaut
und
somit wird klar, dass bei der Einhaltung funktionaler Sicherheit auch immer Aspekte der IT-Sicherheit beibehalten werden müssen.

Sicherheit in der GA aus Sicht des Betreibers
Sicherheitsfokus in der Unternehmens-IT vs. GA

Aspekten	Gebäudeautomation	IT
Sicherheitsprioritäten	Verfügbarkeit, Prozess Sichtbarkeit, Prozess Operation, Integrität, Vertraulichkeit	Vertraulichkeit, Integrität, Verfügbarkeit
Verfügbarkeit des angebotenen Dienstes	24/7	Neustart, wenn benötigt
Verzögerung	Echtzeitanforderung	Variierende Antwortzeiten sind akzeptiert
Software Robustheit	Erwartet günstige Umgebung; Protokolle versagen, wenn gestört	Implementiert unter ständiger Hack-Gefahr, Schwachstellen entfernt
Anti Malware / Virus	Nicht gängig; unzureichende Ressourcen in alten Betriebssystemen	Standard
Patching	Fordern ein OK des Herstellers; Test; schwere Installation in einer 24/7 Umgebung	Nahezu sofort, wenn verfügbar
Passwörter	Fest einprogrammiert; niemals geänderte Gruppenpasswörter	Regelmäßiger Wechsel
Physische Sicherheit	Oftmals sehr gut; gesicherte Betriebsräume: verschlossene Schaltschränke	Hoch für Server und Netzwerk; niedrig für das Büro
Sicherheitsbewusstsein	Variiert sehr stark	Ständige Aufmerksamkeit
Lebenszyklus	10 bis 25 Jahre; ein Hersteller	3 bis 5 Jahre; ständig wechselnde Hersteller

Sicherheit in der GA aus Sicht des Betreibers
Problem „Zwei Welten“

Sicherheit in der GA aus Sicht des Betreibers
Beispiele / Lösungswege / neue Kulturen

- Berührungspunkte zu IT intensivieren, Beispiel Projekt „Neue Filiale“
- Aus Fehlern lernen ⟹ Sicherheitsvorfall Fernwartung
- Awareness aufbauen
- Technologische Grundlagen schaffen (Anwendungsneutrale Netze, Netzwerkarchitektur)

Sicherheit in der GA aus Sicht des Betreibers
Projekt Neue Filiale

Dortmund, Neue Filiale
In Ausführung
Fertigstellung 2019

Gebäudeautomation

Lagerverwaltungs- & Steuerungssystem

Sicherheitstechnische Anlagen

Videosystem H

IT-Sicherheit in der Bundesbank

IT-Risiokomanagementprozess

Festlegung des Schutzbedarfs

Ermittlung der IT-Sicherheitsanforderungen und potentiellen IT-Risiken

Feststellung von Maßnahmen und Bewertung von IT-Restrisiken

Berichterstattung und IT-Restrisikogenehmigung

IT-Sicherheit in der Bundesbank
interne Welt: IT-Sicherheitsanforderungen

Sicherstellung des angemessenen Schutzes von Informationen.

Sicherstellung des korrekten und sicheren Betriebs der informationsverarbeitenden Einrichtungen.

Umsetzung und Aufrechterhaltung eines angemessenen Grads an Informationssicherheit und Dienstleistungserbringung, in Übereinstimmung mit den Liefervereinbarungen mit Dritten.

Schutz der Integrität von Software und Informationen.

Aufdeckung nicht genehmigter informations-verarbeitender Aktivitäten.

Das Risiko von Systemfehlern und Systemausfällen zu minimieren.

Informationen in Netzen und die unterstützende Infrastruktur zu schützen.

Vermeidung von Verstößen gegen Gesetze, amtliche oder vertragliche Verpflichtungen, und gegen jegliche Sicherheitsanforderungen

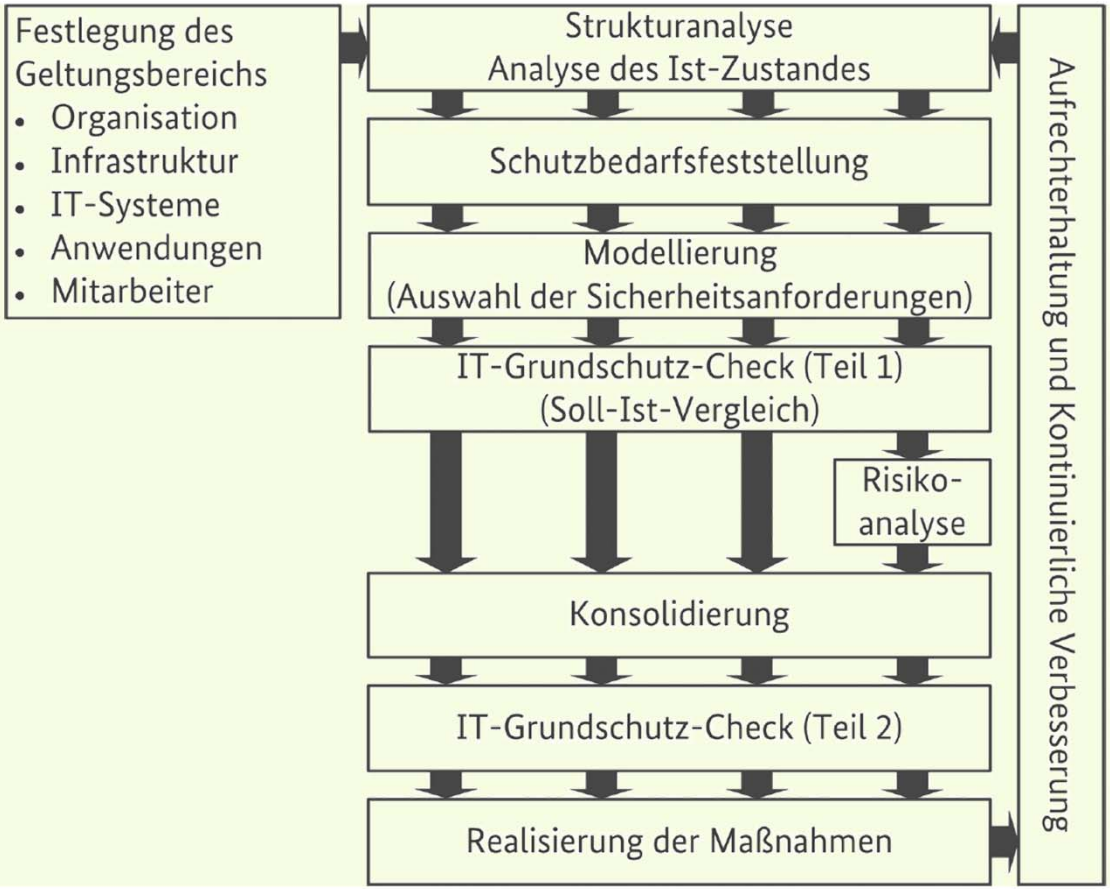
Verhindern von unbefugtem Benutzerzugriff, Kompromittierung und Diebstahl von Informationen und informationsverarbeitenden Einrichtungen.

Verhinderung von Fehlern, Verlust oder unberechtigter Veränderung oder Missbrauch von Informationen in Anwendungen.

Reduktion des Risikos der Ausnutzung veröffentlichter technischer Schwachstellen.

Befugten Benutzern den Zugang zu Informationssystemen zu sichern und unbefugten Zugang zu Informationssystemen zu verhindern.

BSI Grundschutz
Vorgehen



IT-Risikomanagement
Zeitliche Einordnung IT-Projektmanagement

IT-Projekt

Initiative	Voruntersuchung	Hauptuntersuchung	Durchführung	Projektabschluss
Skizze der Aufgabenstellung **Initiativvermerk**	Projektziele, mgl. Lösungswege, grobe Nutzen & Kosten **VU-Bericht**	Realisierungsfertige Ausarbeitung des Lösungsweg, Mittel & Kosten **HU-Bericht**	Erstellung / Bezug eines einsatzreifen Produkts, Betriebskonzept, Abnahme, **Freigabe**	Projektnachschau, Übernahme in Regelorganisation **Projektabschlussbericht**

IT-Architektur

Projektinitiative begleiten	Lösungsarchitektur erarbeiten	Update?	Lösungsarchitektur-ergebnisse aufnehmen
• Architekturbedeutung und –aufgabe analysieren • Lösungsarchitekt und (Kern-)Team zusammenstellen **Interne Dokumentation**	• Architekturziele festlegen, inkl. **IT-Sicherheitsziele** • Lösungsarchitektur ermitteln, inkl. **IT-Sicherheitsmaßnahmen** • Lösungsarchitektur (Soll) abschließen **LAD (Lösungsarchitekturdokument)**	**Überarbeitetes LAD**	**Zentrale Architekturübersichten**

IT-Sicherheit

Schutzbedarf festlegen	IT-Risikomanagementprozess durchführen	Update?
• Verfügbarkeit, Integrität und Vertraulichkeit einstufen • Weitere Angaben (Datenschutz, BCM, Nachprüfbarkeit, Authentizität) ergänzen **Abgestimmter Schutzbedarf**	• Generische und spezifische **IT-Sicherheitsziele** und potentielle IT-Risiken ermitteln • **IT-Sicherheitsmaßnahmen** anhand **Lösungsarchitektur** feststellen und IT-Restrisiken bewerten • Berichterstattung und IT-Restrisikogenehmigung **ZITR (Zusammenfassung der IT-Risikolage), IT-Restrisikogenehmigung**	**Überarbeitete ZITR** **Angepasste IT-Restrisikogenehmigung**

Sicherheit in der GA aus Sicht des Betreibers
Projektphasen IT vs. Bau / Betrieb

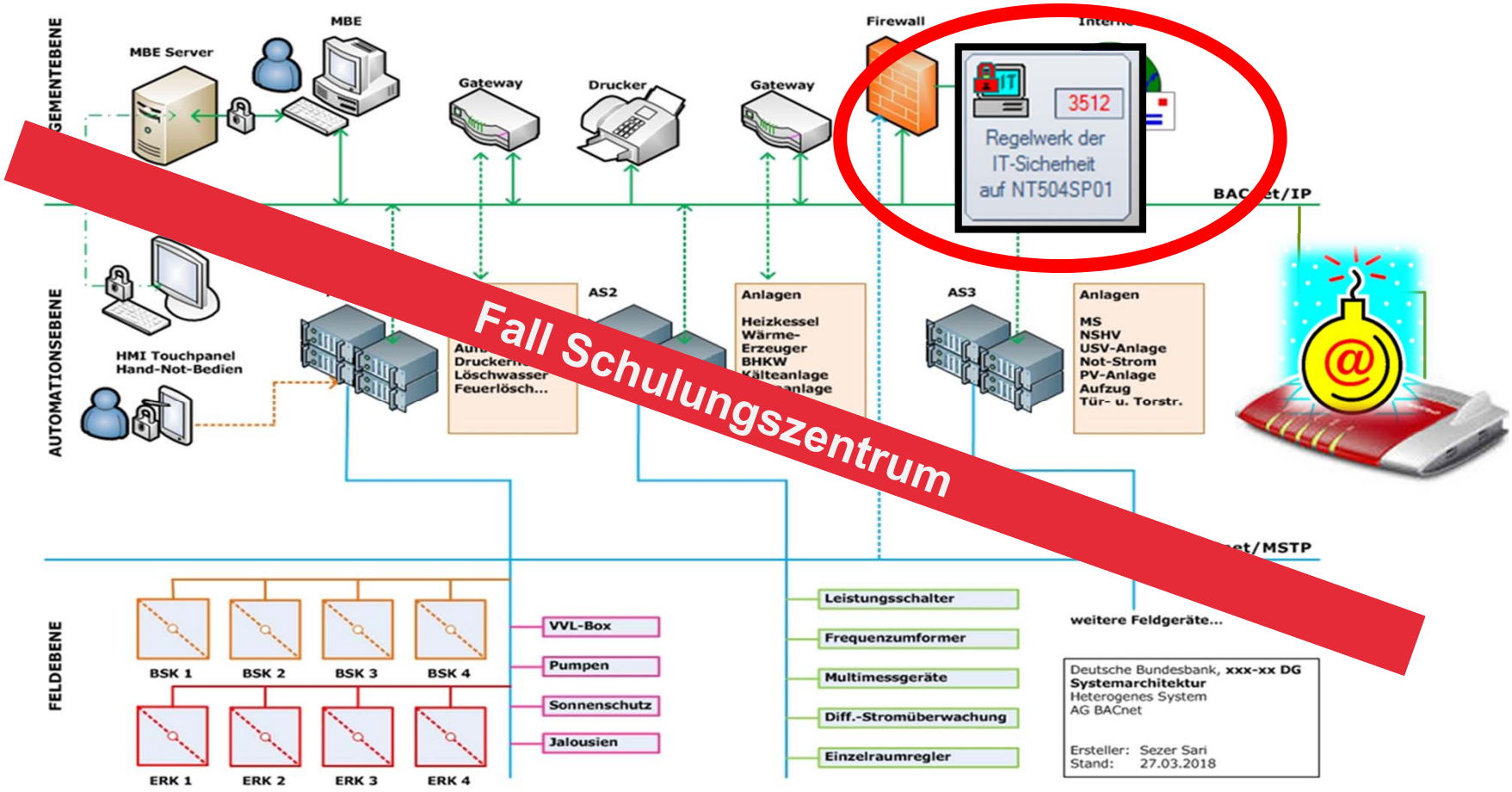
DB 1-15 Management von IT Projekten	DB 2-21 Bauwesen der BBk	
1. Initiative	0. Projektentwicklung	?
	1. Grundlagenermittlung	?
2. Voruntersuchung (VU)	2. Vorplanung	?
Risiken identifizieren , analysieren und bewerten – **„DAS REGELWERK DER IT`-SICHERHEIT“**	3. Entwurfsplanung	
	4. Genehmigungsplanung	
	5. Ausführungsplanung	?
	6. Vergabevorbereitung	
	7. Mitwirken bei der Vergabe	
4. Durchführung	8. Projektüberwachung	
5. Abschluss	9. Projektbetreuung/Dokumentation	

1. **Was tue ich?**
   Wende ich die Vorschriften u. Regeln an?
2. **Was tut die Bundesbank?**
   In wie weit werden diese Vorschriften bzw. Regeln in unserem Haus angewendet?
3. **Was tut der Projektleiter?**
   Werden neue IT-Sicherheitsprozesse in Bau Projekten umgesetzt?

Sicherheit in der GA aus Sicht des Betreibers
Projekt Neue Filiale – Lessons Learnt

- Das interne Vorgehen gem. IT-Risikomanagementprozess funktioniert mit externen Unternehmen nicht
- Für die Auftragnehmer ist IT-Sicherheit im angestrebten Umfang unbekannt
- Know-How ist bei Auftragnehmern praktisch nicht vorhanden und wird über Security-Consultants (Subunternehmer) eingekauft
- Das Lagerverwaltungssystem war eine sehr arbeitsintensive Erfahrung. Erkenntnisse daraus wurden auf alle weiteren Gewerke mit starkem IT-Bezug übertragen
- Bei den Bau-Gewerken (wie z.B. Gebäudeautomation) handelt es sich in einem hohen Grad um klassische IT-Landschaften
- Fernwartung ist ein Thema, welches uns immer wieder begegnet

Sicherheit in der GA aus Sicht des Betreibers
Sicherheitsvorfall Fernwartung



Sicherheit in der GA aus Sicht des Betreibers
Sicherheitsvorfall

Schwachstelle Mitarbeiter

In den letzten Jahren haben Cyber-Kriminelle den Fokus auch auf eine neues, vermeintlich einfacheres Angriffsziel verändert – den Mitarbeiter

ca. 80% aller Cybersicherheits-Vorfälle entstehen durch „Schwachstelle Mensch“

z.B. durch schnelle Klicks auf dubiosen E-Mail Anhang oder URL Links (professionelle Phishing-Mails, Spear-Phishing), USB-Stick, Umgang mit Passwörter, Soziale Netzwerke usw…

Security Awareness / Sicherheitsbewusstsein ist ein „must have“ Element der IT-Sicherheit

Sicherheit in der GA aus Sicht des Betreibers
Sicherheitsvorfall

Ziele für Mitarbeiter

- Stärkung guter Cybersicherheits-Gewohnheiten und Fertigkeiten
- Vermittlung von IT Kenntnissen, sicherer Umgang mit GA-Netzwerken

Ziele für Vorgesetzte

- Einschätzung der Security Skills im Unternehmen und wo ggf. Verbesserungen notwendig sind
- Effektiv, dauerhaft und messbar
- ggf. mehrere Zyklen im Laufe des Jahres

DEUTSCHE BUNDESBANK EUROSYSTEM

Security Awareness Workshop

Multiseminar in Eltville vom 01. – 03. Oktober 2019

Sezer Sari (3-10122) und Jochem Gombert (3-101)

Sicherheit in der GA aus Sicht des Betreibers
Security Awareness Workshop (Schwerpunkte)

- **MASSNAHMEN ZUR ERHÖHUNG DER SICHERHEIT AUS SICHT DER BEDIENER**
  - Soziale Manipulation
  - Passwörter und Benutzerkonten
  - Verbreitung sensibler Informationen

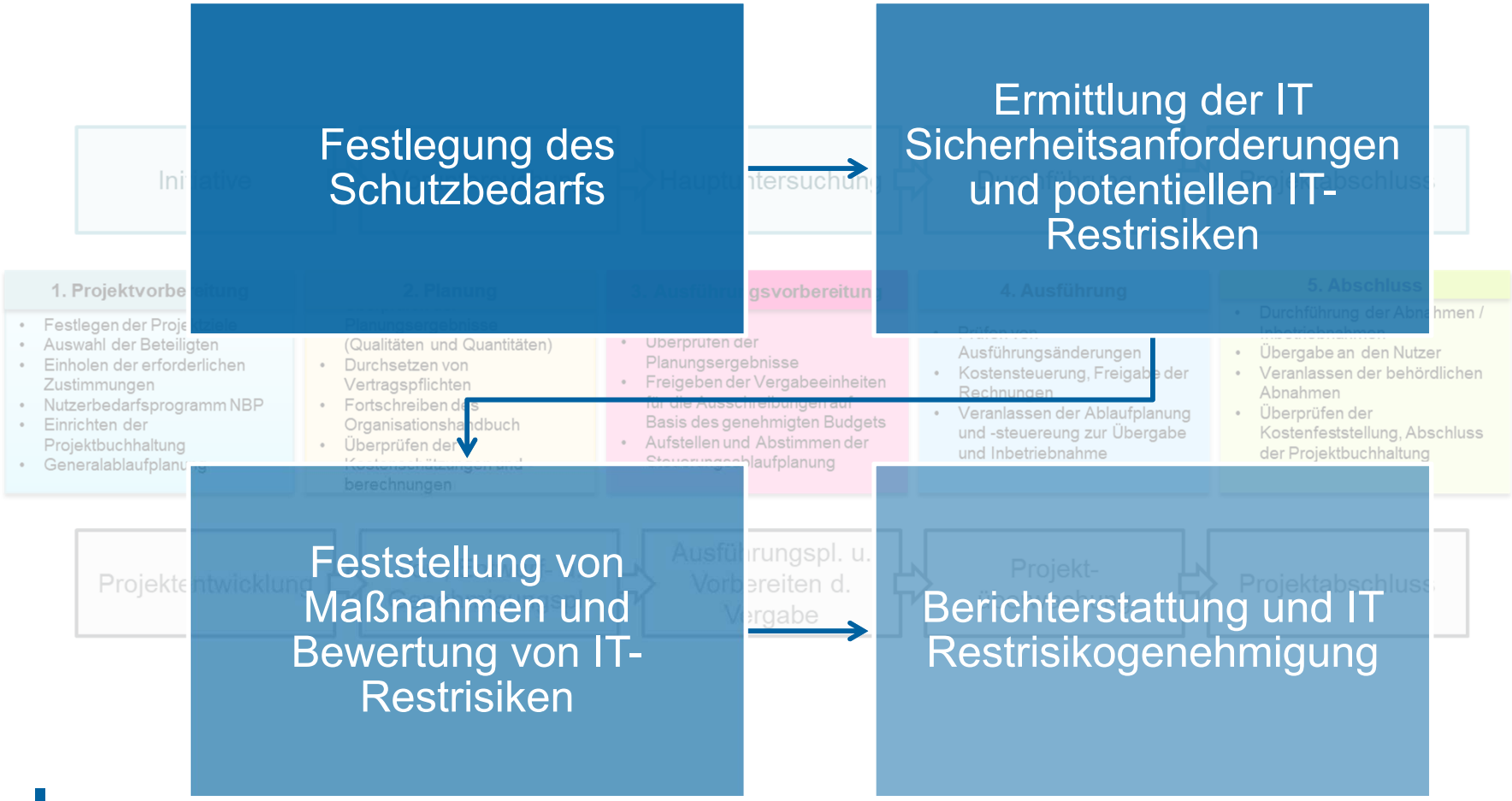
- **UMSETZUNG „Regelwerk der IT-Sicherheit“ PROJEKTPHASEN**
  - Risiken identifizieren, analysieren und eliminieren
  - Wann und an welcher Stelle?

- **SCHWACHSTELLEN VON AUTOMATISIERUNGSSYSTEMEN**
  - Beginn eines ganz normalen Arbeitstags in der Leitwarte
  - Frage: USB-Stick gefunden?
  - Auswirkungen von Sicherheitsverletzungen
  - Zunehmende Bedrohungen

- **SICHERHEITSMASSNAHMEN**
  - Anforderungen an Corporate- (IT) und Control (OT) Netze, Physische Sicherheitsmaßnahmen, Technische Sicherheitsmaßnahmen

Sicherheit in der GA aus Sicht des Betreibers

Projektphasen im Bau- und Instandhaltungsmanagement



Sicherheit in der GA aus Sicht des Betreibers
Anwendungsneutrale Netze, Netzwerkarchitektur

Zentralbereich IT
IT-Leitung
IT-Leitung-Notiz 2019/0015
Verfasser: **xxxxxxxx**
Datum: 02.05.2019

An: Zentrales Baumanagement
Kopie: IT1-IT-Plattformmanagement-Arbeitsplatz, IT5-IT-Basisinfrastruktur, IT52-Netzwerke

Betreff:
Modernisierung der Verkabelungsinfrastruktur in den Liegenschaften der Bank

Bauanforderung

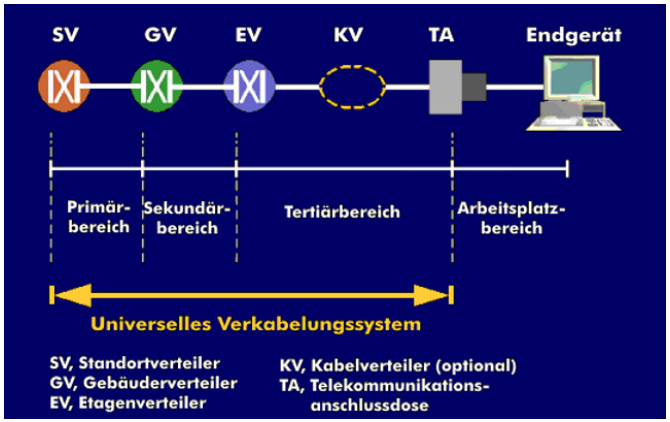
Sehr geehrte Damen und Herren,

die Verkabelungsinfrastruktur in den Liegenschaften der Bank ist in großen Teilen über 20 Jahre alt. Auf Grund der über Jahre gewachsenen Strukturen lässt sich nur schwer bewerten, in welchem Umfang künftige Anforderungen erfüllt werden können.

Im Zusammenhang mit der voranschreitenden Digitalisierung ist abzusehen, dass immer mehr Projekte neue Anforderungen an die Verkabelungsinfrastruktur stellen. Um darauf schnell und flexibel reagieren und verlässliche Aussagen über Nutzbarkeit der Verkabelungsinfrastruktur treffen zu können, muss die Datenverkabelung in den Liegenschaften der Bundesbank auf einen einheitlichen Mindeststandard gebracht werden.

Sicherheit in der GA aus Sicht des Betreibers
Anwendungsneutrale Netze, Netzwerkarchitektur

Aufbau Universeller Verkabelungssystem



Anforderung der IT:

IT-Standards

Sicherheit in der GA aus Sicht des Betreibers
Anwendungsneutrale Netze, Netzwerkarchitektur

Bereitstellung von IT – Diensten im universellen Verkabelungssystem für das Gebäude 4.0

Mit der fortschreitenden Entwicklung im IoT benötigen technische System im Gebäude Netzwerkinfrastrukturen wie sie bereits in der IT-Branche etabliert sind.

Folglich kann mit der Virtualisierung von Netzen die physikalisch Infrastruktur von universellen Verkabelungssystem sowohl für das Corporate- und das GA-Netz genutzt werden.

Nachteile:

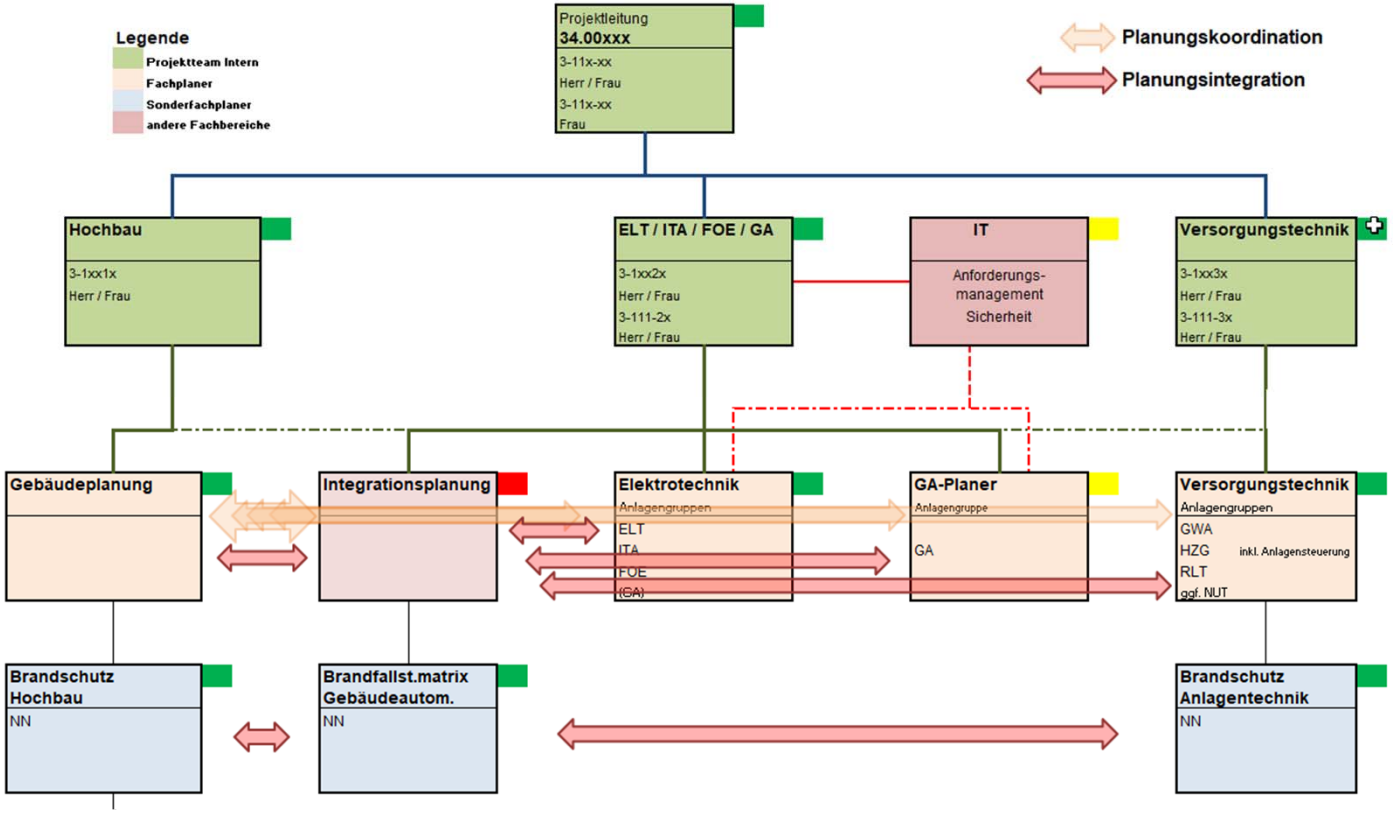
- Zusammenarbeit zwischen Bau / IT / HvD muss neu definiert werden
- Etablierte Projektstrukturen, Planungs- und Beschaffungsprozesse müssen neu definiert werden

Vorteile:

- Aufgabenbündelung bei der IT
- Sicherheitsniveau für kritische Infrastrukturen kann durch etablierte Standardverfahren der IT sichergestellt werden
- Know How muss nicht bei GA-Anbietern gekauft werden

Sicherheit in der GA aus Sicht des Betreibers
Anwendungsneutrale Netze, Netzwerkarchitektur

Etablierte Projektstrukturen müssen neu definiert werden



Sicherheit in der GA aus Sicht des Betreibers
Resümee

* Auch schon heute verbaute GA-Lösungen in der Bundesbank sind als Schatten-IT anzusehen

* GA-Lösungen beinhalten einen großen Anteil an IT Komponenten. Beim Kommunikationsmedium handelt es sich um klassische (IT-)Netzwerke.

* Vb schreibt aus, lässt verbauen, nimmt ab und übergibt an die Administration (Betriebsorganisation) ohne das klassische IT-Aspekte einfließen.

* Vb fordert in allen GA-Lösungen ein (GA-typisches) Standardprotokoll namens BACnet

* IT kennt die konkreten Anforderungen von GA-Lösungen nicht
  Rückschluss: IT kann nicht einschätzen, ob interne IT-Vorgaben / Standards und best-practises innerhalb von GA-Lösungen anwendbar sind

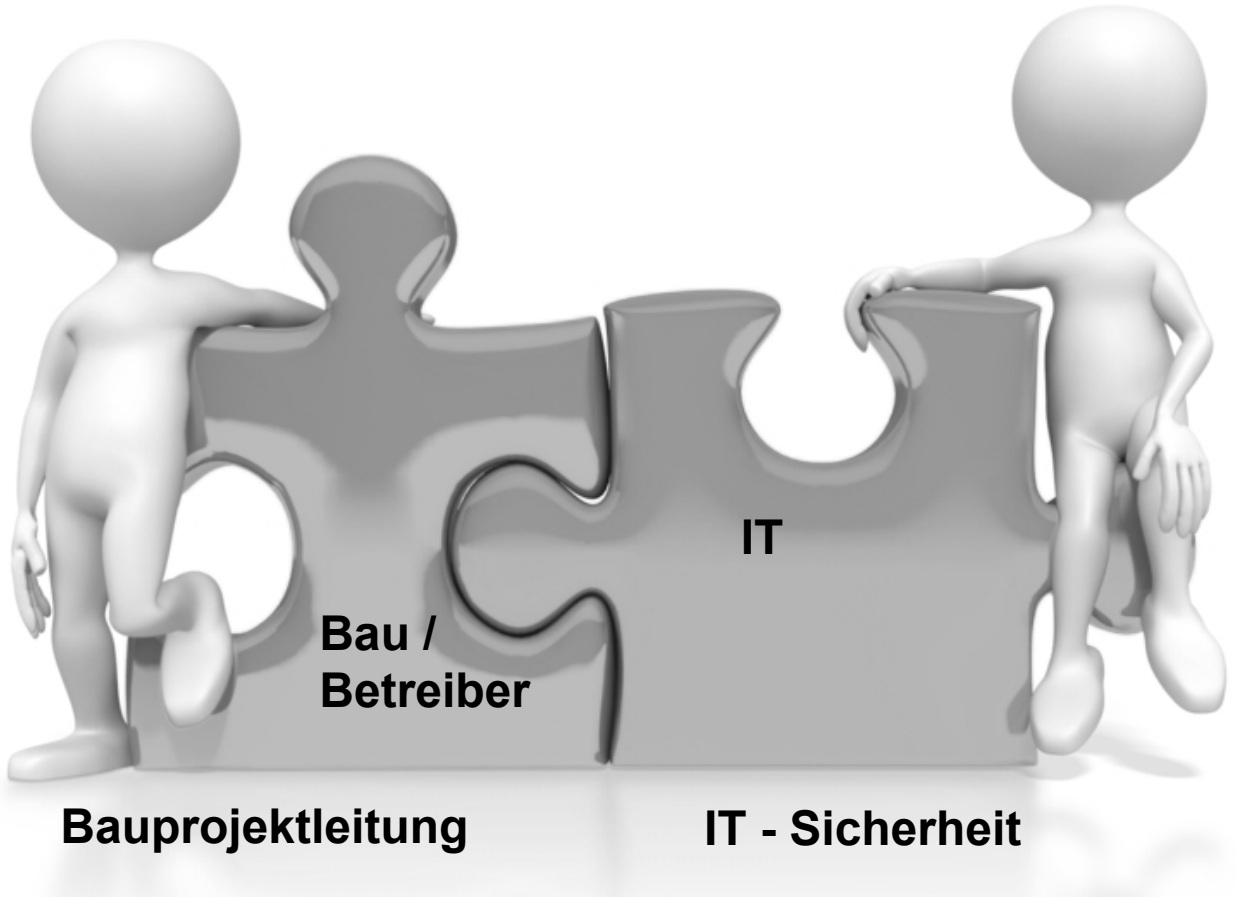
Sicherheit in der GA aus Sicht des Betreibers
Resümee

* Die Organisation muss das Thema "Digitalisierung in der Gebäudeautomation" angehen. Nicht nur der Betreiber

* Mittelfristig müssen Entscheidungen getroffen werden, welche mit den derzeitigen Ressourcen und Strukturen nur sehr schwer zu bewältigen sind:

  a) Vb "macht" IT-Technik und baut sich IT know-how auf
  und /oder
  b) IT unterstützt Vb in jedem Projekt und stellt know-how zur Verfügung und erhöht gleichzeitig Betreiber Wissen auf

Sicherheit in der GA aus Sicht des Betreibers
Ausblick



Sicherheit in der GA aus Sicht des Betreibers

Jochem Gombert
Dipl. Ing. (FH) Elektrotechnik
Master of Facility Management

Schwerpunkte: TGA und zuständig für die betriebstechnischen Standards der Deutschen Bundesbank

seit 1994: bei der Deutschen Bundesbank
seit 2012: Leitung Projektbüro Rhein-Main 2