Bundesamt
für Sicherheit in der
Informationstechnik

Umsetzungshinweise zum Baustein INF.14 Gebäudeautomation

1. Einleitung

Die Gebäudeautomation (GA, englisch Building Automation and Control Systems, BACS) stellt die technische Infrastruktur für den gewerkübergreifenden und automatisierten Betrieb von Gebäuden. Wesentliche technische Funktionen eines Gebäudes werden durch die technische Gebäudeausrüstung (TGA) bereitgestellt, die mit den Leistungen des technischen Gebäudemanagements (TGM) betrieben, gepflegt und weiterentwickelt werden. Die GA ist somit ein zentrales Werkzeug des TGM, um für den Gebäudebetrieb die gesetzte Zielrichtung umzusetzen (siehe Abbildung 1).

Eine gut auf die Gegebenheiten des Gebäudes abgestimmte und sichere Realisierung der GA ist essentiell, um die TGA-Anlagen eines Gebäudes optimal zu steuern.

Die GA führt Automatisierungsaufgaben wie automatisierte Messung, Steuerung und Regelung (MSR) sowie Aufgaben für Monitoring, Service und Diagnose, Optimierung, Bedienung und Management für die TGA eines Gebäudes durch.

1.1. Abgrenzung

Die GA nutzt neben den zentralen Systemen gegebenenfalls auch weitere dedizierte Komponenten, die MSR-Aufgaben übernehmen, z. B. Sensoren, die kein integraler Bestandteil einer TGA-Anlage sind. Gemäß TGA-Definition in VDI 4700 Blatt 1 sind solche Komponenten auch der TGA zuzuordnen. Um Missverständnisse zu vermeiden, nutzen der Baustein INF.14 *Gebäudeautomation* und diese Umsetzungshinweise zum Baustein einheitlich den Begriff GA-relevante Komponenten für zentrale Systeme, dedizierte Komponenten der GA und Komponenten der TGA-Anlagen, die Schnittstellen zur GA bereitstellen. TGA-Anlagen mit allen integralen Bestandteilen gehören nicht zur GA und werden in der GA nur über die in der GA sichtbaren Schnittstellen, z. B. zur Steuerung einer TGA-Anlage, erfasst.

Im Baustein INF.14 *Gebäudeautomation* und somit auch in diesen Umsetzungshinweisen wird der Begriff Gebäude synonym für Gebäude, Gebäudekomplex, Liegenschaft und Liegenschaftsportfolio genutzt (siehe Abbildung 2). Falls Aspekte für spezielle Gebäudetypen gelten, werden diese explizit genannt. Ein Gebäudekomplex ist eine Gruppe von Gebäuden, die baulich miteinander verbunden sind und als Gesamteinheit wahrgenommen werden. Eine Liegenschaft ist ein Grundstück inklusive seiner Bebauung. Zur Bebauung gehören alle unbeweglichen Sachen, d. h. Gebäude und sonstige Dinge, die nicht ohne weiteres vom Grundstück entfernt werden können. Als Liegenschaftsportfolio wird die Gesamtheit der Liegenschaften im Besitzstand bezeichnet. Der Begriff Gebäude beschreibt jedoch nicht nur Häuser und Hallen, sondern auch beispielsweise einen Fernsehturm oder eine Bohrinsel. Im Folgenden wird der Begriff Gebäude für alle Gebäudetypen synonym genutzt.

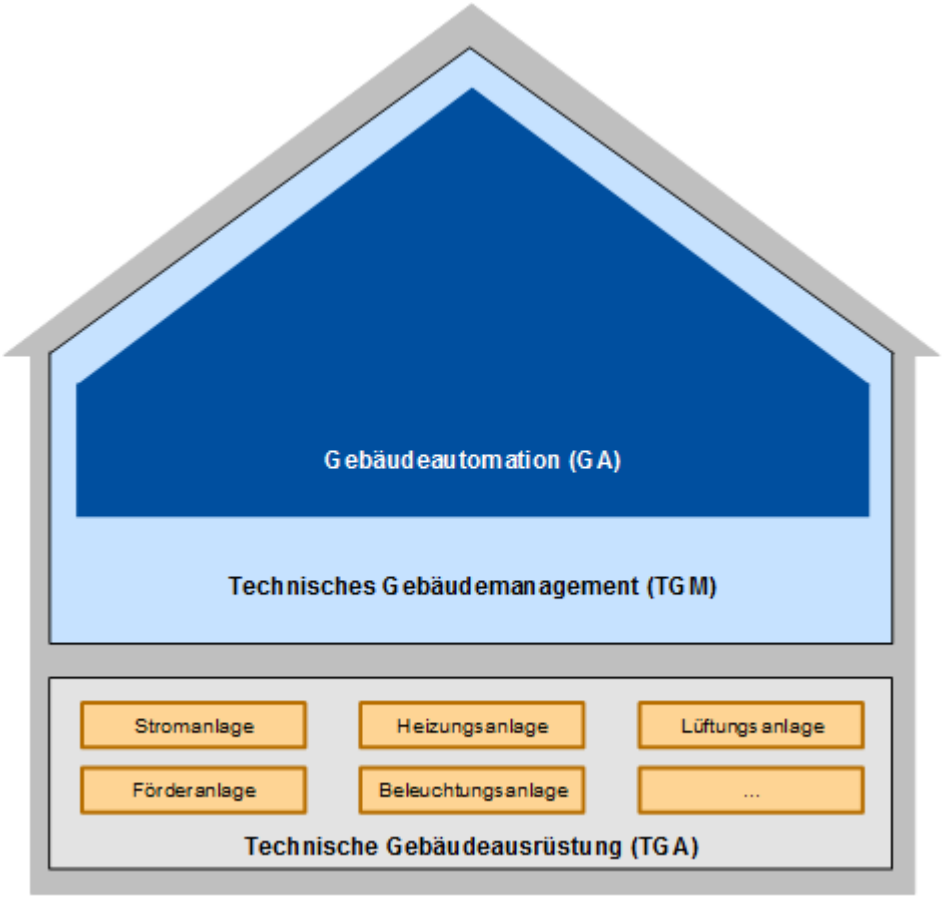

Abbildung 1: Abgrenzung TGM, GA und TGA-Anlagen

Die GA wird innerhalb eines Gebäudes für eine oder gegebenenfalls mehrere Nachfrageorganisationen bereitgestellt. Hierfür können die TGA-Anlagen mit Hilfe der GA separat z. B. für verschiedene Mieter oder Räume gesteuert werden.

Im Folgenden werden analog zu VDI 3814-1 die Begriffe GA-Segment, Raum oder GA-Bereich genutzt (siehe Abbildung 2).

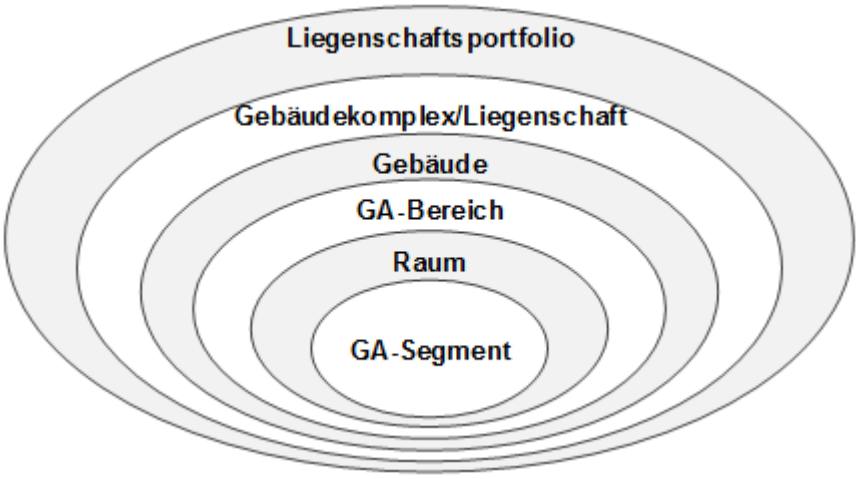

Abbildung 2: Schalenmodell der GA gemäß VDI 3814-1

In einem Gebäude kann die GA abhängig von den genutzten TGA-Anlagen durch mehrere parallele GA-Systeme umgesetzt werden (siehe Abbildung 3). Ein GA-System stellt die technische Realisierung der GA dar und beinhaltet jeweils das GA-Management zur übergreifenden Steuerung von Anlagenautomation (AA) und Raumautomation (RA) sowie die Schnittstellen zu den gesteuerten TGA-Anlagen und MSR-Komponenten. Auch mehrere Gebäude innerhalb eines Gebäudekomplexes oder einer Liegenschaft können durch ein GA-System gesteuert werden. Verschiedene GA-Systeme können kooperieren, aber auch vollständig unabhängig voneinander betrieben werden.

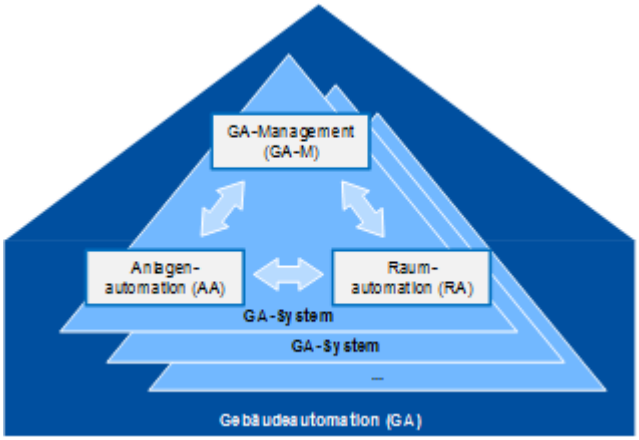

Abbildung 3: Gebäudeautomation gemäß VDI 3814

2. Maßnahmen

Im Folgenden sind spezifische Maßnahmen für die Anforderungen des Bausteins INF.14 *Gebäudeautomation* aufgeführt.

Alle Maßnahmen (gekennzeichnet mit M) sind aufsteigend nummeriert und korrespondieren mit den entsprechenden Anforderungen (gekennzeichnet mit A).

2.1. Maßnahmen zum Baustein INF.14 Gebäudeautomation

INF.14.M1 Planung der Gebäudeautomation (B)

Inzwischen ist in praktisch allen Gebäudetypen die Gebäudeautomation (GA) in unterschiedlicher Ausprägung und unterschiedlichem Umsetzungsgrad realisiert und oft sogar allgegenwärtig. Beispielsweise kann die GA derzeit die folgenden Bereiche, oft durch TGA-Anlagen realisiert, miteinander koordinieren:

- Heizung, Lüftung, Klima, Luftqualität und Verschattung

- Beleuchtung und Raumbeschilderung sowie Präsenzerkennung
- Energie- und Technikzentralen sowie Energierückgewinnung
- Verbrauchsdatenerfassung (Wärme, Gas, Strom, Wasser)
- Automatische Steuerung von Multimediasystemen und Geräten
- Zutrittskontrolle, Videoüberwachung, Gefahrenmeldeanlagen wie Brandmeldeanlagen (BMA), Einbruchmeldeanlagen (EMA) und Überfallmeldeanlagen (ÜMA)

Alle TGA-Anlagen werden in einem oder mehreren GA-Systemen zusammengeführt und automatisiert gesteuert. Neben TGA-Anlagen werden in der GA auch weitere Komponenten eingebunden, um Informationen über die Gebäude oder im Gebäude befindliche Personen zu liefern, z. B. Sensoren oder Beacons, die unabhängig von spezifischen TGA-Anlagen Informationen für die GA bereitstellen.

Daher muss für eine zielgerichtete Steuerung eines Gebäudes die GA konsequent und detailliert geplant werden (siehe auch [VDI 3814-2]) und bereits im Planungsprozess auch die Informationssicherheit angemessen berücksichtigt werden. Um die GA sicher gestalten zu können, muss vor der Planung eine Aufnahme der Gegebenheiten durchgeführt werden und diese unter Sicherheitsgesichtspunkten für die GA bewertet werden.

Abhängig vom Umfang der GA sollte die Planung eine detaillierte Anforderungsanalyse gemäß INF.14.M8 *Anforderungsspezifikation für GA-Systeme* sowie eine ausreichende Grobkonzeptionierung gemäß INF.14.M9 *Entwicklung eines GA-Konzepts* beinhalten.

Die Planung der GA muss bereits vor oder mindestens parallel zur Planung des Gebäudes erfolgen, da nur so alle baulichen Anforderungen der GA berücksichtigt werden können. Daher sollte die GA auch im Building Information Modeling (BIM, siehe Baustein INF.13 *Technisches Gebäudemanagement*), das zunehmend als Basis für die Planungs- und Bauprozesse von Gebäuden genutzt wird, als integraler Bestandteil berücksichtigt werden. Wird eine rechtzeitige Planung versäumt, kann es beispielsweise vorkommen, dass Sensoren funkbasiert angebunden werden müssen, da die Menge der Kabel nicht ausreichend geplant wurde. Je nach Bauweise des Gebäudes kann hierdurch sogar die Betriebsstabilität reduziert sein.

Oft werden Gebäude erbaut, bevor alle Nachfrageorganisationen und Betriebsorganisationen und deren Anforderungen an die GA bekannt sind. In solchen Fällen muss die GA möglichst universell geplant werden, um gegebenenfalls auch Nutzungsänderungen des Gebäudes zu ermöglichen.

Die Planung der GA muss einen ganzheitlichen Ansatz verfolgen und insbesondere die Sicherheitsanforderungen und das Zusammenspiel der TGA-Anlagen beachten. Die Planung muss umfassend dokumentiert werden (siehe INF.14.M5 *Dokumentation der GA*) und Verweise auf Aufbewahrungsorte wichtiger Unterlagen enthalten.

Aufnahme der Gegebenheiten

Im Vorfeld der Planung muss grundsätzlich erfasst werden, welche organisatorischen, architektonischen, statischen, regulatorischen und technischen Gegebenheiten in dem Gebäude für die Planung zu beachten sind. Hierzu gehören:

- Betreibermodell für ein Gebäude (siehe auch Baustein 13 *Technisches Gebäudemanagement)*
- Nutzungsmodell für ein Gebäude

Für die Gebäudenutzung müssen zum einen allgemeine Anforderungen, die unabhängig von Nachfrageorganisationen bestehen, sowie die konkreten Anforderungen von Nachfrageorganisationen aufgenommen werden.

- Gebäudespezifische Vorgaben oder regulatorische Vorgaben

Neben den Anforderungen, die sich aus dem Nutzungsmodell eines Gebäudes ergeben, müssen auch gebäudespezifische Vorgaben, beispielsweise aus statischen Gegebenheiten heraus, und regulatorische

Vorgaben, beispielsweise Bereitstellung einer Gefahrenmeldeanlage (siehe INF.14.M4 *Berücksichtigung von Gefahrenmeldeanlagen in der GA*), berücksichtigt werden.

- Umgebungsbedingungen für die eingesetzten GA-relevanten Komponenten (siehe 14.M23 *Einsatz von physisch robusten Komponenten für die GA*)
- Unterteilung des Gebäudes in dediziert steuerbare Bereiche, z. B. GA-Segmente, GA-Bereiche

Die Planung des Gebäudes für dediziert steuerbare Bereiche sollte eine größtmögliche Flexibilität bieten, um auf eine veränderte Nutzung des Gebäudes angemessen vorbereitet zu sein.

Ebenso müssen hier spezifische Anforderungen von Nachfrageorganisationen berücksichtigt werden, die beispielsweise eine strikte und sichere Trennung von anderen Nachfrageorganisationen benötigen (siehe INF.14.M10 *Bildung von unabhängigen GA-Bereichen*).

Festlegung und Auswahl der einzusetzenden Technik

Im Rahmen der Planung muss in einem ersten Schritt festgelegt werden, wie viele GA-Systeme für die GA erforderlich sind. Entscheidend hierfür sind

- die anzubindenden TGA-Anlagen,
- zusätzlich erforderliche GA-relevante Komponenten sowie
- die durch TGA-Anlagen und GA-relevante Komponenten vorgegebenen Techniken zur Anbindung und zur Kommunikation.

Hierfür müssen die gebäudespezifischen und regulatorischen Vorgaben mit den Anforderungen hinsichtlich Informationssicherheit und der gewünschten Funktionalität in Einklang gebracht werden. Ziel dieser Planung ist eine Minimierung der Anzahl von GA-Systemen und der eingesetzten Techniken.

Insbesondere muss im Einklang mit den relevanten Sicherheitsrichtlinien (siehe INF.14.M7 *Festlegung einer Sicherheitsrichtlinie für die GA*) festgelegt werden, welche Protokolle zur Kommunikation innerhalb von GA-Systemen und zwischen GA-Systemen genutzt werden (siehe INF.14.M12 *Nutzung sicherer Übertragungsprotokolle für die GA*).

Es sollten standardisierte Protokolle und Schnittstellen eingesetzt werden. Jedoch kann es in der GA vorkommen, dass Komponenten angebunden werden müssen, die auf proprietären Kommunikationsprotokollen basieren. Auf solche proprietären Lösungen sollte verzichtet werden, insbesondere wenn diese nicht dem Stand der Technik bezüglich der Informationssicherheit genügen.

Die automatisierte Steuerung der TGA-Anlagen erfordert eine synchrone Zeit, die von allen GA-relevanten Komponenten genutzt werden kann. Hier muss die Planung unter anderem festlegen, mit welchem Protokoll und welchen Abhängigkeiten die Zeitsynchronisation realisiert wird (siehe INF.14.M24 *Zeitsynchronisation für die GA* und INF.14.M30 *Bereitstellung eines GA-eigenen Zeitservers zur Zeitsynchronisation*).

Detailplanung der GA-Systeme

Zur Minimierung von Wechselwirkungen und Abhängigkeiten von TGA-Anlagen und GA-relevanten Komponenten muss für jedes GA-System detailliert geplant werden, welche Parameter für eine Steuerung von TGA-Anlagen genutzt werden und wie negative Auswirkungen durch eine fehlerhafte oder ausbleibende Übertragung der Parameter vermieden werden können (siehe auch INF.14.M21 *Anzeigen der Gültigkeit von Informationen in GA-Systemen*).

Außerdem sollte bereits bei der Planung geprüft werden, ob in der GA Cloud-Dienste genutzt werden und wie groß die Abhängigkeit der GA von einem solchen Cloud-Dienst ist. Ein potenzieller Wechsel des Cloud-Dienstleisters sollte möglichst frühzeitig in der Planung berücksichtigt und in der Detailplanung bei Bedarf sogar genauer betrachtet werden, um einen reibungslosen Wechsel zu ermöglichen. Dabei muss in der Detailplanung auch die Auswirkung auf die eingesetzten betroffenen TGA-Anlagen berücksichtigt werden.

Die Mechanismen und Topologien der GA-Netze müssen detailliert geplant werden. Insbesondere sollten die beschriebenen Maßnahmen zur Separierung und Segmentierung in INF.14.M6 *Separierung von Netzen der GA*, INF.14.M13 *Netzsegmentierung in der GA* und INF.14.M28 *Physische Trennung der GA* in der Planung berücksichtigt werden. Ergänzend hierzu sollten die Zugangspunkte zu den Netzsegmenten und die zu ergreifenden Schutzmaßnahmen wie z. B. Firewalls detailliert geplant werden. In der Detailplanung der GA-Netze sollten mindestens folgende Punkte angemessen berücksichtigt werden:

- eine sichere gebäudeübergreifende Vernetzung, speziell Internet, WAN, LAN, WLAN und andere Funknetze, Feldbusse, (siehe 14.M12 *Nutzung sicherer Übertragungsprotokolle für die GA* und INF.14.M13 *Netzsegmentierung in der GA*)
- die Absicherung der Zugriffe auf GA-relevante Komponenten (siehe INF.14.M14 *Nutzung eines GA-geeigneten Zugriffsschutzes*)
- die Absicherung von frei zugänglichen Ports (siehe 14.M11 *Absicherung von frei zugänglichen Ports und Zugängen der GA*)
- die sichere Anbindung von GA-externen Systemen, z. B. TGM (siehe INF.14.M18 *Sichere Anbindung von GA-externen Systemen*)
- die Absicherung und Nachverfolgung eingerichteter Fernwartungszugriffe (siehe INF.14.M14 *Nutzung eines GA-geeigneten Zugriffsschutzes*, INF.14.M18 *Sichere Anbindung von GA-externen Systemen* und INF.14.M26 *Protokollierung in der GA*)
- die Absicherung der Kommunikation in GA-spezifischen sowie nicht kabelgebundenen Netzen (siehe 14.M15 *Absicherung von GA-spezifischen Netzen*, INF.14.M16 *Absicherung von drahtloser Kommunikation in GA-Netzen* und INF.14.M17 *Absicherung von Mobilfunkkommunikation in GA-Netzen*)

Wichtigstes Protokoll zur Kommunikation innerhalb der GA ist das Internet Protocol (IP) in Version 4 und 6. Die sichere Nutzung dieses Protokolls setzt voraus, dass Adressbereiche skalierbar für Erweiterungen gewählt, angepasst aufgeteilt und umgesetzt werden (siehe INF.14.M19 *Nutzung dedizierter Adressbereiche für GA-Netze*). Aber auch die von den Komponenten genutzten IP-Mechanismen wie Broadcast und Multicast sollten angemessen geplant werden, um eine Überlastung der Netze zu vermeiden (siehe INF.14.M20 *Vermeidung von Broadcast-Kommunikation in GA-Netzen*). Beispielsweise sollten die IP-Subnetze so geplant werden, dass fehlerhafte Komponenten, die das Subnetz mit Paketen fluten, z. B. ein fehlkonfigurierter Sensor, nur eine überschaubare Menge anderer Komponenten beeinträchtigen. Ein weiteres Beispiel ist die Planung einer Meldungsaggregation, um die Anzahl der Pakete zu verringern und eine Überlastung der Kommunikationssysteme zu verhindern.

Viele GA-relevante Komponenten nutzen Power over Ethernet (PoE) zur Stromversorgung oder Power Line Communication (PLC) zur Kommunikation. Die Nutzung dieser Techniken muss angemessen geplant und mit den entsprechenden Gewerken abgestimmt werden.

Essentieller Teil der GA-Planung ist die Festlegung von Schutzmaßnahmen an den Schnittstellen zu TGA-Anlagen, die

- als autarke Anlagen rückwirkungsfrei betrieben werden müssen (siehe INF.14.M22 *Sicherstellung von autark funktionierenden GA-Systemen und TGA-Anlagen*) oder
- die aufgrund von technischen Gegebenheiten nicht integriert werden können (siehe 14.M3 *Sichere Anbindung von TGA-Anlagen und GA-Systemen*).

Insbesondere muss im Detail spezifiziert werden, durch welche Komponenten und Mechanismen diese Schutzmaßnahmen umgesetzt werden, z. B. GA-Management-System oder Firewalls vor TGA-Anlage (siehe auch INF.14.M29 *Trennung einzelner TGA-Anlagen*).

Die Detailplanung muss alle Parameter, die für eine sichere GA relevant sind, festlegen und liefert konkrete Konfigurationsvorgaben. Beispielsweise sollten für die GA-Management-Systeme spezielle Sichten bzw. Menüs für unterschiedliche Nutzergruppen spezifiziert werden.

Umsetzungsplanung

In der Umsetzungsplanung wird festgelegt, wie die Detailplanung umgesetzt werden soll. Die einzelnen notwendigen Schritte werden spezifiziert und hierfür Reihenfolge, Zuständigkeiten und Zeitrahmen festgelegt. Im Rahmen der Abnahme sollte geprüft werden, dass die Detailplanung exakt abgebildet wird und alle dort getroffenen Vorgaben und Festlegungen berücksichtigt werden. Abweichungen sollten auf die Detailplanung zurückgespielt und dort analysiert und gegebenenfalls korrigiert werden.

Außerdem müssen für die Umsetzungsplanung alle Wechselwirkungen und Abhängigkeiten von TGA-Anlagen und GA-relevanten Komponenten sowie von GA-Systemen untereinander erfasst werden. Hierauf aufbauend muss die Inbetriebnahme der GA detailliert geplant werden (siehe INF.14.M2 *Festlegung eines Inbetriebnahme- und Schnittstellenmanagements für die GA*).

Im Rahmen der Umsetzungsplanung werden auch Tests spezifiziert, die für die Inbetriebnahme der GA-Systeme durchzuführen sind.

Planung der Betriebssicherheit

Nach Detail- und Umsetzungsplanung muss auch der sichere Betrieb der GA geplant werden, indem mindestens folgende Punkte angemessen spezifiziert werden:

- Sicherheitsmaßnahmen auf den Systemen der GA-Management-Ebene (INF.14.M12 *Nutzung sicherer Übertragungsprotokolle für die GA*, INF.14.M13 *Netzsegmentierung in der GA* und INF.14.M14 *Nutzung eines GA-geeigneten Zugriffsschutzes*)
- Sicherstellung eines angemessenen Rollen- und Berechtigungskonzepts
- Zentrale Verteilung von Konfigurationsdateien auf die Komponenten der GA-Systeme
- Einbindung der GA-relevanten Komponenten in das Monitoring, die Alarmierung und Protokollierung (siehe INF.14.M25 *Dediziertes Monitoring in der GA* und INF.14.M26 *Protokollierung in der GA*)
- Einrichtung einer eigenen Datensicherung für die GA oder Anbindung der GA-relevanten Komponenten an eine zentrale Datensicherung

Darüber hinaus sollte bereits bei der Planung bedacht werden, dass gerade bei einer 24x7-Verfügbarkeit nicht immer geschultes Personal für akut anfallende Arbeiten vor Ort ist. Daher ist es wichtig, die entsprechenden Prozesse und Arbeiten an die Qualifizierung der entsprechenden Mitarbeiter vor Ort anzupassen bzw. im Umkehrschluss die entsprechenden Mitarbeiter dahingehend zu schulen, dass sie diese anfallenden Arbeiten ausführen können (siehe auch INF.14.M27 *Berücksichtigung von Wechselwirkungen zwischen Komponenten der GA in der Notfallplanung*).

Im Betrieb sollten regelmäßige Revisionen aller in der Planung erstellten konzeptionellen Teile durchgeführt werden, um das Niveau der Informationssicherheit zu erhalten oder sogar zu verbessern. Dabei sollte ein Soll-Ist-Vergleich zwischen den Vorgaben in Anforderungsspezifikationen und GA-Konzept bzw. Planung gegen den aktuellen Zustand durchgeführt werden. Auch sollte regelmäßig geprüft werden, ob die Systeme gemäß den Vorgaben konfiguriert sind. Die Ergebnisse der Prüfung sollten nachvollziehbar dokumentiert werden und Abweichungen sollten begründet oder umgehend behoben werden.

INF.14.M2 Festlegung eines Inbetriebnahme- und Schnittstellenmanagements für die GA

Die Festlegungen im Rahmen des Inbetriebnahme- und Schnittstellenmanagements müssen vollumfänglich dokumentiert und bei Änderungen angepasst werden. Sowohl regelmäßig als auch ergänzend bei Bedarf müssen die Festlegungen geprüft und gegebenenfalls nachjustiert werden.

Inbetriebnahmemanagement

Das Inbetriebnahmemanagement stellt sicher, dass ein Gebäude in Übereinstimmung mit der Planung und den betrieblichen Anforderungen funktioniert. Die Aufgabe des Inbetriebnahmemanagements ist es, die unterschiedlichen Gewerke und Beteiligten durch alle Phasen eines Bauprojektes und darüber hinaus in der ersten Nutzungsphase zu koordinieren. Aufgrund der Komplexität und der Vielzahl an Gewerken und Komponenten, die in die GA eingebunden werden müssen, muss die Inbetriebnahme gewerkeübergreifend geplant werden. Insbesondere muss die GA bereits während der Gebäudeplanung miteinbezogen werden.

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.

Dabei können einzelne Personen mehrere Rollen abdecken. Dies ist der Fall, wenn beispielsweise TGA-Anlagen durch einen Dienstleister betrieben und administriert werden. Wiederum können einzelne Rollen durch mehrere Gruppen abgedeckt werden wie z. B mehrere Mieter in einem Gebäude.

Zusätzlich zur Rollendefinition muss das Inbetriebnahmemanagement auch die Wechselwirkung und Abhängigkeit zwischen den TGA-Anlagen, GA-relevanten Komponenten und Prozessen berücksichtigen. Die Inbetriebnahme der angebundenen TGA-Anlagen muss aufeinander abgestimmt und justiert werden. Grundsätzlich müssen die folgenden Punkte festgelegt werden:

- Inbetriebnahme-Reihenfolgen von TGA-Anlagen
- Reihenfolge der Anbindung an ein GA-System (siehe INF.14.M3 *Sichere Anbindung von TGA-Anlagen und GA-Systemen*)
- Reihenfolge der Inbetriebnahme der Anbindung von GA-Systemen an andere GA-Systeme und sonstigen Systemen, z. B. TGM

Für die jeweiligen Inbetriebnahmen müssen typische Prüfpunkte festgelegt werden, die erfüllt sein müssen, bevor der nächste Inbetriebnahmeschritt erfolgen darf. Nach Abschluss der Bauphase und initialen Inbetriebnahme muss sichergestellt werden, dass die Prozesse und Festlegungen des Inbetriebnahmemanagements auf die Betriebsphase angepasst werden. Beispielsweise müssen Zugänge und Konten für den Zugriff von Dritten, z. B. Integratoren, die nur für die Inbetriebnahmephase erforderlich waren, gelöscht werden.

Auch während der Betriebsphase ist das Inbetriebnahmemanagement von essentieller Bedeutung. Beispielsweise kann der Neustart einer TGA-Anlage die Automatisierung unterbrechen. Ein solcher Neustart kann z. B. nach einer erforderlichen Nachjustierung von TGA-Anlagen erforderlich werden. Daher muss festgelegt werden, ob und in welcher Reihenfolge TGA-Anlagen und sonstige GA-relevante Komponenten bei einem Neustart einer anderen TGA-Anlage ebenfalls neugestartet werden müssen. Auch die Inbetriebnahme von erneuerten Anlagen muss im Inbetriebnahmemanagement während der Betriebsphase berücksichtigt werden. Das Inbetriebnahmemanagement liefert durch die Festlegung und zugehörige Vorgehensweise der Reihenfolge der Inbetriebnahme außerdem eine wichtige Grundlage für die Notfallplanung (siehe INF.14.M27 *Berücksichtigung von Wechselwirkungen zwischen Komponenten der GA in der Notfallplanung*).

Schnittstellenmanagement

Aufgrund der Komplexität und der Vielzahl an Gewerken, Komponenten und TGA-Anlagen, die in die GA eingebunden werden müssen, sollten alle Schnittstellen sorgfältig geplant und die beteiligten Organisationseinheiten bereits während der Gebäudeplanung einbezogen werden.

GA-relevante Komponenten sind vielfach untereinander abhängig und kommunizieren oft auch mit Systemen im TGM oder Büro-Bereich. Gegebenenfalls sind auch solche Systeme in GA-Prozesse eingebunden. Auch werden die Netze der GA immer häufiger über zentrale Netzkomponenten der Institution miteinander gekoppelt.

Hierfür müssen mindestens die folgenden Punkte abgestimmt und dokumentiert werden:

- Erfassung aller Betreiberorganisationen, die im Zusammenhang mit der GA relevant sind

Hierzu gehören auch die Betreiberorganisationen für die angebundenen TGA-Anlagen sowie gegebenenfalls für das TGM und sonstige IT-Bereiche der Institution.

- Erfassung aller Abhängigkeiten und Kommunikationswege zwischen GA-relevanten Komponenten und Systemen, die organisatorisch nicht zur GA gehören
- Technische Abstimmung der Anforderungen wie z. B. Verfügbarkeit an alle gemeinsam genutzten Ressourcen, beispielsweise allgemeines Netz, Netzdienste, Authentisierungs- oder Verzeichnisdienste
- Festlegung der Dienstgüte der gemeinsam genutzten Ressourcen, insbesondere die Einhaltung von geforderten Leistungsparametern, z. B. Bandbreite und Wiederverfügbarkeit bei Ausfällen
- Organisatorische Abstimmung von Zuständigkeiten und Berechtigungen auf den gemeinsam genutzten Ressourcen

Dritte, die in den Betrieb von OT- oder Office-Netzen involviert sind, müssen ebenfalls in die Abstimmung integriert werden.

- Technische und organisatorische Abstimmung über Komponenten, die die Trennung zu GA-Netzen realisieren, z. B. Switches zur Anbindung von GA-Netzen an ein übergeordnetes Netz der Institution

Eine Fortschreibung des Schnittstellenmanagements muss entlang der Phasen des Bauprozesses sowie während des Gebäudebetriebs wiederkehrend durchgeführt werden.

Für alle Schnittstellen, Tätigkeiten und Ressourcen müssen Prozessdefinitionen erstellt werden. Beispielsweise muss festgelegt werden, wer für erforderliche Änderungen zuständig ist und wer berechtigt ist, diese zu veranlassen. Auch muss in den Prozessdefinitionen berücksichtigt werden, welche Qualifikationen das Betriebspersonal aufweisen muss. Dies muss für die gesamte Betriebszeit gewährleistet werden, gegebenenfalls auch für einen 24x7-Betrieb.

INF.14.M3 Sichere Anbindung von TGA-Anlagen und GA-Systemen (B)

Als Grundlage für die Planung der Anbindung müssen alle TGA-Anlagen bzw. Komponenten eines GA-Systems mit allen Schnittstellen, Funktionalitäten und kritischen Parametern erfasst werden. Darüber hinaus müssen, sofern technisch möglich, die TGA-Anlagen sequentiell an ein GA-System angebunden werden, um bei einem Fehlverhalten eine schnelle Fehleranalyse zu ermöglichen.

Sowohl für eine Integration als auch für eine Kopplung sind folgende Schritte essentiell:

- Alle beteiligten TGA-Anlagen und GA-relevanten Komponenten sollten vor der Anbindung hinsichtlich ihrer Funktion autark getestet werden.

Auftretende Fehler innerhalb dieses Funktionstests müssen vor der Anbindung an das GA-System behoben werden.

Dies stellt auch für die Notfallvorsorge einen gegebenenfalls notwendigen autarken Betrieb einer TGA-Anlage sicher.

- Die Anbindung von TGA-Anlagen in ein GA-System muss, sofern technisch möglich, sequentiell durchgeführt und getestet werden. Insbesondere muss vor Aufnahme des produktiven Betriebs die Anbindung getestet werden.

Hierbei muss sichergestellt werden, dass ausschließlich die festgelegten Informationen und gegebenenfalls Aktionen zwischen GA-Management und den in der GA sichtbaren Teilen der TGA-Anlage möglich sind.

Darüber hinaus sollte sichergestellt werden, dass ausschließlich die festgelegten Kommunikationswege und Zugriffe zwischen GA-Management und TGA-Anlage mit der festgelegten Absicherung, z. B. Verschlüsselung, genutzt werden.

Auftretende Fehler und Abweichungen müssen vor der Anbindung der nächsten Anlage bzw. Komponente oder vor der Inbetriebnahme behoben werden.

- Ein GA-System darf erst dann an ein anderes GA-System angebunden werden, wenn die Anbindung von GA-relevanten Komponenten und TGA-Anlagen an das betreffende GA-System erfolgreich durchgeführt wurde.
- Die Reglementierung der erlaubten Aktionen erfolgt über das GA-Management oder über eine Kommunikationskontrolle auf einer Firewall bzw. einer vergleichbaren Sicherheitskomponente.

Integration von TGA-Anlagen

GA-relevante Komponenten bzw. TGA-Anlagen, die in ein GA-System integriert werden, können durch Meldungen und Informationen anderer GA-relevanter Komponenten zu Aktionen beeinflusst werden. Daher muss die Integration von Komponenten bzw. TGA-Anlagen in ein GA-System besonders sorgfältig geplant und geprüft werden. Dies gilt darüber hinaus in besonderem Maße, falls sich GA-Systeme untereinander beeinflussen können.

Hierfür müssen mindestens die folgenden Eckpunkte berücksichtigt werden:

- Für alle kritischen Parameter muss während einer Baselining-Phase festgelegt werden, in welchem Wertebereich diese durch das GA-System geändert werden dürfen, z. B. maximaler Temperaturbereich der Heizung.
- Es muss reglementiert werden, welche automatisierten Aktionen von welchen Komponenten eines GA-Systems ausgelöst werden dürfen.

Ebenfalls muss reglementiert werden, welche automatisierten Aktionen und Prozesse von anderen GA-Systemen auf dem betrachteten GA-System ausgelöst werden dürfen.

- Für die Aktionen sollte eine Plausibilitätsprüfung erfolgen, bevor die Aktion ausgeführt wird.

Kopplung von TGA-Anlagen an ein GA-System

Insbesondere TGA-Anlagen, die Gefahrenmeldeanlagen realisieren, dürfen in der Regel nicht in ein GA-System integriert werden. Hier kann eine Kopplung an ein GA-System erfolgen. In diesem Fall schickt die TGA-Anlage Informationen an das GA-System, die dort verarbeitet werden und gegebenenfalls Aktionen innerhalb des GA-Systems auslösen. Die TGA-Anlage wird jedoch nicht von dem GA-System beeinflusst.

Auch die Kopplung von TGA-Anlagen muss sorgfältig geplant und geprüft werden.

INF.14.M4 Berücksichtigung von Gefahrenmeldeanlagen in der GA (B)

Gefahrenmeldeanlagen, z. B. Brandmeldeanlagen, dürfen nur rückwirkungsfrei an GA-Systeme oder andere TGA-Anlagen gekoppelt werden (siehe auch Baustein IND.2.7 *Safety Instrumented Systems*). Dies bedeutet insbesondere, dass eine solche Anlage zwar Informationen mit anderen Komponenten austauschen, jedoch auf Basis von empfangenen Informationen nicht beeinflusst werden darf.

Eine Gefahrenmeldeanlage umfasst sowohl die zentralen Komponenten als auch die verteilten dezentralen Komponenten, insbesondere Sensoren. Beispielsweise gehören zu einer Brandmeldeanlage

die Brandmeldezentrale, die Bedien- und Anzeigeeinheit sowie alle im Gebäude verteilten Sensoren wie Brandmelder, Rauchmelder oder Kanalrauchmelder und Handfeuermelder.

Falls die Kommunikation von Gefahrenmeldeanlagen mit GA-Systemen auf drahtlosen Techniken basieren, sollte diese die relevanten Anforderungen der EN- und VdS-Spezifikationen für Komponenten in sicherheitsrelevanten Anwendungen wie Brandschutz, Einbruchschutz oder Zugangskontrolle erfüllen. Es sollten für diesen Einsatzbereich zertifizierte Mechanismen genutzt werden, die auch eine fehlerfreie Interoperabilität von Komponenten gewährleisten, auch wenn innerhalb der Gefahrenmeldeanlagen Komponenten unterschiedlicher Hersteller eingesetzt werden. Beispielsweise stellt IP500 einen solchen zertifizierten Mechanismus zur Verfügung.

Gefahrenmeldeanlagen müssen in dedizierten physisch getrennten Netzsegmenten positioniert werden. Die Kommunikation mit diesen Netzsegmenten sollte auf das betrieblich unbedingt notwendige Maß reduziert, streng kontrolliert und überwacht werden, z. B. durch Firewalls. Die zentralen Komponenten sollten in ein Netz- und Systemmonitoring und ein Security Monitoring eingebunden werden.

Folgendes muss daher bei der Netzintegration von Gefahrenmeldeanlagen zwingend beachtet werden:

- Segmente für Gefahrenmeldeanlagen müssen funktional autark gestaltet und auch hinsichtlich der Leistung autark dimensioniert werden, so dass die Funktionalität und Leistung der GA-relevanten Komponenten nicht durch einen Abbruch von Verbindungen zu der Umgebung oder durch einen fehlenden Datenaustausch mit der Umgebung beeinflusst werden.

Hierfür sollten physisch separierte Kabelwege und Komponenten genutzt werden. Ebenfalls darf keine Abhängigkeit von übergeordneten Netzdiensten bestehen, d. h. die Netzdienste müssen durch eigene Instanzen erbracht werden oder die GA-relevanten Komponenten müssen auch bei nicht verfügbaren Netzdiensten ihren vollen Funktionsumfang behalten.

- Die Übergänge zu den umgebenden Netzen müssen derart kontrolliert werden, dass die Integrität der Funktionen der GA-relevanten Komponenten nicht durch versehentliche oder vorsätzliche Übermittlung von falschen oder überflüssigen Daten oder Signalen aus der Umgebung beeinflusst werden.

Hierfür sollten Sicherheitskomponenten eingesetzt werden, die eine starke Kontrolle und Reglementierung von Daten- und Signalverbindungen gewährleisten können, z. B. Firewalls.

Alternativ sollte die Kommunikation ausgehend aus der TGA-Anlage unidirektional im Sinne einer Datendiode erfolgen, d. h. es wird eine ausschließlich unidirektionale Kommunikation erlaubt.

- Jegliche unberechtigte und nicht notwendige Kommunikation in Netzsegmente mit Gefahrenmeldeanlagen muss unterbunden werden. Hierfür muss die Netzsegmentierung so geplant werden, dass funktional unabhängige Anlagen in unterschiedliche Netzsegmente separiert werden.
- Bei der Auswahl der Funktechniken und Festlegung der Frequenzbereiche muss beachtet werden (siehe auch INF.14.M15 *Absicherung von GA-spezifischen Netzen* und INF.14.M16 *Absicherung von drahtloser Kommunikation in GA-Netzen*), dass Interferenzen zwischen Gefahrenmeldeanlagen und anderen Systemen sowie zwischen mehreren Gefahrenmeldeanlagen unterbunden werden.

INF.14.M5 Dokumentation der GA (B)

Die gesamte GA muss nachhaltig dokumentiert werden. Hierfür müssen die erstellten Dokumentationen regelmäßig geprüft und aktualisiert werden, um sicherzustellen, dass sie stets den aktuellen Stand der GA abbilden. Mit einer solch aktuellen Dokumentation kann im Fehlerfall schneller reagiert werden. Abhängigkeiten können schneller gefunden werden und auch Wechselwirkungen, z. B. bei einem Change, können schon im Vorfeld abgeschätzt werden.

Es muss sichergestellt werden, dass jegliche betriebsrelevante Änderung in der Anlagendokumentation erfasst wird. Zusätzlich sollten regelmäßig Prüfungen auf Aktualität durchgeführt werden, um Versäumnisse im Tagesgeschäft zu identifizieren und nachzuholen.

Die Form der Dokumentationsführung sollte sich an den jeweiligen GA-Systemen orientieren und möglichst praktikabel gestaltet werden. Die Dokumentation kann in Form von einem oder mehreren Dokumenten separat für die einzelnen GA-Systeme oder gemeinsam für alle GA-Systeme erfolgen. Um hier eine Austauschbarkeit zu gewährleisten, sollten für alle GA-Systeme inklusive der angebundenen TGA-Anlagen die Datenstrukturen und die mindestens zu erfassenden Inhalte festgelegt werden. Grundsätzlich sollten die Dokumentationen der einzelnen Teile (GA-Systeme) jedoch in eine gemeinsame Dokumentation zusammengeführt werden, beispielsweise durch Einbettung der Dokumente in einer gemeinsamen Website oder einem Dokumentationswerkzeug. Auch sollten die Dokumentationsinhalte zwischen den GA-Systemen austauschbar sein.

Die Dokumentation muss jederzeit verfügbar sein, insbesondere muss sie auch in Störungs- und Notfallsituationen umgehend zugänglich sein. Dies kann etwa durch Replikation auf Notsysteme oder als Ausdruck in Papierform am jeweiligen Arbeitsplatz und/oder am Notfallstandort erfolgen. Gleichzeitig muss jedoch die Dokumentation vor unbefugten Zugriffen geschützt werden.

INF.14.M6 Separierung von Netzen der GA (B)

Die in der Vergangenheit übliche konsequente physische Trennung von GA-Netzen vom restlichen Netz der Institution ist oft nur noch in gewissen Ausnahmefällen z. B. bei Gefahrenmeldeanlagen (siehe INF.14.M4 *Berücksichtigung von Gefahrenmeldeanlagen in der GA*) anwendbar. Die GA basiert mittlerweile immer stärker auf einer umfangreichen Kommunikation mit dem TGM oder Diensten der Büro-IT. Darüber hinaus wird die GA oft übergreifend für mehrere Gebäude realisiert. Hier ist die Einrichtung von dedizierten Verbindungen für die GA in der Regel nicht wirtschaftlich praktikabel. Jedoch sollten GA-Netze grundsätzlich so strukturiert werden, dass keine direkte Kommunikation von „außen“ auf eine GA-relevante Komponente ermöglicht wird und die Sicherheitskomponenten nur die notwendige Kommunikation weiterleiten.

Daher müssen für die GA unter besonderer Berücksichtigung der entsprechenden Anforderungen im Baustein NET.1.1 *Netzarchitektur und -design* weitere Mechanismen zur Trennung umgesetzt werden:

- Die GA muss mindestens logisch vom restlichen Netz der Institution getrennt werden (siehe Abbildung 4). Alle GA-relevanten Komponenten müssen möglichst an zentraler Stelle mit dem restlichen Netz der Institution, insbesondere Büro-IT und gegebenenfalls OT, gekoppelt werden.
- Die Absicherung der Trennung zwischen GA und restlichem Netz muss über mindestens eine Sicherheitskomponente mit Firewall-Funktionen erfolgen (siehe Baustein 3.2 *Firewall*).
- Abhängig von den Anforderungen sollte darüber hinaus sollte am Übergang zwischen GA und restlichem Netz eine DMZ eingerichtet werden, in der GA-spezifische Sicherheitskomponenten wie Application Layer Gateways, Sprungserver oder Datenaustauschserver positioniert werden. Zudem sollte in Betracht gezogen werden, am Übergang Funktionalitäten von Next Generation Firewalls (NGFW) wie Applikationskontrolle, identitätsbasierter Filterung und Anomalie-Erkennung über ein Intrusion Detection System (IDS) bzw. Intrusion Prevention System (IPS, auch in Kombination Intrusion Detection System and Prevention System, IDPS genannt) zu nutzen.

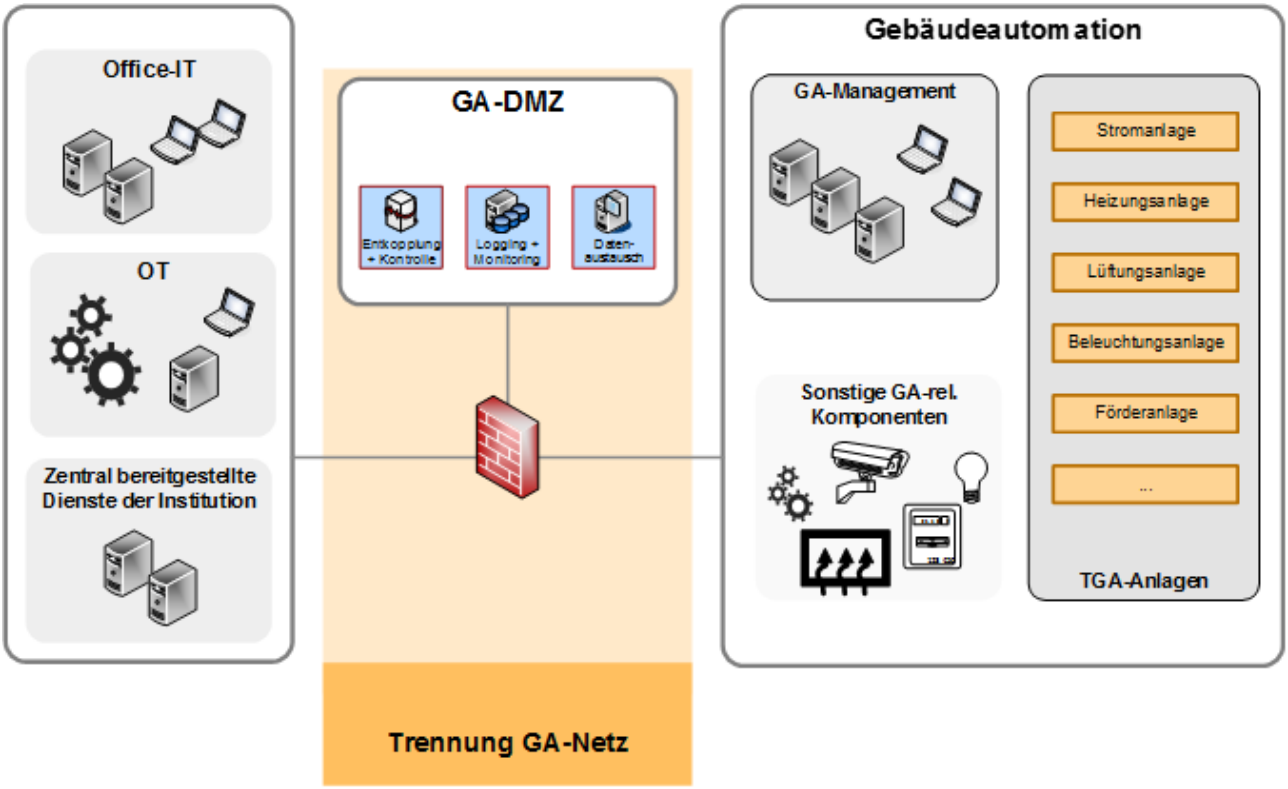

Abbildung 4: Trennung der GA auf Ebene der Netze

Verbindung von GA-Netzen verschiedener Gebäude

Wird die GA für verschiedene Gebäude oder Liegenschaften übergreifend realisiert, müssen die GA-Netze der Gebäude verbunden werden. Dies erfolgt meist über die Layer-1-Verbindungen des Campus-Netzes oder über das Wide Area Network (WAN) einer Institution.

Auf den Verbindungsnetzen muss dabei die logische Separierung der GA mittels VLAN-Tagging, VRF, MPLS-Tagging oder vergleichbaren Mechanismen durchgängig realisiert werden (siehe Abbildung 5). Werden GA-Netze in verschiedenen Liegenschaften via Internet gekoppelt, so muss die Separierung der GA mittels VPN oder vergleichbarer Techniken sichergestellt werden.

Die Verbindung zu GA-Netzen Dritter, z. B. durch Dienstleister bereitgestellte TGA-Anlagen, darf nur gemäß den Sicherheitsanforderungen gestattet werden, die in NET.1.1 *Netzarchitektur und -design* für die Anbindung externer Netze gefordert werden. Beispielsweise bedeutet dies, dass gegebenenfalls die Kommunikation mit solchen Netzen zusätzlich nach Stand der Technik verschlüsselt werden muss.

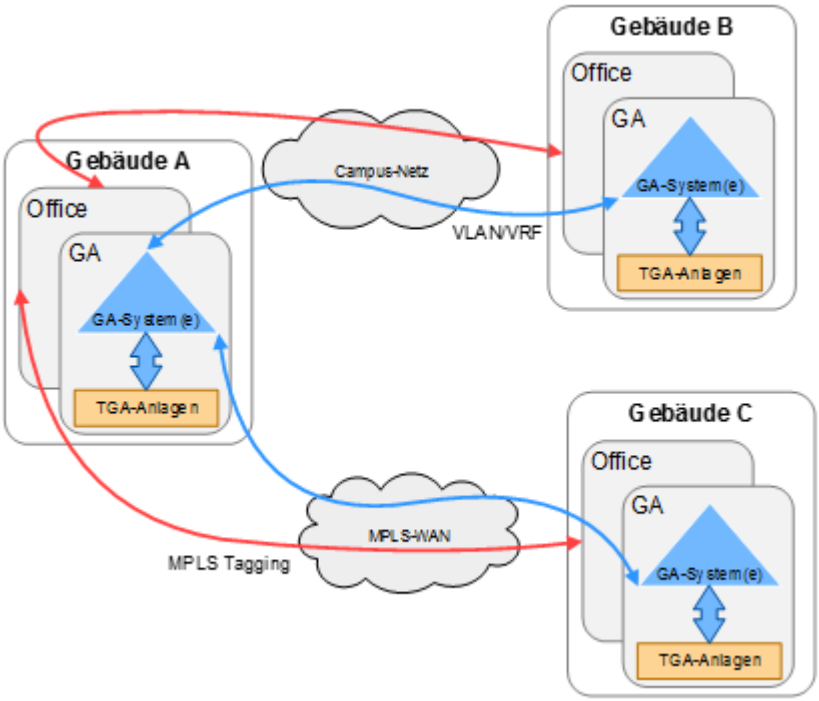

Abbildung 5: Logische Trennung der GA auf Verbindungsnetzen

Zugriff auf GA-relevante Komponenten

Abhängig von den Sicherheitsanforderungen der GA sollten auch sonstige Netze, beispielsweise ein Büro- oder OT-Netz, als unsicheres Netz vergleichbar zum Internet eingestuft werden. Jegliche Kommunikation mit GA-relevanten Komponenten aus solchen Netzen sollte über eine Sicherheitskomponente, z. B. Firewall, kontrolliert und gesteuert werden und gegebenenfalls entkoppelt werden.

Die Entkopplung im Sinne einer Kommunikationskontrolle sollte dann auf Ebene der Anwendung durch eine P-A-P-Struktur umgesetzt werden, siehe hierzu auch NET.1.1 *Netzarchitektur und -design*. Je nach Sicherheitsrichtlinien der GA bzw. der Institution kann hierbei auf eine physische Trennung der Netzkomponenten verzichtet werden (siehe Abbildung 6).

Auch der Zugriff von Dritten auf GA-relevante Komponenten darf nur gemäß den Anforderungen des Bausteins OPS.1.2.5 *Fernwartung* erfolgen.

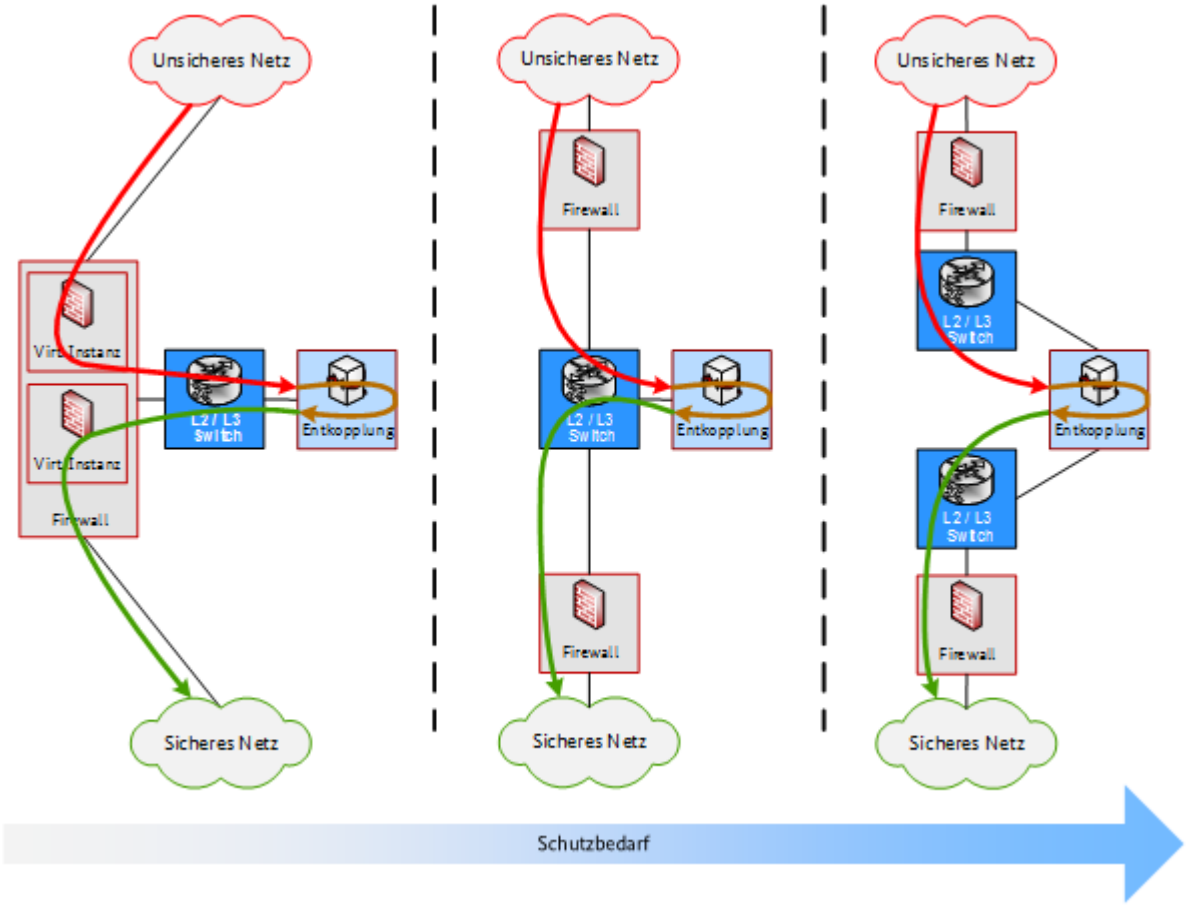

Abbildung 6: Mögliche P-A-P-Strukturen für Zugriffe auf die GA

Trennung von Netzdiensten

Die speziellen Sicherheitsanforderungen der GA, insbesondere hinsichtlich Verfügbarkeit, bedingen auch spezielle Sicherheitsanforderungen an die Netzdienste. Werden die Netzdienste zentral durch die Büro-IT bereitgestellt, müssen hiermit die Sicherheitsanforderungen vollumfänglich umgesetzt werden. Gegebenenfalls müssen hierfür dedizierte Instanzen in der GA vorgehalten werden, die mit der zentralen Instanz abgeglichen werden.

Internet-Zugang

Erfolgt der Internet-Zugang der GA-Komponenten über den zentralen Internet-Zugang der Institution, muss dieser den Anforderungen der GA entsprechen und die Trennung der GA muss auch für die Verbindung zwischen GA und Internet-Zugang sichergestellt werden.

Soll die GA als autarkes Netz realisiert werden, kann ein dedizierter Internet-Zugang für die GA und gegebenenfalls für die TGA-Anlagen in Betracht gezogen werden. Dieser muss die entsprechenden Anforderungen des Bausteins NET.1.1 *Netzarchitektur und –design* umsetzen und die erlaubte Kommunikation über diesen Internet-Zugang auf die zwingend erforderlichen Verbindungen und die Zeit der Nutzung einschränken.

Trennung von Endgeräten

Die Trennung der GA für Endgeräte kann durch verschiedene Maßnahmen erreicht werden:

- Die Switches werden gemeinsam für den Anschluss von Endgeräten genutzt und statisch unterteilt, indem Ports fest für Endgeräte der GA vorgesehen werden, z. B. per farblicher Markierung. Die logische Trennung im Switch erfolgt in der Regel auf Basis von VLANs.
- Die Ports eines gemeinsam genutzten Switches werden via Mechanismen zur Netzzugangskontrolle (Network Access Control, NAC, siehe 14. *Absicherung von frei zugänglichen Ports und Zugängen der GA*) abhängig vom angeschlossenen Endgerät selektiv den

auf dem Switch eingerichteten Zonen zugeordnet. Die netztechnische Abbildung der Segmente in den Switches erfolgt in der Regel über VLANs.

- Im Rahmen einer physischen Trennung werden für den Anschluss von GA-Endgeräten dedizierte Switches bereitgestellt, d. h. gegebenenfalls erhöht sich die Anzahl der erforderlichen Switches.

INF.14.M7 Festlegung einer Sicherheitsrichtlinie für die GA (S)

Die zu erstellende Sicherheitsrichtlinie legt die Rahmenbedingungen zur Ausgestaltung der Themen in der Anforderungsspezifikation und den Konzepten fest. Ihr Detailgrad ist weniger tief als der eines Konzepts oder einer Anforderungsspezifikation. Die Sicherheitsrichtlinie spezifiziert die allgemeinen Vorgaben, die für die gesamte GA mit allen GA-Systemen und Komponenten gelten. Sie hat Weisungscharakter und muss ebenso wie ihre Aktualisierungen allen Personen, die in der GA beteiligt sind, bekanntgemacht werden. Dies ist wichtig, um die Beteiligten für die getroffenen Sicherheitsvorschriften zu sensibilisieren (siehe auch Baustein ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit*). Gerade Administratoren mit ihren privilegierten Rechten und die Kommunikation zur Steuerung von TGA-Anlagen bilden ein lukratives Angriffsziel. Daher ist es auch wichtig, die Umsetzung der Inhalte der Sicherheitsrichtlinie regelmäßig und nachvollziehbar zu prüfen. Hierfür können z. B. Soll-Ist-Vergleiche herangezogen werden. Außerdem sollte der Stand der Technik in regelmäßigen Aktualisierungen der Sicherheitsrichtlinie einfließen.

Die Sicherheitsrichtlinie dokumentiert die wesentlichen Bedingungen, die für die GA berücksichtigt werden sollten. Sie macht Vorgaben, die übergreifend für alle GA-Systeme gelten und sollte beispielsweise folgende Themen abdecken:

- Vorgaben, welche TGA-Anlagen über die GA automatisiert gesteuert werden sollen
  Insbesondere sollte auch festgelegt werden, welche TGA-Anlagen autark realisiert werden sollen und wie diese an die GA angebunden werden.
- Vorgaben für eingesetzte Werkzeuge
  Zunächst sollten allgemeine Vorgaben für alle für die GA eingesetzten Systeme spezifiziert werden. Gegebenenfalls gibt es darüber hinaus spezielle Vorgaben für eingesetzte Werkzeuge, Systeme oder MSR-Komponenten.
- Vorgaben für die sichere Anbindung von eingeschränkt vertrauenswürdigen GA-relevanten Komponenten
  Hier sollte festgelegt werden, wie mit Bestandssystemen, die die Sicherheitsvorgaben nicht mehr erfüllen, umgegangen wird, z. B. durch Festlegung eines Austauschzeitfensters. Neu beschaffte Komponenten sollten die Sicherheitsvorgaben vollumfänglich erfüllen.
  Ebenfalls sollte festgelegt werden, ob und wie ein IT-System eines Wartungstechnikers, der nicht unter der Verantwortung der Institution fällt und somit nur eingeschränkt vertrauenswürdig ist, im LAN oder direkt an GA-relevanten Komponenten angebunden werden darf.
- Vorgaben zur Zutritts-, Zugangs- und Zugriffskontrolle
  Zentrale Komponenten der GA sollten sich grundsätzlich in physisch geschützten Bereichen befinden. Zugangs- und Zugriffsrechte sollten nach dem Minimalprinzip vergeben werden und den allgemeinen Richtlinien der Institution folgen. Der Zugang zu Systemen und der Zugriff auf Informationen sollte nur nach erfolgreicher Authentisierung erlaubt werden (siehe auch Baustein ORP.4 *Identitäts- und Berechtigungsmanagement*). Spezielle Regelungen zur Authentisierung sollten festgehalten werden. Zugang und Zugriff sollten grundsätzlich auf personengebundene Konten beschränkt werden.
- Vorgaben zum Schutz der Kommunikation
  Die GA-Kommunikation sollte über sichere Protokolle erfolgen. Hieraus resultieren Anforderungen für alle in der GA eingesetzten Kommunikationsmedien. Ebenso sollte vorgegeben werden, nach welchen Kriterien nicht ausreichend sichere Protokolle eingesetzt werden dürfen.

- Vorgaben zum Monitoring
  Mindestens die zentralen Komponenten der GA-Systeme sollten in ein Monitoring eingebunden werden. Die Richtlinie sollte festlegen, welche Typen von Komponenten in ein Monitoring eingebunden werden.
- Vorgaben zur Protokollierung
  Mindestens die zentralen Komponenten der GA-Systeme sollten in eine zentrale Protokollierung eingebunden werden. Auch hier sollte die Richtlinie festlegen, welche Typen von Komponenten in eine zentrale Protokollierung eingebunden werden sollen.

Abhängig von der individuellen Situation einer Institution kann eine übergreifende Sicherheitsrichtlinie für TGM und GA erstellt werden. Hier sollte darauf geachtet werden, dass die Sicherheitsrichtlinie alle GA-relevanten Themen berücksichtigt.

Wird das TGM von einer anderen Institution, z. B. der Betreiberorganisation des Gebäudes, durchgeführt, die GA jedoch von der Institution bereitgestellt und betrieben, muss auch hier die TGM-Sicherheitsrichtlinie für die GA-Sicherheitsrichtlinie berücksichtigt werden.

INF.14.M8 Anforderungsspezifikation für GA-Systeme (S)

Die Anforderungsspezifikation konkretisiert die GA-Sicherheitsrichtlinie und wird in zwei Schritten durchgeführt: Zunächst erfolgt eine detaillierte Anforderungsanalyse, in der die aufgenommenen Anforderungen bewertet werden, und erst dann werden die konkreten Anforderungen an alle GA-relevanten Komponenten festgeschrieben.

Detaillierte Anforderungsanalyse

In der Anforderungsanalyse werden alle organisatorischen und technischen Anforderungen an eine sichere GA ermittelt. Diese Anforderungsanalyse bezüglich der Informationssicherheit ergänzt die Bedarfsplanung gemäß VDI 3814 Blatt 2.1 (siehe [VDI3814-2]). Die Anforderungsanalyse ist sowohl für die Konzeptionierung von GA-Systemen als auch für den Beschaffungsprozess wichtig.

Im Rahmen der Anforderungsanalyse sollten alle Anforderungen der TGA-Anlagen hinsichtlich einer Anbindung an die GA sowie der Nachfrage- und Betreiberorganisationen aufgenommen werden. Für die GA sollten alle unverzichtbaren und wünschenswerten Funktionen aufgenommen und hinsichtlich Informationssicherheit bewertet werden. Außerdem sollten die gewünschten und möglichen Zugriffsmöglichkeiten auf die GA-relevanten Komponenten analysiert werden.

Diese Anforderungen müssen koordiniert bewertet und gegebenenfalls angepasst werden. Beispielsweise kann eine Nachfrageorganisation nicht fordern, dass sie für ein Funksystem einen Frequenzbereich alleinig nutzen darf, wenn innerhalb eines Gebäudes weitere Nachfrageorganisationen auch Funktechnik in diesem Frequenzbereich nutzen wollen.

Für ein neu zu erbauendes Gebäude, für das gegebenenfalls die Nachfrageorganisationen noch nicht feststehen, sollten bereits während der Planungsphase sinnvolle und zeitgemäße, d. h. universelle Anforderungen hinsichtlich der GA ermittelt werden. Beispielsweise sollte für ein Bürogebäude eine flexible Steuerung unterschiedlicher Räume und Gebäudeteile vorgesehen werden.

Die Anforderungsanalyse sollte auch die Betriebssituation der GA berücksichtigen. Grundsätzlich setzt eine sichere GA voraus, dass sie von vertrauenswürdigem und kompetentem Personal betrieben wird. Jedoch kann die Verfügbarkeit von kompetentem Personal nicht für alle Betriebszeiten und alle GA-relevanten Komponenten gewährleistet werden. Beispielsweise kann außerhalb der Regelarbeitszeit nicht sichergestellt werden, dass komplexe Fehlersituationen umgehend behoben werden können. Daher kann die eingeschränkte Betriebssituation außerhalb von Regelarbeitszeiten zu speziellen Anforderungen an Komponenten führen. Beispielsweise sollten Fehler an MSR-Komponenten auch nachts mittels einfachem Komponententausch durch vorkonfigurierte MSR-Komponenten behoben werden können. Darüber hinaus sollten alle Anforderungen hinsichtlich eines sicheren GA-Betriebs im Rahmen der Anforderungsanalyse erfasst werden.

Weiterhin müssen alle Anforderungen gegenüber den legalen und regulatorischen Vorgaben, die die GA betreffen, geprüft werden. Beispielsweise dürfen Funkfrequenzen in Deutschland nur genutzt werden, wenn sie für den Einsatzzweck von der Bundesnetzagentur freigegeben sind.

Anforderungsspezifikation

Die Anforderungsspezifikation dokumentiert die organisatorischen und technischen Anforderungen hinsichtlich Informationssicherheit, die aus der Anforderungsanalyse resultieren, sowohl an die GA-relevanten Komponenten als auch an den Betrieb der GA. Ebenfalls sollten spezifische Anforderungen an Netzstruktur und Netzkomponenten festgelegt werden (ergänzend zur Bausteinschicht NET *Netze und Kommunikation*). Hierdurch wird die Anforderungsspezifikation gemäß [VDI3814-2] um Anforderungen hinsichtlich Informationssicherheit ergänzt.

Die Anforderungsspezifikation für die GA sollte auch die speziellen Anforderungen von Gebäuden berücksichtigen, z. B. für Universitätskliniken oder Universitätsgebäude.

Um eine universelle Nutzung der Gebäude sicherzustellen, sollten auch Vorgaben für eine mögliche Erweiterbarkeit der GA spezifiziert werden. Dabei sollten sowohl aktuelle als auch langfristig absehbare Anforderungen berücksichtigt werden.

Werden alle Anforderungen an die verschiedenen Typen von GA-relevanten Komponenten in einem oder mehreren Lastenheften erfasst und gewichtet, kann darauf bei jeder Beschaffung zurückgegriffen werden. So kann verhindert werden, dass unter Zeitdruck Komponenten bestellt werden, die die Anforderungen nur unzureichend erfüllen.

Im Rahmen der Anforderungsspezifikation sollten mindestens alle in INF.14.M1 *Planung der Gebäudeautomation* genannten Punkte detailliert festgelegt werden, beispielweise für die Zugriffsmöglichkeiten:

- Vorgaben für die IT-Systeme, die auf eine GA-relevante Komponente einen Zugriff erhalten
- Festlegung der erlaubten Zugriffsmöglichkeiten, z. B. Remote-Zugriff nur über Sprungserver
- Festlegung der erlaubten Rollen und Berechtigungen für die Zugriffe
- Vorgabe der zu nutzenden Protokolle für die zuvor spezifizierten Zugriffe
- Festlegung der zu aktivierenden Sicherheitsfunktionen für die erlaubten Protokolle, z. B. sichere Verschlüsselung, Authentisierung, Autorisierung und Integritätsschutz
- Einschränkung der Zugriffsmöglichkeiten, inklusive Zugriffsmöglichkeiten im Notbetrieb
- Vorgabe von erweiterten Sicherheitsmechanismen für die Zugriffe, z. B. 4-Augen-Prinzip für administrative Zugriffe

Die Anforderungsspezifikation für die GA bildet die Basis für die Grobkonzeptionierung (siehe INF.14.M9 *Entwicklung eines GA-Konzepts*) und für die Detailplanung (siehe INF.14.M1 *Planung der Gebäudeautomation*).

INF.14.M9 Entwicklung eines GA-Konzepts (S)

Die Konzeption der GA sollte unter Berücksichtigung der Rahmenbedingungen sowie unter Einhaltung der Anforderungen festgelegt werden und stellt so die Grundlage für einen zuverlässigen und wirtschaftlichen Betrieb dar. Sie beschreibt die Architektur der GA sowie alle Aufgaben und Vorgaben in der GA und ist somit auch bei einem Wechsel der Betreiberorganisation oder bei Erweiterungen der GA von Bedeutung. Für die Entwicklung eines GA-Konzepts sollten sowohl organisatorische als auch technische Fragestellungen beantwortet werden.

Das GA-Konzept stellt eine Grobkonzeptionierung der GA dar und wird in der Detailplanung konkretisiert (siehe INF.14.M1 *Planung der Gebäudeautomation*). Es sollten alle Themen der Sicherheitsrichtlinie und der Anforderungsspezifikation aufgegriffen werden und für alle GA-Systeme sollten grundlegende Festlegungen getroffen werden. Im GA-Konzept sollten mindestens folgende Aspekte ersichtlich sein:

- Gestaltung der GA, insbesondere Aufteilung in GA-Systeme und Unterteilung des Gebäudes in dediziert zu steuernde Einheiten (GA-Segmente oder -Bereiche)
- Funktionsbeschreibung der angebundenen TGA-Anlagen und Automationsschemata
- Schnittstellen der GA-Systeme zu anderen Systemen, z. B. TGM
- Abhängigkeiten zwischen GA-Systemen und anderen Systemen
- Kommunikations- und Übertragungsprotokolle
- Netzarchitektur der GA inklusive Segmentierung
- Sicherung der Verfügbarkeit, z. B. durch Redundanzen
- Generelles Rollen- und Berechtigungskonzept
- Reglementierung und Absicherung der Zugriffe

Die Konzeption der GA sollte regelmäßig und zusätzlich auch bei Bedarf geprüft und gegebenenfalls aktualisiert werden, um dem aktuellen Stand der Technik zu entsprechen und auch neueste Erkenntnisse abdecken zu können. Außerdem sollte regelmäßig ein Soll-Ist-Vergleich zwischen den Vorgaben der Konzepte und dem aktuellen Zustand durchgeführt werden, um unerlaubte Abweichungen von den Konzepten aufzudecken, aber auch um gegebenenfalls notwendige Aktualisierungen der Konzepte erkennen zu können.

INF.14.M10 Bildung von unabhängigen GA-Bereichen (S)

GA-Bereiche, die gleiche Funktionen bereitstellen, sollten mit gleichartiger Technik realisiert werden, um Planungsvorgänge, Betriebsabläufe und Betriebsstabilität der GA insgesamt zu optimieren. Beispielsweise können Etagen mit gleichartigen Büroräumen oder Besprechungsräume mit vielen GA-relevanten Komponenten, z. B. mit Licht, Verdunklung, Klimatisierung, Medientechnik und Zutrittskontrolle, jeweils als GA-Bereiche eingerichtet werden, die dann im Rahmen der Raumautomation separat gesteuert werden können.

Hinsichtlich Netzarchitektur und Adressierung bzw. Subnetzbildung sollten derartige GA-Bereiche wie im Folgenden beschrieben separiert werden. Hierdurch wird eine Beeinträchtigung eines anderen GA-Bereichs vermieden, z. B. wenn eine GA-relevante Komponente durch einen Fehlerzustand das Subnetz mit Broadcast-Nachrichten flutet. Auch im GA-Management sollten die GA-Bereiche erkennbar und separat steuerbar sein.

Gemäß den Sicherheitsanforderungen sollten für GA-Bereiche jeweils dedizierte Netzkomponenten genutzt werden. Die IP-Adressierung sollte so geplant werden, dass die GA-Bereiche einheitliche Subnetze hinsichtlich Größe und Strukturierung erhalten, die an übergeordneten Layer-3-Switches zusammengefasst werden können. Hierdurch werden die Routing-Tabellen für eine eventuelle Fehlersuche optimiert.

Vorbereitend für die Strukturierung der GA in GA-Bereiche und die Gestaltung von GA-Bereichen sollten alle Abhängigkeiten zwischen den vorgesehenen GA-Bereichen und sonstigen GA-relevanten Komponenten erfasst werden.

Die Kommunikation mit GA-Bereichen sollten abhängig von den Sicherheitsanforderungen der GA oder einzelner GA-Bereiche durch Firewall-Funktionen kontrolliert und reglementiert werden. Um GA-Bereiche voneinander zu trennen, ohne die Netzarchitektur der jeweiligen GA-Bereiche zu ändern, können transparente Firewalls vorgeschaltet werden. Diese ermöglichen eine Kontrolle innerhalb eines IP-Subnetzes. Die transparenten Firewalls müssen im Netzplan dokumentiert werden, da bei einer fehlenden Dokumentation das Entdecken dieser Firewalls im Rahmen einer Fehlersuche einen hohen Aufwand verursachen kann.

INF.14.M11 Absicherung von frei zugänglichen Ports und Zugängen der GA (S)

Frei zugängliche Netzports

Über frei zugängliche Netzports, z. B. über LAN-Ports von Bedien- und Anzeigeeinrichtungen in Räumen, kann ein unautorisierter Zugriff auf das GA-Netz erfolgen. Daher sollten diese geeignet abgesichert werden. Dies sollte über eine Netzzugangskontrolle (Network Access Control, NAC) erfolgen, die möglichst immer nach dem Standard IEEE 802.1X umgesetzt wird.

Für NAC ist hierzu ein sogenannter Authentication Server erforderlich, der die Authentisierung über RADIUS und bei IEEE 802.1X zusätzlich über EAP durchführt. Der Authentication Server sollte redundant ausgelegt werden, um eine hohe Verfügbarkeit des Authentisierungsdiensts zu gewährleisten. Der Authentication Server sollte dabei von der Betreiberorganisation der GA bereitgestellt und betrieben werden.

Um eine möglichst sichere Authentisierung zu gewährleisten, sollten möglichst nur GA-relevante Komponenten eingesetzt werden, die eine Authentisierung über sichere EAP-Methoden unterstützen. Mindestens sollte die NAC-Lösung aber auf Basis einer MAC-Adress-Authentisierung nur registrierten GA-relevanten Komponenten den Zugang zu GA-Netzen ermöglichen.

Für die Umsetzung einer standardkonformen NAC-Lösung in GA-Netzen ist die Unterstützung von IEEE 802.1X durch die Switches erforderlich, an die die GA-relevanten Komponenten angeschlossen werden. Sollten diese Switches IEEE 802.1X nicht oder nur unzureichend unterstützen, sollte geprüft werden, ob die im Standard beschriebenen Funktionalitäten auf der nächst höheren Netzebene implementiert werden können. Zum Beispiel ist es möglich, dass ein Switch kein IEEE 802.1X unterstützt, aber dafür der übergeordnete Access-Switch (siehe Abbildung 7).

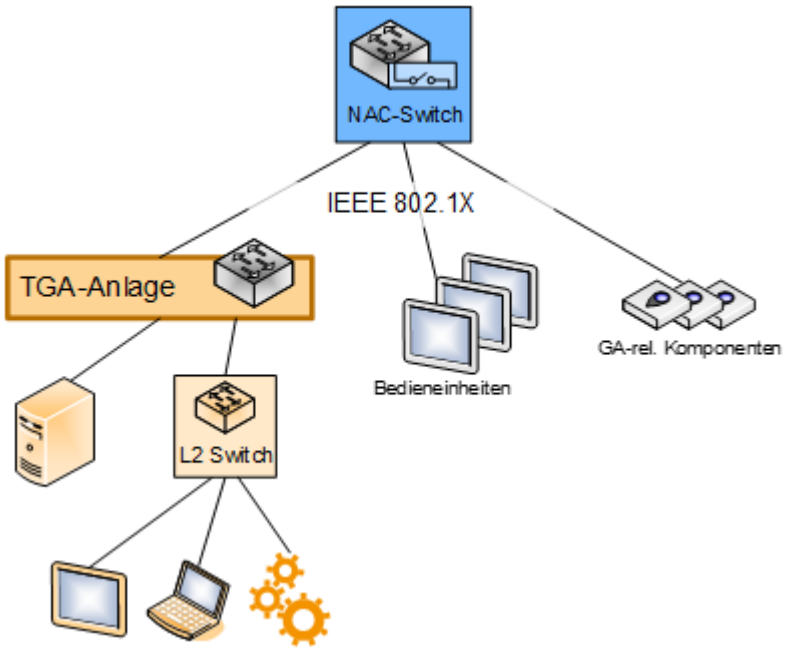

Abbildung 7: Absicherung von frei zugänglichen Ports über NAC

Die Verlagerung der Funktion auf die nächst höhere Netzebene ist aber nur unter den folgenden Voraussetzungen möglich:

- Die Switches der übergeordneten Netzebene sollten an einem Access-Port mehrere Authentisierungssitzungen individuell handhaben können. Dies schließt die individuelle Behandlung einer Sitzung (zulassen oder sperren) wie die individuelle Zuweisung eines Segments je Sitzung mit ein. Andernfalls können, beispielsweise durch Anschluss eines weiteren Switches am Access-Port, der die Authentisierung durchführt, mehrere MAC-Adressen sichtbar werden und zu einer Deaktivierung des Ports für alle Sitzungen führen.
- Wird EAP zur Authentisierung genutzt, muss der authentisierende Access-Switch EAPoL-Pakete der Endgeräte erhalten. Zwischengeschaltete Switches müssen daher EAPoL-Pakete an die nächsthöhere Netzebene weiterleiten können. Ist dies nicht der Fall, kann eine Authentisierung mittels EAP nicht durchgeführt werden und es muss eine weniger sichere Methode zur Authentisierung gewählt werden.

- Bei der Kaskadierung von mehreren Switches kann es vorkommen, dass der für die Authentisierung genutzte übergeordnete Switch das Ausschalten oder Abstecken einer GA-relevante Komponente nicht mitbekommt. Die Switches mit IEEE-802.1X-Funktionalität sollten Sitzungen von nicht mehr angeschlossenen Systemen erkennen und beenden können, damit keine nicht benötigten Sitzungen offen bleiben und missbraucht werden können.

Für eine Authentisierung von GA-relevanten Komponenten mittels IEEE 802.1X muss eine GA-Komponente einen sogenannten Supplicant nutzen. Bei einer hohen Anzahl von zu verwaltenden Endgeräten ist es besonders relevant, auf eine mögliche zentrale Verwaltung von NAC-Konfigurationen und Anmeldeinformationen zu achten, da bei individueller Konfiguration sehr hohe Betriebsaufwände entstehen.

Unterstützt ein Endgerät keinen Supplicant, kann eine Authentisierung über RADIUS auf Basis der MAC-Adresse durchgeführt werden, sobald das entsprechende Endgerät aktiv Daten aussendet.

Ist eine standardkonforme Netzzugangskontrolle für frei zugängliche Netzports wie oben beschrieben nicht möglich, sollten die Ports mindestens über eine der folgenden Maßnahmen geschützt werden:

- Vorschaltung einer Sicherheitskomponente
  Zwischen Port und Access Switch sollte eine transparente Sicherheitskomponente vorgeschaltet werden, die sicherstellt, dass kein unautorisiertes Gerät an dem frei zugänglichen Port angeschaltet wird.
- Manuelle Einschränkung der Kommunikation am Access Switch (Port Security)
  Access-Switch-Ports, die frei zugängliche GA-relevante Komponenten anbinden, sollten so konfiguriert werden, dass die Kommunikation auf Basis erwünschter IP-Adressen und TCP-Ports eingeschränkt wird.
- Manuelle Freischaltung
  Die frei zugänglichen Ports sollten grundsätzlich deaktiviert sein und nur bei Bedarf manuell freigeschaltet werden. Für diese organisatorische Maßnahme sollten entsprechende Betriebsprozesse angepasst werden.
- Physische Sicherung der Ports
  Wenn die manuelle Aktivierung der Netzports nicht umzusetzen ist, sollten Netzports physisch abgesichert sein, so dass nur nach Genehmigung der physische Anschluss für Systeme möglich ist. Beispielsweise können die Ports in Schließschränken positioniert werden oder durch Schlösser gesichert werden.
- Nutzung von nicht-standardkonformen NAC-Lösungen
  Wird für Netzports nur eine nicht-standardkonforme bzw. proprietäre NAC-Lösung unterstützt, so kann diese temporär zur Absicherung genutzt werden. Solche Lösungen basieren häufig auf SNMP oder der Anmeldung an einem Portal oder realisieren ein Monitoring und Alarmierung auf bekannte und unbekannte MAC-Adressen. Häufig haben diese Lösungen das Manko, dass Kommunikation zugelassen werden muss, bevor eine Authentisierung und Autorisierung der NAC-Lösung erfolgt, und nicht sitzungsbasiert, sondern portbasiert erfolgt.

Nach einer erfolgreichen Authentisierung erfolgt am Access-Port eine Zuweisung zu den berechtigten Ressourcen. Hier kann beispielsweise eine dynamische Zuweisung zu vorhandenen Netzsegmenten erfolgen (siehe auch INF.14.M6 *Separierung von Netzen der GA* und INF.14.M13 *Netzsegmentierung in der GA*). Dies gilt auch für Ports in GA-Netzen, die für einen Anschluss von speziellen Wartungsgeräten bereitgestellt werden und frei zugänglich sind. Diese Ports sollten einem dedizierten Service-Segment zugeordnet werden, das durch eine Firewall vom restlichen GA-Netz getrennt wird. Die Firewall sollte die Kommunikation kontrollieren und gegebenenfalls reglementieren. Das Service-Segment sollte dem entsprechenden Port möglichst automatisiert über eine Netzzugangskontrolle zugewiesen werden. Eine NAC-Lösung kann in der Regel die Geräte automatisiert erkennen, diese dem Service-Segment zuordnen und den Zugriff protokollieren. Vor Zuweisung des Service-Netzes, d. h. vor einer

erfolgreichen Authentisierung und Autorisierung, sollte ein Zugriff durch das angeschlossene Wartungsgerät blockiert werden.

Frei zugängliche Ports an GA-relevanten Komponenten

Bieten GA-relevante Komponenten frei zugängliche Schnittstellen für Wechseldatenträger oder mobile Endgeräte, z. B. USB-Schnittstellen, sollten diese deaktiviert oder geschützt werden. Solche Schnittstellen sind beispielsweise häufig an Bedienelementen in Räumen verfügbar. Diese sollten wie frei zugängliche Netzports nur bei Bedarf aktiviert werden oder durch ein Schloss gesichert werden.

Lokale Konsolenports an GA-relevanten Komponenten

Ein notwendiger Zugriff auf den lokalen Konsolenport einer GA-Komponente sollte sich auf die Erstkonfiguration im Rahmen der Inbetriebnahme beschränken. Danach sollte die Konfiguration ausschließlich über einen geeignet abgesicherten Netzzugriff erfolgen. Der lokale Konsolenport wird meist nicht deaktiviert, um für einen Netzausfall einen alternativen Zugriff zu gewährleisten.

Der Zugriff auf den Konsolenport sollte grundsätzlich durch ein individuelles Passwort gesichert und auf autorisierte Zugänge beschränkt werden. GA-relevante Komponenten, die diese Mindestanforderungen an die Zugriffskontrolle nicht erfüllen können, sollten nur nach einer Risikoanalyse mit zusätzlichem physischem Schutz eingesetzt werden.

Der physische Zugang zu lokalen Konsolenports an frei zugänglichen GA-relevanten Komponenten mit Bedienfunktion kann beispielsweise über ein Port-Schloss erfolgen. GA-relevante Komponenten, die nicht unmittelbar von Nutzern erreichbar sein müssen, können in abschließbaren Schränken positioniert werden.

INF.14.M12 Nutzung sicherer Übertragungsprotokolle für die GA (S)

Schützenswerte Informationen sollten sicher übertragen werden. Dies kann realisiert werden, indem Protokolle, die nach dem derzeitigen Stand der Technik als sicher eingestuft werden, für die Kommunikation genutzt werden. Beispielsweise können die Protokolle HTTPS und FTPS als sicher eingestuft werden, wenn sie TLS nach Stand der Technik für die Verschlüsselung nutzen.

Nutzen GA-relevante Komponenten proprietäre Kommunikationsprotokolle, so sollte für diese geprüft werden, ob die Protokolle als sicher einzustufen sind bzw. sicher konfiguriert werden können.

Als unsicher einzustufende Protokolle wie Telnet oder FTP bzw. TFTP sollten nur genutzt werden, wenn die GA-relevanten Komponenten ausschließlich in einem vertrauenswürdigen Segment kommunizieren oder die Verbindung nach Stand der Technik angemessen verschlüsselt und authentisiert ist (siehe NET.3.3 *VPN*).

Schnittstellen, die über unsichere Protokolle erreichbar sind, sollten grundsätzlich deaktiviert werden, um einen unbefugten Zugriff auf die GA-relevanten Komponenten zu verhindern.

INF.14.M13 Netzsegmentierung in der GA (S)

Das GA-Netz sollte in mehrere Netzsegmente gemäß dem individuellen Schutzbedarf aufgeteilt werden. Basis für die Netzsegmentierung ist eine zu erstellende Kommunikationsmatrix der GA, die erfasst, welche GA-relevanten Komponenten innerhalb eines GA-Systems miteinander kommunizieren und welche Kommunikationsbeziehungen zu Zielen außerhalb eines GA-Systems bestehen. Es sollte auch erfasst werden, welche Protokolle zum Einsatz kommen und welche Nachfrage- bzw. Betreiberorganisation beteiligt sind.

Die Kommunikation innerhalb von Netzsegmenten wird nicht reglementiert. Jedoch sollte die netzsegmentübergreifende Kommunikation kontrolliert und auf das betrieblich notwendige Maß reduziert werden. Der Verbindungsaufbau sollte grundsätzlich aus dem Netzsegment mit dem höheren Schutzbedarf in das Netzsegment mit dem niedrigeren Schutzbedarf aufgebaut werden. Für die Reglementierung der Kommunikation sollte eine Firewall genutzt werden (siehe auch Baustein NET.1.1 *Netzarchitektur und -design*).

Mindestens sollten die folgenden Netzbereiche als Netzsegmente in Betracht gezogen werden:

- GA-Systeme
- Gruppen von TGA-Anlagen innerhalb eines GA-Systems
- einzelne TGA-Anlagen innerhalb eines GA-Systems
- GA-relevante Komponenten von Nachfrageorganisationen
- von verschiedenen Betreiberorganisationen verantwortete Netzbereiche

Umfasst ein GA-System verschiedene Gebäude, die gegebenenfalls über unzureichend vertrauenswürdige Verbindungen gekoppelt sind, sollte hier eine Segmentierung gemäß Baustein NET.1.1 *Netzarchitektur und -design* umgesetzt werden. GA-Systeme, die mehrere Gebäude über vertrauenswürdige Verbindungen, z. B. LAN-Erweiterungen über Dark Fiber, umfassen, können in einem Netzsegment zusammengefasst werden, sofern nicht andere Gründe eine Segmentierung bedingen.

Die Segmentierung innerhalb von TGA-Anlagennetzen erfolgt nach den Vorgaben der jeweils relevanten IND-Bausteine, z. B. IND.1 *Betriebs- und Steuerungstechnik*.

Bei der Konzeption und Umsetzung der Netzsegmentierung müssen alle betrieblichen Abhängigkeiten und Anforderungen ermittelt und analysiert werden. Die Netzsegmentierung darf die geforderte Betriebsstabilität nicht beeinträchtigen.

Die eingerichteten Netzsegmente sowie die Kommunikationsmatrix sollten regelmäßig und zusätzlich bei Bedarf, z. B. bei Erneuerung einer TGA-Anlage, geprüft und gegebenenfalls angepasst werden. Basis hierfür ist eine vollumfängliche Dokumentation der Segmentierung, die auch alle eingesetzten Sicherheitselemente zur Segmentierung, insbesondere auch transparente Firewalls zur Mikrosegmentierung, erfasst.

Mikrosegmentierung von unzureichend sicheren GA-relevanten Komponenten

Um die Gesamtheit der GA zu schützen, sollten GA-relevante Komponenten, die nur eine unzureichende Sicherheit umsetzen, separiert werden. Beispielsweise sollten nicht-patchbare Komponenten wie Sensoren oder Aktoren in dedizierten Segmenten verortet werden. Die Mikrosegmentierung sollte die resultierende Gefährdung durch die unzureichend sicheren Komponenten berücksichtigen und verschiedene Varianten der Segmentierung in Betracht ziehen:

- Abtrennung von einzelnen Komponenten oder TGA-Anlagen (siehe Maßnahme 14.M29 *Trennung einzelner TGA-Anlagen*)
- Sammeln von unsicheren, z. B. mit Schwachstellen behafteten, Komponenten in Mikrosegmenten
- Abschottung des restlichen Netzes vor Komponenten, die keinen ausreichenden Zugriffsschutz bieten

Abhängig von den entsprechenden Sicherheitsrichtlinien sollte die Anbindung von Mikrosegmenten weitestgehend einheitlich erfolgen.

Für die Absicherung von Mikrosegmenten werden häufig transparente Firewalls auf OSI Layer 2, auch Inline-Firewall genannt, eingesetzt. Transparente Firewalls ermöglichen eine Kontrolle innerhalb eines IP-Subnetzes.

Insbesondere wenn ein Mikrosegment nur eine GA-relevante Komponente enthält, kann die Kommunikation am Übergang, also dem Netzanschluss, kontrolliert werden, indem beispielsweise Netzkomponenten mit ACLs eingesetzt werden (siehe auch Baustein NET.2.1 *Router und Switches* sowie NET.3.2 *Firewall*). Hierauf werden z. B. dynamische ACL (dACL) über eine Netzzugangskontrolle auf den entsprechenden Port geladen.

INF.14.M14 Nutzung eines GA-geeigneten Zugriffschutzes (S)

Um einen sicheren Zugriffsschutz für die GA zu gewährleisten, sollte für die GA ein Identitäts- und Berechtigungsmanagement gemäß Baustein ORP.4 *Identitäts- und Berechtigungsmanagement*

umgesetzt werden. Eine wesentliche Grundlage liefert hierzu ein spezifisches Rollen- und Berechtigungskonzept für die GA, das die Verantwortlichkeiten und Zuständigkeiten im Gebäude angemessen berücksichtigt. Insbesondere muss die Konstellation mit gegebenenfalls mehreren Nachfrage- und Betreiberorganisationen berücksichtigt werden (siehe auch INF.14.M2 *Festlegung eines Inbetriebnahme- und Schnittstellenmanagements für die GA* und Baustein INF.13 *Technisches Gebäudemanagement*).

Authentisierungslösung

Für die Umsetzung des Rollen- und Berechtigungskonzepts sollte eine Authentisierungslösung eingesetzt werden, in das möglichst alle GA-relevanten Komponenten eingebunden werden. Die Authentisierungslösung sollte abhängig von den Anforderungen der GA an Autarkie und der Konstellation im Gebäude als unabhängige Lösung für die GA eingerichtet werden. Hierbei muss die Betreiberorganisation der GA den vollständigen Betrieb der Lösung inklusive Notfallvorsorge übernehmen. Alternativ kann für die GA eine Replikation einer Authentisierungslösung, die auch von anderen IT-Bereichen genutzt wird, eingerichtet werden. Hierbei erfolgt der Betrieb durch den IT-Betrieb der Institution. Auch eine solche Replikation kann so eingerichtet werden, dass gewisse Autarkie-Anforderungen der GA erfüllt werden. Beispielsweise gewährleistet eine Replikation die Authentisierung auch bei Ausfall der Netzverbindung zur zentralen Instanz.

Die Abwägung der geeigneten Variante sollte grundsätzlich die Konstellation von Nachfrage- und Betreiberorganisationen im Gebäude berücksichtigen.

Rollen

Die Organisation der Berechtigungen auf die Funktionen der GA erfolgt zweckmäßigerweise in Rollen. Eine Rolle wird eingerichtet, wenn mehrere Benutzer die gleichen Berechtigungen für die gleichen Objekte erhalten sollen. Dadurch wird verhindert, dass bei Änderungen der Berechtigungen jeder Nutzer einzeln angepasst werden muss. Die notwendigen Rollen für die GA ergeben sich aus der jeweiligen Konstellation von Nachfrage- und Betreiberorganisationen für das Gebäude und den organisatorischen Regelungen innerhalb der Organisationen.

Es muss sichergestellt werden, dass die eingerichteten Rollen die Konstellation eines Gebäudes derart abbilden, dass Informationen über GA-relevante Komponenten nur einer berechtigten Institution bzw. Nachfrageorganisation zugänglich sind. Insbesondere darf eine Nachfrageorganisation keine Information über die spezifischen GA-relevanten Komponenten einer anderen Nachfrageorganisation erhalten.

Beispielsweise wird für eine Nachfragorganisation, z. B. ein Mieter, eine Rolle mit einem lesenden Zugriff auf die zentrale Gebäudeinfrastruktur eingerichtet. Vollen Zugriff auf die zentrale Gebäudeinfrastruktur erhält nur die zuständige Betreiberorganisation.

Jedem Benutzer können eine oder mehrere Rollen zugewiesen werden und umgekehrt einer Rolle ein oder mehrere Benutzer. Bei Anmeldung an einem GA-System wird die Rolle des angemeldeten Benutzers ausgelesen und auf der Grundlage der zugewiesenen Berechtigungen eine entsprechende Bedienoberfläche mit verfügbaren Funktionen angezeigt.

Rollen, zugewiesene Benutzer und Berechtigungen sollten gemäß dem Lebenszyklus der GA vergeben werden. Insbesondere sollten Rollen, Benutzer und Berechtigungen, die ausschließlich während der Bauphase erforderlich sind, entzogen werden bzw. auf die Betriebsphase angepasst werden. Auch sollten diese bei Wechsel einer Nachfrageorganisation, z. B. durch Auszug eines Mieters, entsprechend angepasst werden.

Berechtigungen

In der Regel werden für die beschriebenen Rollen drei aufeinander aufbauende Berechtigungsstufen vorgesehen, die pro Rolle für eine Bedien- und Managementfunktion der GA festgelegt werden:

- nur lesender Zugriff auf Parameter der GA
- lesender und schreibender Zugriff, d. h. Änderungen an Parametern sind erlaubt

- Lesen und Schreiben sowie auch Anlegen oder Löschen von Parametern, Grenzwerten, Profilen usw.

Die vollumfänglichen Berechtigungen sind meist nur während der Inbetriebnahme oder für größere Umstellungen von GA-Funktionen erforderlich und sollten nur besonders qualifizierten Benutzergruppen und Administratoren zugewiesen werden.

Die Berechtigungen sollten den Rollen so zugwiesen werden, dass die Benutzer nur auf solche Informationen zugreifen dürfen, die zur Erfüllung der jeweiligen Aufgabe benötigt werden und die ihrem Verantwortungsbereich entsprechen. Beispielsweise sollte eine Nachfrageorganisation, z. B. ein Mieter, nur auf solche Informationen schreibend zugreifen dürfen, für die sie die Verantwortung trägt, z. B. eigene WLAN-Installationen. Andere Nachfrageorganisationen sollten hierauf jedoch nicht zugreifen können.

Umgang mit Wartungsgeräten

Wartungsgeräte oder Engineering-Werkzeuge, die an GA-relevante Komponenten direkt angeschlossen werden, stellen eine besondere Gefährdung für die Sicherheit des gesamten GA-Systems dar und müssen im Rollen- und Berechtigungskonzept besonders berücksichtigt werden.

Solche Werkzeuge, die zur Inbetriebnahme oder Wartung genutzt werden, sollten grundsätzlich nur angeschlossen werden dürfen, wenn sie über einen aktuellen Schutz vor Schadsoftware und über einen aktuellen Patch-Level verfügen.

Darüber hinaus sind Konsolenports bei manchen GA-relevanten Komponenten für den Anschluss von Wartungsgeräten oft nicht ausreichend abgesichert, d. h. ein Zugriff ist ohne Nutzerkennung und Passwort möglich oder die vom Hersteller vorgegebenen Zugriffsparameter können nicht geändert werden. Solche Komponenten sollten nicht genutzt werden bzw. kurz- bis mittelfristig ersetzt werden. Auch Komponenten, die über Netze ohne ausreichenden Zugriffsschutz administriert werden können, sollten ersetzt oder über ergänzende Maßnahmen abgesichert werden. Mindestens sollten dabei Maßnahmen wie eine Segmentierung (siehe INF.14.M13 *Netzsegmentierung in der GA*) von Wartungsgeräten, gegebenenfalls in Verbindung mit einer Netzzugangskontrolle (siehe INF.14.M11 *Absicherung von frei zugänglichen Ports und Zugängen der GA*), einen entsprechenden Schutz für andere Netzbereiche gewährleisten.

INF.14.M15 Absicherung von GA-spezifischen Netzen (S)

Für GA-spezifische Netze wie beispielsweise BACnet, KNX oder M-Bus sollten dieselben Sicherheitsmaßnahmen umgesetzt werden, die auch für das jeweilig übergeordnete Netzsegment erforderlich sind, insbesondere eine Authentisierung der Kommunikationspartner und gegebenenfalls eine Verschlüsselung der Kommunikation. Dies sollte auch für industrielle Feldbusse gemäß IEC 61784-1 und IEC 61784-2, die teilweise auch im Rahmen der GA genutzt werden, sowie für eine Datenübertragung über Stromleitungen (PowerLAN) umgesetzt werden.

Die Absicherung der Kommunikation sollte mit einem Mechanismus erfolgen, der nach Stand der Technik als sicher gilt, z. B. BACnetSC mit derzeit TLS 1.3 für IPv4 und IPv6.

Unterstützt eine GA-Komponente keine angemessene Absicherung, sollte der Einsatz im Rahmen der Risikoanalyse überprüft werden. Beispielsweise können manche älteren Systeme aufgrund von knappen Ressourcen die Anforderungen nicht umsetzen. Auch wenn der Einsatz von solchen Komponenten im Rahmen der Risikoanalyse erlaubt wird, sollte ein Austausch der GA-relevanten Komponenten geplant und umgesetzt werden, sobald dies technisch möglich ist. Bis zum Austausch sollten diese GA-relevanten Komponenten in dedizierten Subnetzen konzentriert werden, deren Kommunikation dann am Übergang zum restlichen Netz kontrolliert und reglementiert wird. Die erforderlichen Firewall-Funktionen können durch das Gateway, das das IP-basierte Netz mit dem GA-spezifischen Netz koppelt, oder durch eine vorgeschaltete Firewall umgesetzt werden (siehe auch INF.14.M13 *Netzsegmentierung in der GA*).

Die Gateways zu einem GA-spezifischen Netz sollten grundsätzlich derart konfiguriert werden, dass ausschließlich erlaubte Kommunikation weitergeleitet wird. Beispielsweise können für GA-spezifische

Netze, die auf Ethernet basieren, wie z. B. BACnet/IP, Switches genutzt werden, die Access Control Lists (ACLs) unterstützen. Falls Übergangskomponenten verfügbar sind, die angemessene Firewall-Funktionen zur Kontrolle und Reglementierung der Kommunikation bereitstellen, sollten diese Funktionen genutzt werden. Falls die Gateways keine angemessenen Sicherheitsfunktionen unterstützen, kann eine transparente Layer-2-Firewall vor einem Gateway ohne Sicherheitsfunktionen positioniert werden.

Auch sollte das Netz so strukturiert werden, dass kein Kurzschluss des Netzes über ein GA-spezifisches Netz oder eine Übergangskomponente ermöglicht wird. Beispielsweise sollte ein Gateway, das zwei BACnet-Segmente anbindet, so konfiguriert werden, dass eine unautorisierte Weiterleitung der Kommunikation zwischen den Segmenten unterbunden wird.

INF.14.M16 Absicherung von drahtloser Kommunikation in GA-Netzen (S)

Neben Techniken wie WLAN, Bluetooth und Richtfunk, die auch in der IT eingesetzt werden, nutzt die GA auch andere drahtlose Kommunikationstechniken. Wichtige Beispiele sind:

- Bluetooth Low Energy (BLE)
  BLE mit einer Reichweite von etwa 10 Metern funkt im Frequenzbereich von 2,4 GHz und unterstützt in aktuellen Versionen eine Absicherung über AES-CCM mit 128 Bit Schlüssellänge.
- BACnet über Zigbee
  Zigbee wurde zunächst für drahtlose Sensor- und Steuernetze spezifiziert, realisiert eine Reichweite von ca. 15 m und nutzt Frequenzen im Bereich 2,4 GHz und 868 MHz. Die Zigbee-Kommunikation erfolgt grundsätzlich verschlüsselt mit AES-128 oder AES-256.
- Long Range Wide Area Network (LoRaWAN)
  LoRaWAN mit einer Reichweite von bis zu 40 km (in ländlichen Gebieten) nutzt die Frequenzbereiche 868 MHz oder 434 MHz. Die Kommunikation wird mit AES-128 verschlüsselt.
- EnOcean
  EnOcean kann in freiem Gelände mit batterielosen Geräten eine Reichweite von bis zu 300 m erreichen und nutzt den Frequenzbereich 868 MHz. Die Kommunikation kann mit AES-128 verschlüsselt werden.
- KNX-RF
  KNX-RF mit einer Reichweite von bis zu 150 m nutzt den Frequenzbereich von 868 MHz und verschlüsselt die Kommunikation mittels AES-CCM (mit 128 Bit Schlüssellänge.
- IP500
  Die IP500 Alliance spezifiziert einen Industriestandard für Funkanwendungen mit besonderen Anforderungen an Robustheit und Sicherheit. Er basiert auf drahtloser Übertragung mittels IEEE 802.15.4 (Wireless Personal Area Network, WPAN) oder 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks), nutzt grundsätzlich IPv6 und sichert die Kommunikation mittels IPsec mit AES-128. IP500 sieht ein Dualband-Verfahren vor, das im Frequenzbereich 2,4 GHz und 900 MHz agiert.

Darüber hinaus nutzen einige Produkte in der GA auch funkbasierte Feldbusse, die bevorzugt im Umfeld der Operational Technology (OT) zum Einsatz kommen, sowie proprietäre Funktechniken.

Falls im Rahmen der GA WLAN genutzt wird, sollte der Einsatz mit den anderen Betriebseinheiten abgestimmt werden. Die Absicherung von WLAN wird in den Bausteinen NET.2.1 *WLAN-Betrieb* und NET.2.2 *WLAN-Nutzung* thematisiert. Dabei sollte der Einsatz von NAC in WLAN mit dem Einsatz im kabelbasierten LAN abgestimmt werden (siehe INF.14.M11 *Absicherung von frei zugänglichen Ports und Zugängen der GA*).

Vertraulichkeit und Integrität

Für alle Techniken zur drahtlosen Kommunikation sollte eine Absicherung gemäß dem Stand der Technik genutzt werden. Insbesondere sollte die Kommunikation über die Luftschnittstelle

grundsätzlich verschlüsselt erfolgen. Hier sollten neben WLAN- und Bluetooth-Netzen auch GA-spezifische Netze wie BACnet über Zigbee beachtet werden.

Unterstützt eine GA-relevante Komponente für eine Technik keine nach Stand der Technik sichere Authentisierung und Verschlüsselung auf der Luftschnittstelle, sollte der Einsatz im Rahmen der Risikoanalyse überprüft werden. Beispielsweise können ältere Systeme aktuelle Anforderungen an Zertifikate zur Authentisierung oft nicht erfüllen bzw. die Verschlüsselung nicht in einer angemessenen Geschwindigkeit umsetzen. In einer Risikoanalyse sollte abgewogen werden, ob mit solcher Kommunikation auch ohne oder mit nur unzureichend sicheren Verschlüsselung eingesetzt werden darf.

Grundsätzlich sollte eine drahtlose Kommunikation auf bekannte GA-relevante Komponenten beschränkt werden. Auf den Zugangspunkten zur drahtlosen Kommunikation, z. B. WLAN Access Points, sollten entsprechende Einschränkungen eingerichtet werden.

Verfügbarkeit

Über die Absicherung der Verfügbarkeit und Integrität hinaus ist in der GA die Sicherstellung der Verfügbarkeit ein wesentliches Element. Für die funkbasierten Netze kann die Verfügbarkeit durch Interferenzen der verschiedenen Funktechniken erheblich beeinträchtigt werden.

Daher sollten in GA-Netzen Interferenzen vermieden werden, die durch parallel genutzte Funktechniken entstehen können, z. B. WLAN, Bluetooth, Zigbee und Richtfunk im 2,4-GHz-Bereich. Aber auch Interferenzen mit sonstigen Netzen, insbesondere mit den Büro- und OT-Netzen, sollten vermieden werden. Hierfür sollten übergreifend alle drahtlosen Netze der Institution erfasst werden. Hierfür sollte als Basis für die Planung und Nutzung von drahtloser Kommunikation alle genutzten Funktechniken sowie deren Ausprägung und Ausleuchtung für alle Gebäude erfasst werden. Hierbei sollten neben WLAN, Richtfunk und Bluetooth auch alle funkbasierten Netze mit geringen Reichweiten berücksichtigt werden.

Für alle verwendeten Frequenzbereiche bzw. Frequenzteilbereiche sollten die Primär- und Sekundärnutzer festgelegt werden. Dabei sollte auch geregelt werden, wie mit Interessenskonflikten innerhalb eines Frequenzbereichs umgegangen wird.

Für alle funkbasierten Netze sollten die Nutzungsparameter festgelegt werden. Beispiele für solche Regelungen sind:

- Da immer mehr Endgeräte und Systeme, beispielsweise aus dem Internet of Things (IoT), Funktechniken im Frequenzbereich 2,4 GHz nutzen, sollte für WLAN bevorzugt das 5-GHz-Frequenzband verwendet werden. So kann eine potenzielle gegenseitige Störung von WLAN- und sonstigen Endgeräten, die im Frequenzbereich bei 2,4 GHz agieren, z. B. Bluetooth-Geräte beim Verbindungsaufbau, ausgeschlossen werden.
  Hinweis: Im normalen Sendebetrieb nutzt Bluetooth durch das Adaptive Frequency Hopping (AFH) in der Regel Frequenzkanäle, die keine spürbaren Störungen mit WLAN-Komponenten erzeugen.
- Für mobile Bluetooth-Geräte mit hoher Sendeleistung sollte festgelegt werden, ob und wie oft ein erneuter Verbindungsaufbau durchgeführt wird, wenn die ursprüngliche Verbindung verloren wurde, um Störungen der anderen Funktechniken im 2,4-GHz-Bereich zu vermeiden.
- Im europaweit festgelegten SRD-Band (Short Range Device, d. h. Kurzstreckengerät), das genehmigungsfrei genutzt werden darf, sollte ebenfalls festgelegt werden, welche GA-relevanten Komponenten bzw. TGA-Anlagen Primärnutzer sind. Beispielsweise sollten GA-relevante Komponenten, die über KNX-RF, LoRaWAN, EnOcean oder Z-Wave kommunizieren, in dem Frequenzbereich um 868 MHz nicht von drahtlosen Mikrofonen, Kopfhörern oder Fernsteuerungen gestört werden.
- Um potenzielle Interferenzen zu verhindern, sollten für die genutzten GA-relevanten Komponenten und Funktechniken verschiedene Frequenzbereiche genutzt werden, z. B. LoRaWAN im Frequenzbereich 434 MHz und EnOcean im Frequenzbereich 868 MHz. Abhängig

von den Funktechniken sollten die Funkparameter so konfiguriert werden, dass die GA-relevanten Komponenten unterschiedliche Frequenzen, Zeitschlitze oder Codes nutzen.

- Werden mehrere Funktechniken für die GA parallel eingesetzt, so sollte vor Inbetriebnahme der GA eine unterbrechungs- und störungsfreie Kommunikation über Funk sichergestellt werden. Hierfür sollte die parallele Kommunikation der GA-relevanten Komponenten getestet werden und gegebenenfalls sollten die Funkparameter wie z. B. Sendekanal oder -leistung geeignet angepasst werden.
- Können Interferenzen durch Anpassung der Funkparameter nicht behoben werden, sollte geprüft werden, ob ein beteiligtes Netz auf eine andere Funktechnik mit gegebenenfalls anderem Frequenzbereich umgestellt werden kann.

Die Verfügbarkeit von GA-relevanter Kommunikation kann auch reduziert werden, wenn die Kommunikation durch metallische Bauteile oder elektromagnetische Strahlung behindert wird. Beispielsweise können metallbedampfte Scheiben oder eine Stahlbetonwand eine drahtlose Kommunikation empfindlich stören und die Kommunikation zwischen GA-relevanten Komponenten unterbinden. Bereits während der Planung der GA sollten mit Hilfe von Simulationen oder ähnlichen Methoden die möglichen Auswirkungen von derartigen Störquellen auf die GA-Kommunikation untersucht und die Ergebnisse in die Planung einbezogen werden.

Zur Minimierung von elektromagnetischen Störquellen sollten zusätzlich die relevanten EMV-Normen berücksichtigt werden (siehe Kapitel Wissenswertes).

In folgenden Fällen sollte ein Einsatz von drahtloser Kommunikation vermieden werden:

- In schwierigen Umgebungsbedingungen, bei denen Störungen in der Kommunikation wahrscheinlich sind
  Beispielsweise können die Funksignale durch die Bausubstanz des Gebäudes stark abgeschirmt werden, so dass eine zuverlässige Kommunikation nicht gewährleistet ist.
- Bei Konflikten mit dem Primärnutzer der Funktechnik
  Beispielsweise kann für WLAN im Frequenzbereich 5 GHz die OT als Primärnutzer festgelegt sein, so dass dieser Frequenzbereich für die GA nicht zur Verfügung steht.
- In Außen- bzw. Grenzbereichen der Institution, wenn ein erhöhtes Störpotenzial oder eine Abschottung durch andere Gebäude wahrscheinlich sind
  Beispielsweise kann im Außenbereich der Funkverkehr durch externe Störquellen unterbunden werden.

INF.14.M17 Absicherung von Mobilfunkkommunikation in GA-Netzen (S)

Je nach Mobilfunktechnik sind unterschiedliche Sicherheitsfunktionen integriert und verfügbar. Daher sollte vor der Verwendung einer bestimmten Mobilfunktechnik überprüft werden, ob deren Sicherheitsfunktionen und das Betriebsmodell für den jeweiligen Anwendungsfall, der in der GA über Mobilfunktechniken umgesetzt werden soll, geeignet sind.

Öffentliches Mobilfunknetz

Wird ein Provider-betriebenes oder öffentliches Mobilfunknetz verwendet, sollte bei dem jeweiligen Provider erfragt werden, welche Sicherheitsmechanismen (z. B. Verschlüsselung) für die verwendete Mobilfunktechnik zum Einsatz kommen. Diese sollten derart umgesetzt werden, dass die Sicherheitsanforderungen an die GA erfüllt werden. Sind die Sicherheitsmechanismen nicht ausreichend für die Sicherheitsanforderungen der übertragenen Informationen, sollten zusätzliche Maßnahmen ergriffen werden, beispielsweise eine zusätzliche eigene Verschlüsselung der übertragenen Daten in der Verantwortung der GA.

Häufig nutzen GA-relevante Komponenten integrierte Mobilfunkendgeräte mit eigenen SIM-Karten zur Anbindung an die Cloud des jeweiligen Herstellers oder an Dienstleister wie den Stromversorger. In diesem Fall sollte eine unkontrollierte Kommunikation über eine solche GA-Komponente mit

anderen GA-relevanten Komponenten verhindert werden, indem die Kommunikation über eine Firewall-Funktion kontrolliert und reglementiert sowie gegebenenfalls entkoppelt wird.

Ebenso sollte – falls möglich - unterbunden werden, dass GA-relevante Komponenten über öffentlichen Mobilfunk dauerhaft an einen Hersteller oder Dienstleister angebunden sind oder dass Hersteller oder Dienstleister eine Verbindung zu GA-relevanten Komponenten einer Institution, z. B. für Auto-Updates, initiieren können. Hier sollten nur temporäre Verbindungen, die von den GA-relevanten Komponenten der Institution initiiert werden, genutzt werden.

Grundsätzlich müssen alle derartigen Verbindungen mit den zugehörigen Parametern umfassend dokumentiert werden.

Privates Mobilfunknetz

Werden Mobilfunknetze privat aufgebaut und betrieben, wie es beispielsweise bei 5G (und in einem gewissen Rahmen bei LTE) möglich ist, sollten die verfügbaren Sicherheitsmechanismen genutzt werden. Hierzu sollten Maßnahmenkataloge und Konfigurationsvorgaben der Hersteller beachtet werden, ebenso wie Hilfestellungen vergleichbar zu der EU Toolbox für 5G der EU-Behörde für Cyber-Sicherheit ENISA. Betreibt ein Provider private Mobilfunknetze in der GA, so sollten für den Betrieb dieser Umgebung auch diese Vorgaben gelten und deren Umsetzung regelmäßig überprüft werden.

Wenn die Mobilfunktechnik virtuelle Mobilfunknetze analog zu Slices in 5G unterstützt, so sollten diese genutzt werden. So können innerhalb der GA spezifische virtuelle Netzbereiche aufgebaut werden, beispielsweise für bestimmte TGA-Anlagen oder für besondere Anforderungen wie Echtzeitübertragung oder sehr hohe Datenraten.

Mindestens bei der Nutzung eines virtuellen Mobilfunknetzes als Teil einer öffentlichen Infrastruktur sollte der Netzverkehr auf Anomalien und Auffälligkeiten überprüft werden.

Der Netzübergang zwischen Mobilfunknetzen und anderen GA-Netzbereichen sollte mindestens durch Firewall-Techniken abgesichert werden. Ist das Vertrauensgefälle zwischen den Netzbereichen zu hoch, beispielsweise zwischen einer Slice als Teil eines öffentlichen 5G-Netzes und Netzen einer kritischen Anlage, sollte die Kommunikation entkoppelt erfolgen.

Zusätzlich sollten für Mobilfunktechniken als drahtlose Übertragungstechniken die Maßnahmen in INF.14.M16 *Absicherung von drahtloser Kommunikation in GA-Netzen* beachtet werden.

Low Power Wide Area Network (LPWAN)

LPWANs, die zunächst primär für IoT-Geräte entwickelt wurden, werden zunehmend auch in der GA genutzt. Der Begriff LPWAN umfasst verschiedene Netzprotokolle, die Niedrigenergiegeräte wie batteriebetriebene Sensoren mit einem Anwendungs-Server verbinden. Mittels LPWAN können Endgeräte trotz niedrigem Energieverbrauch eine vergleichsweise große Reichweite (bis 50 km) bis zum Gateway (auch Basisstation genannt) überbrücken (siehe Abbildung 8).

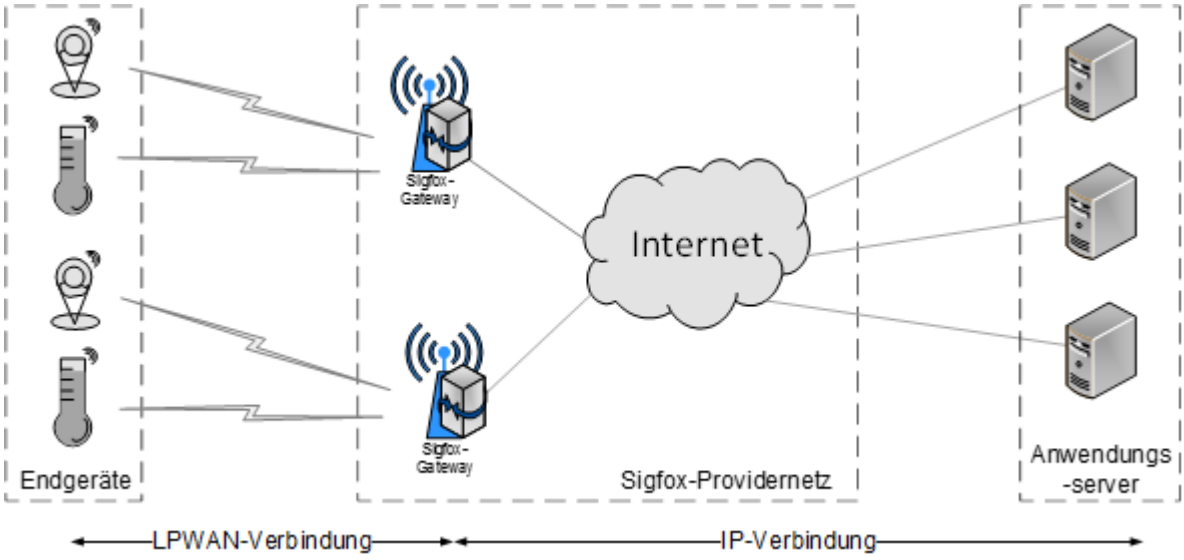

Abbildung 8: Sigfox-Netz

Als kommerzielles LPWAN ist in Deutschland das Sigfox-Netz verfügbar, das das Frequenzband von 868 MHz nutzt. Sigfox-Geräte senden in festgelegten Intervallen maximal 140 kurze Nachrichten pro Tag an eine Basisstation, die diese dann in eine Datenbank des jeweiligen Empfängers weitergibt. Die Funkkommunikation im Sigfox-Netz kann mit AES-128 verschlüsselt werden.

LoRaWAN (siehe auch INF.14.M16 *Absicherung von drahtloser Kommunikation in GA-Netzen*) gehört ebenfalls zur Kategorie der LPWANs, ist aber in Deutschland nicht als Provider-Netz verfügbar. In der Schweiz ist ein flächendeckendes LPWAN der Swisscom verfügbar, das auf LoRaWAN basiert.

Für die Funkkommunikation im LPWAN sollte eine Absicherung gemäß dem Stand der Technik genutzt werden. Wird dies nicht unterstützt, sollte erwogen werden, auf eine andere Technik zu wechseln.

INF.14.M18 Sichere Anbindung von GA-externen Systemen (S)

GA-Systeme kommunizieren oft auch mit GA-externen Systemen, insbesondere im TGM, aber auch mit Systemen der Büro-IT oder OT sowie mit sonstigen Systemen außerhalb der Institution. Hierbei sollten mindestens die folgenden Punkte berücksichtigt werden:

- Alle Abhängigkeiten und Kommunikationswege zwischen GA-Systemen und GA-externen Systemen sollten erfasst und dokumentiert werden.
- Innerhalb eines GA-Systems sollten ausschließlich die GA-Managementsysteme mit GA-externen Systemen kommunizieren. GA-relevante Komponenten der Steuerungs- und Feldebene sollten nur innerhalb eines GA-Systems kommunizieren (siehe auch Abbildung 9).
- Die Kommunikationswege sollten auf definierte Schnittstellen, Protokolle und Systeme eingeschränkt werden. Diese Einschränkung der Kommunikation sollte an geeigneter Stelle im Netz kontrolliert und umgesetzt werden.

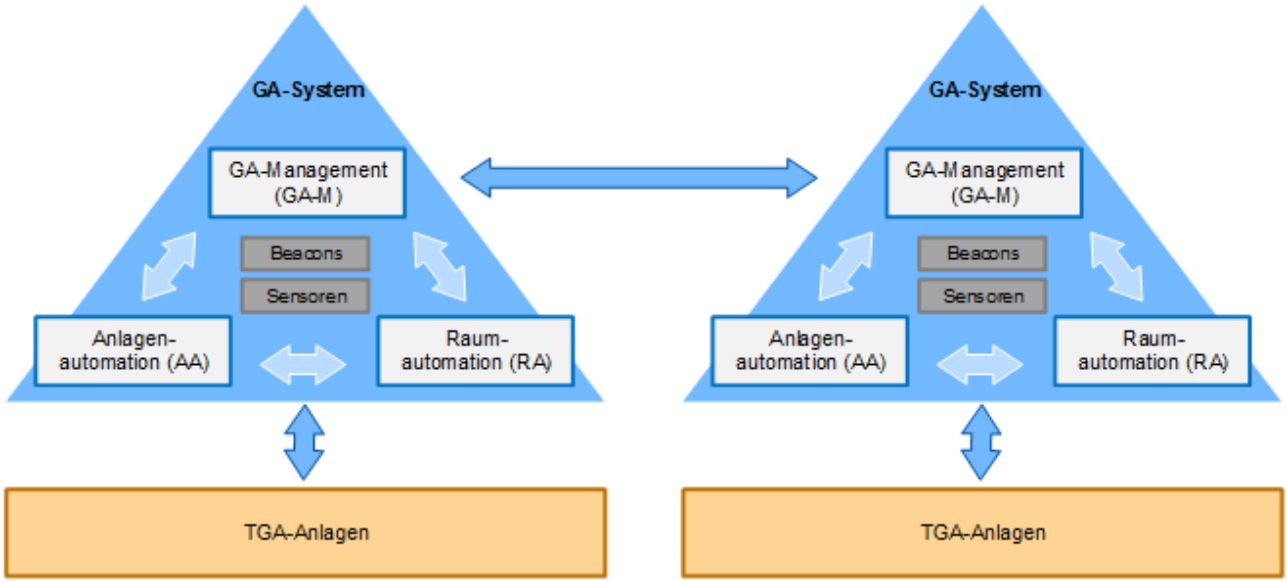

Abbildung 9: Kommunikation eines GA-Systems

Nicht zwingend notwendige Kommunikation sollte nur in begründeten Ausnahmefällen zugelassen werden.

- Ein administrativer Zugriff von GA-externen Systemen auf GA-Systeme sollte ausschließlich entkoppelt erfolgen.

Wenn GA-relevante Komponenten Ressourcen gemeinsam mit TGM, Büro-IT oder OT nutzen, so sollten mindestens folgende Punkte festgelegt werden:

- Die Anforderungen an alle gemeinsam genutzten Ressourcen, beispielsweise Netz, Netzdienste, Authentisierungs- oder Verzeichnisdienste hinsichtlich Verfügbarkeit, Vertraulichkeit und Integrität sollten abgestimmt werden.
- Daraus sollte die notwendige Dienstgüte der gemeinsam genutzten Ressourcen, insbesondere die Einhaltung von geforderten Leistungsparametern, z. B. Bandbreite und Wiederverfügbarkeit bei Ausfällen, abgeleitet werden.
- Die Kommunikationswege bzw. Schnittstellen und Protokolle, über die auf die gemeinsam genutzten Ressourcen zugegriffen werden, sollten festgelegt werden. Wird beispielsweise ein allgemeines Netz zur Kopplung von GA-Segmenten genutzt, sollte festgelegt werden, über welche Switches die Anbindung erfolgt. Für diese Switches sollten dann technische und organisatorische Regelungen abgestimmt werden.
- Die Zuständigkeiten und Berechtigungen hinsichtlich der gemeinsam genutzten Ressourcen sollten spezifiziert werden. Insbesondere sollten die privilegierten Berechtigungen festgelegt werden.
- Für alle Tätigkeiten und alle Komponenten bzw. Ressourcen sollten Prozessdefinitionen erstellt werden. Beispielsweise sollte festgelegt werden, wer für erforderliche Änderungen an einem gemeinsam genutzten Authentisierungsdienst zuständig ist und wer berechtigt ist, diese zu veranlassen.
- Dritte, die in den Betrieb der gemeinsamen Ressourcen involviert sind, sollten ebenfalls in die organisatorische und technische Abstimmung integriert werden.

INF.14.M19 Nutzung dedizierter Adressbereiche für GA-Netze (S)

IP-Adresskonzepte sind meist auf den Bedarf der Büro-IT zugeschnitten und adressieren primär die Bereitstellung von Adressen für Arbeitsplätze. Diese können nicht einfach für die GA übernommen werden, da in den IP-Adresskonzepten für die GA insbesondere die Vielzahl der GA-relevanten Komponenten zu berücksichtigen ist. Daher sollten für die GA möglichst IP-Adressbereiche reserviert und genutzt werden, die von sonstigen Adressbereichen, insbesondere der Büro-IT und OT, überlappungsfrei getrennt sind. Der Adressbereich sollte für die gesamte GA der Institution, d. h. für alle Gebäude, dimensioniert sein und zusammenhängend bereitgestellt werden, damit die Routing-Übergänge zu anderen Netzen optimiert möglich sind (Route Summarization).

Falls das TGM aufgrund der organisatorischen Struktur der Institution einen dedizierten Adressbereich erhält, kann erwogen werden, diesen Adressbereich gemeinsam für GA und TGM zu strukturieren.

Der Adressbereich der GA sollte gemäß den Anforderungen der GA unterteilt und in Subnetze aufgeteilt werden. Die Subnetzgröße sollte anhand der Kommunikationsanforderungen der TGA-Anlagen und GA-relevanten Komponenten festgelegt werden. Die Subnetzgröße sollte für die gesamte GA möglichst einheitlich geplant werden. Falls dies aufgrund der unterschiedlichen Kommunikationsanforderungen und Anlagen-Ausprägungen nicht sinnvoll möglich ist, sollte die Anzahl der verschiedenen Subnetzgrößen minimiert und jeweils in Adressbereichen zusammengefasst werden, um eine Route Summarization an den Routing-Übergängen zu ermöglichen.

Das IP-Adresskonzept für die GA sollte derart gestaltet werden, dass die IP-Adressen Grundinformationen zu Art und Standort der GA-Komponente wiederspiegeln. Beispielsweise sollten Gebäude und Komponenten- bzw. Anlagen-Typ anhand des Subnetzes bzw. der IP-Adresse erkennbar sein.

Innerhalb der IP-Subnetze sollte eine einheitliche Adressierung vorgesehen werden. Beispielsweise erhalten auch in GA-Netzen nach einer verbreiteten Konvention die Routing-Komponenten die ersten IP-Adressen im Subnetz und Switches und Gateways die darauf folgenden IP-Adressen.

Falls die GA-relevanten Komponenten die Adresskonfiguration via DHCP (Dynamic Host Configuration Protocol) erhalten, sollten die DHCP-Server der GA mit den entsprechenden Subnetz-Informationen konfiguriert werden und es sollte festgelegt werden, welche Subnetzbereiche für eine dynamische oder eine statische Adressvergabe genutzt werden.

Häufig nutzen GA-relevante Komponenten statische IP-Adressen. Um hier Adresskonflikte durch versehentlich manuell doppelt vergebene IP-Adressen zu vermeiden, sollte die Zuteilung der Adressbereiche sorgfältig geplant und überwacht werden. Auf allen Komponenten, die statische Adressen mit manueller Konfiguration nutzen, sollte die dynamische Vergabe über DHCP deaktiviert werden, um ein unbeabsichtigtes Überschreiben der Konfiguration durch ein DHCP-Paket mit dynamischer Adresse zu vermeiden.

Es sollte geprüft werden, ob die Zuteilung auch der statischen Adressen über DHCP möglich ist und effizient umgesetzt werden kann. Darüber hinaus sollte geprüft werden, ob die GA-relevanten Komponenten auch dynamische IP-Adressen mit langer Lease Time (Gültigkeit der Adresse) nutzen können.

Auch in der GA werden teilweise Bereiche mit identischer IP-Konfiguration eingesetzt, um eine einfache Replikation von GA-Bereichen zu realisieren. Um hier bei einer übergreifenden Kommunikation Konflikte der IP-Adressen zu vermeiden, müssen an den Übergängen zwischen den GA-Bereichen entsprechende Mechanismen diese Adressen umwandeln. Für IP-Adressen werden hier in der Regel NAT-Komponenten (Network Address Translation) genutzt. Die NAT-Komponenten sollten in einer Firewall-Komponente im Umfeld der Anlage positioniert werden. Alternativ kann die Kommunikation auch durch den Einsatz eines ALGs entkoppelt werden, so dass auch hier die interne Adresse nicht nach außen sichtbar wird.

Typischerweise wird auch in der GA die segmentübergreifende Kommunikation über IP in Version 4 oder Version 6 realisiert. GA-spezifische Protokolle wie BACnet werden in der Regel nur in Teilbereichen (Subnetzen) wie z. B. Sensornetzen genutzt und müssen dann nur innerhalb eines Subnetzes eindeutige Adressen nutzen. Diese Subnetze sollten dann einen eindeutigen Übergabepunkt zum IP-Netz nutzen (siehe Abbildung 10). Wird ein GA-spezifisches Protokoll für einen größeren Bereich genutzt, so sollte auch hierfür ein Adresskonzept erstellt und umgesetzt werden, für das ebenfalls die Regeln des IP-Adresskonzepts gelten.

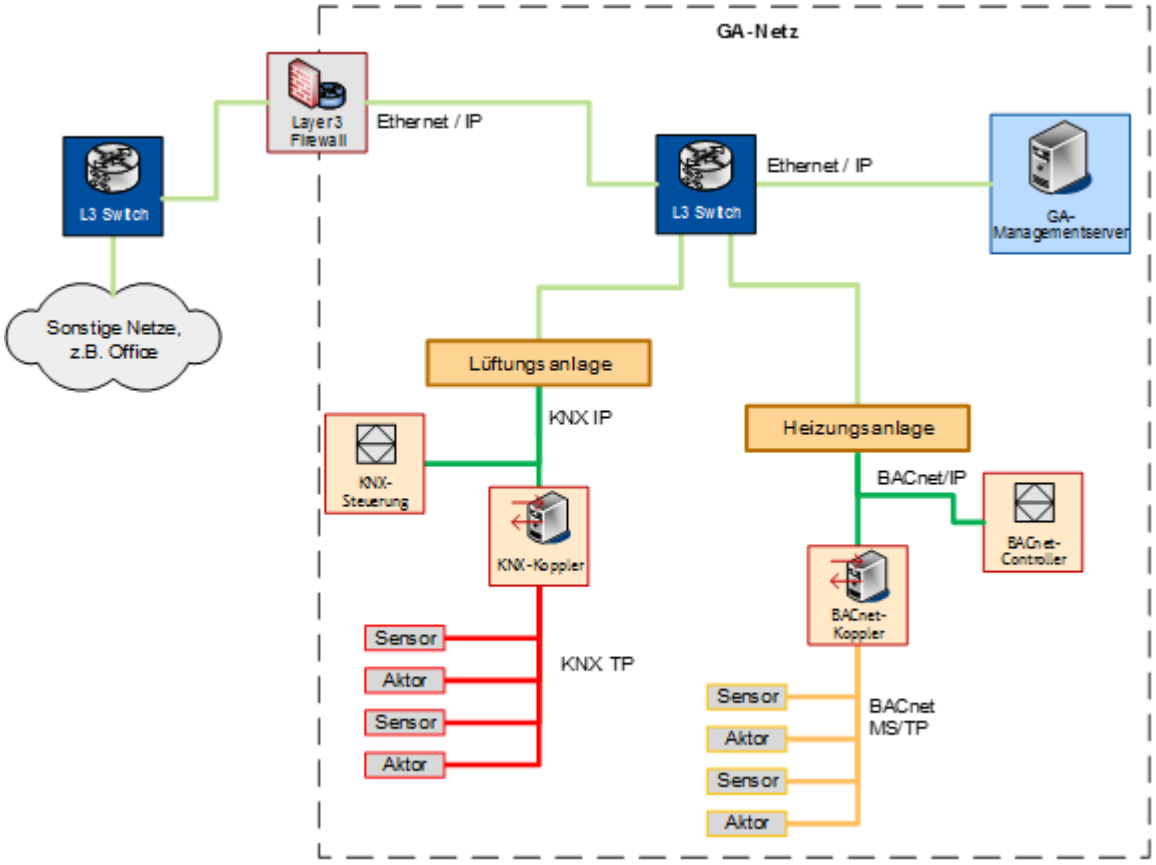

Abbildung 10: Beispiel für Netz mit verschiedenen Protokollen in der GA

INF.14.M20 Vermeidung von Broadcast-Kommunikation in GA-Netzen (S)

Meist werden Broadcast-Pakete nur innerhalb eines IP-Subnetzes übertragen. Jedoch erlaubt das Routing der IPv4-Technik die Übertragung von Layer 2 und Layer 3 Broadcasts in ausgewählte oder in alle Subnetze. Dies wird beispielsweise zur Übertragung von Werksvideos auf verschiedene Monitore genutzt. Aber auch Sensoren und Aktoren nutzen oft Broadcasts zur Übertragung von Informationen.

Die Routing-Komponenten in GA-Netzen sollten so konfiguriert werden, dass Broadcasts nicht weitergeleitet werden (Standardvorgabe gemäß RFC 2644). Ist eine Weiterleitung von Broadcasts zwingend erforderlich, sollte ausschließlich eine Weiterleitung an ausgewählte Subnetze (subnet-directed broadcast) konfiguriert werden.

Falls die Nutzung von Broadcasts auf Layer 2 oder Layer 3 durch GA-relevante Komponenten aus technischen Gründen zwingend ist, sollte die Netzsegmentierung entsprechend angepasst werden. Broadcast-Gruppen sollten weitestgehend zusammengefasst und von GA-Systemen, die potenziell durch eine Broadcast-Kommunikation gestört werden, getrennt werden.

IPv6 unterstützt keine Weiterleitung von Broadcast-Paketen in Routing-Komponenten, hier muss eine Broadcast-basierte Kommunikation auf Multicast- oder Unicast-Routing umgestellt werden.

INF.14.M21 Anzeigen der Gültigkeit von Informationen in GA-Systemen (S)

Angezeigte Informationen sollen dem Nutzer auf einen Blick den Zustand einer Komponente oder TGA-Anlage anzeigen. Hierzu werden kontinuierlich Informationen von Komponenten und TGA-Anlagensteuerungen im GA-Management erfasst. Jedoch können solche Informationen bei einer ausgefallenen Kommunikationsverbindung nicht mehr aktualisiert werden und verlieren ihre Gültigkeit. Das GA-Management sollte die Kontinuität der Informationen überwachen und nicht mehr aktuelle Informationen auf der Benutzeroberfläche entsprechend kennzeichnen. Alternativ sollte der Zeitstempel der Informationen im GA-Management angezeigt werden.

Bei TGA-Anlagen, die einen hohen Schutzbedarf haben, sollte eine geeignete Alarmierung umgesetzt werden, um beispielsweise die Kontrollfrequenz durch das Überwachungspersonal zu erhöhen. Um Fehlalarmierung bei kleinen Systemanomalien zu vermeiden, sollten die Alarmschwellen in Abhängigkeit vom System nicht zu eng eingestellt werden.

INF.14.M22 Sicherstellung von autark funktionierenden GA-Systemen und TGA-Anlagen (S)

Viele TGA-Anlagen müssen autark funktionieren, falls die Anbindung an das GA-Management unterbrochen ist. Beispielsweise darf eine Heizungsanlage nicht ausfallen, falls Meldungen von dezentralen Temperaturfühlern ausbleiben oder z. B. Management- und Bedieneinheiten (MBE) fehlerhafte Informationen übertragen. Ebenso müssen GA-Systeme autark funktionieren, falls die Verbindung zu anderen GA-Systemen oder Systemen wie z. B. TGM-Systeme unterbrochen ist.

Vorbereitend sollten alle Abhängigkeiten und Wechselwirkungen erfasst werden, insbesondere von

- TGA-Anlagen innerhalb eines GA-Systems,
- MBEs, Bedien- und Anzeigeeinrichtungen (BAEs) sowie Lokale Vorrangbedieneinheiten (LVBs), die als GA-relevante Komponenten nicht integraler Teil einer TGA-Anlage sind, sowie
- Automationseinrichtungen und Diensten eines GA-Systems.

Ebenfalls sollten auch alle Abhängigkeiten und Wechselwirkungen zwischen verschiedenen GA-Systemen sowie mit dem TGM und sonstigen Systemen außerhalb der GA erfasst werden. Für alle TGA-Anlagen und GA-Systeme sollte festgelegt werden, für welchen Zeitraum diese autark funktionieren müssen.

Hierfür sollten Maßnahmen für ein GA-System spezifiziert werden, die diese Abhängigkeiten minimieren. Hierbei sollte beachtet werden, dass Anlagenautomation und Raumautomation mit den MBEs bzw. BAEs abgestimmt zusammenwirken müssen, um eine vollständige Funktionalität der GA sicherzustellen.

Um eine vollständige Autarkie zu erreichen, sollten auch die Abhängigkeit vom GA-Netz insbesondere durch eine getrennte Verkabelung sowie dedizierte Netzkomponenten und -dienste in Erwägung gezogen werden.

Soll eine TGA-Anlage oder ein GA-System nur für einen bestimmten Zeitraum autark betriebsfähig sein, sollten übergreifend genutzte Netzdienste entsprechend eingerichtet werden. Beispielsweise kann die DHCP-Adressvergabe mit entsprechend langer Lease Time erfolgen oder eine entsprechende Dienste-Instanz im jeweiligen Subnetz eingerichtet werden, die auch ohne Verbindung zur übergeordneten Instanz für den geforderten Zeitraum überlebensfähig ist. Gegebenenfalls kann auch auf die Nutzung von Netzdiensten wie DHCP verzichtet werden.

Immer mehr GA-relevante Komponenten, insbesondere auch IoT-Komponenten, die in einer TGA-Anlage bzw. einem GA-System genutzt werden, benötigen einen kontinuierlichen Zugang zum Internet, um beispielsweise Systeme in der Cloud des Herstellers zu kontaktieren. Sind solche Komponenten für eine TGA-Anlage oder ein GA-System essentiell und für den geforderten Zeitraum auch durch entsprechende Konfiguration ohne Internet-Zugang nicht überlebensfähig, sollte ein Produktwechsel bei derartigen Komponenten erwogen werden. Alternativ kann ein dedizierter Internet-Zugang für die GA oder nur für einzelne Bereiche der GA erwogen werden, der dann jedoch nach Stand der Technik abgesichert werden muss.

INF.14.M23 Einsatz von physisch robusten Komponenten für die GA (S)

Abhängig von der Art des Gebäudes werden GA-Komponenten auch in rauen bzw. schwierigen Umgebungsbedingungen eingesetzt, zum Teil im direkten Umfeld von OT-Systemen oder außerhalb von geschlossenen Räumen. Abhängig vom Einsatzgebiet sollten die Komponenten entsprechend ausgewählt werden. Hier sollten neben den Netzkomponenten auch Komponenten der Feld- und gegebenenfalls sogar der Automatisierungsebene berücksichtigt werden. Die Komponenten sollten ein physisch robustes Design aufweisen, für welches der jeweilige Hersteller nachweist, dass die Komponente entsprechend den Anforderungen beispielsweise

- eine elektromagnetische Verträglichkeit (EMV) aufweist,
- staubfest,
- rüttelfest,
- feuchtigkeits- oder nässeresistent,
- für einen erweiterten Temperaturbereich geeignet oder
- gemäß EU-Richtlinie ATEX 2014/34/EU für einen Einsatz in explosionsgefährdeten Bereichen geeignet ist.

Die physische Robustheit der Netzkomponenten sollte ein Hersteller durch entsprechende Zertifikate von unabhängigen Prüfstellen nachweisen.

Nicht für jeden Standort benötigt eine GA-Komponente einen umfassenden Schutz gegen alle potenziell widrigen Umgebungsbedingungen. Die Komponenten sollten gemäß den Anforderungen des individuellen Standorts geschützt werden und den individuellen Montageort berücksichtigen, z. B. in einem Doppelboden, an der Decke oder auf einer Hutschiene.

Falls eine Komponente nicht ausreichend gegen widrige Umgebungsbedingungen geschützt werden kann, sollten Kompensationsmaßnahmen, beispielsweise ein Kasten um einen Switch in Außenanlagen, in Erwägung gezogen werden.

INF.14.M24 Zeitsynchronisation für die GA (S)

Viele Prozesse der GA, aber auch Aktivitäten im Bereich des Netz- und Systemmanagements wie Monitoring und Protokollierung, beruhen auf einer genauen und abgestimmten Zeit, z. B. die Gültigkeit und Nachvollziehbarkeit verteilter Informationen zwischen Sensoren und TGA-Anlagen. Daher ist eine synchrone Uhrzeit auf allen TGA-Anlagen und GA-relevanten Komponenten wichtig.

Nur so kann die richtige Reihenfolge der Informationen und Aktionen sichergestellt und die zugehörigen Informationen können sinnvoll korreliert werden.

Es sollte aufgrund der Anforderungen der GA-Systeme abgewogen werden, wie die Zeitsynchronisation innerhalb eines GA-Systems erfolgt. Ebenfalls sollte abgestimmt werden, wie die Zeitsynchronisation übergreifend beispielsweise zwischen GA-Systemen oder GA-Systemen und TGM erfolgt (siehe auch INF.14.M30 *Bereitstellung eines GA-eigenen Zeitservers*).

Das Zeitsignal für die Komponenten der GA sollte aus einer vertrauenswürdigen Quelle stammen. Netzsegmente mit hohem Schutzbedarf etwa sollten ihre Zeit nicht aus einem Netzsegment mit niedrigerem Schutzbedarf beziehen, wenn das Signal möglicherweise manipuliert werden könnte oder die Verfügbarkeit der Anbindung ausfällt.

Alle GA-relevanten Komponenten sollten die Zeit in einem einheitlichen, standardisierten Format interpretieren (z. B. unter Berücksichtigung von Zeitzonen, Winter- und Sommerzeit).

Zur Zeitsynchronisation über alle Gebäude, TGA-Anlagen und GA-relevante Komponenten kann derzeit standardmäßig das Network Time Protocol (NTP) oder das Precision Time Protocol (PTP) verwendet werden. Es gibt aber auch neue Entwicklungen, die gegebenenfalls berücksichtigt werden können.

Falls die Kommunikation von GA-Managementsystemen mit TGA-Anlagen Echtzeit-Anforderungen unterliegt, sollte für die Zeitsynchronisation PTP oder ein vergleichbares Protokoll genutzt werden. Die Zeitsynchronisation sollte auch in GA-spezifische Netze weitergeführt werden, beispielsweise durch Nutzung der BACnet-Zeitsynchronisation, die über einen BACnet-Zeitmaster an eine NTP-Quelle angebunden ist (siehe Abbildung 11).

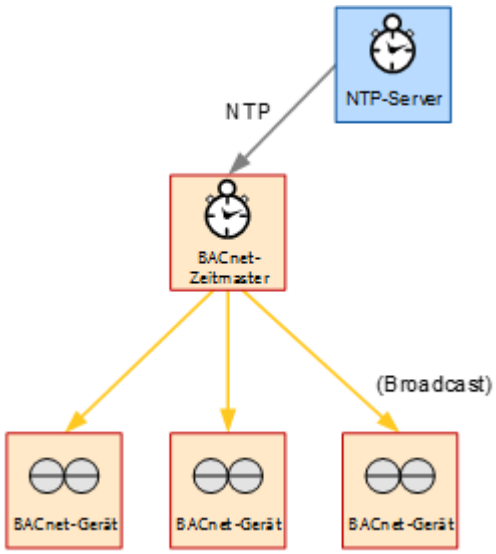

Abbildung 11: Einbindung BACnet in Zeitsynchronisation

Network Time Protocol (NTP)

Das NTP ist erstmals in RFC 958 definiert worden und liegt heute in der Version 4 vor (siehe RFC 5905 und Ergänzungen). Hierbei kann ein lokaler, jedoch zentraler NTP-Server der Institution genutzt werden. Abhängig vom Schutzbedarf von GA-Systemen sollte ein lokaler NTP-Server in der GA genutzt werden, der bei Ausfall der Anbindung an den zentralen NTP-Server der Institution weiterhin eine synchrone Zeit für die GA bereitstellt.

Die Nutzung von SNTP (Simple Network Time Protocol) sollte vermieden werden, da dieses vereinfachte Protokoll eine reduzierte Genauigkeit der Zeitsynchronisation realisiert.

Sicheres Network Time Protocol (NTPsec)

Als sichere Alternative zum NTP kann NTPsec genutzt werden, das kompatibel zum NTP ist. Hierbei sind zusätzliche Sicherheitsmechanismen integriert, um die Übertragung von NTP-Daten abzusichern.

Network Time Security (NTS)

NTS ist eine kompatible Erweiterung zum NTP, die in RFC 8915 standardisiert wird (Proposed Standard). Es bietet eine authentisierte Zeitsynchronisation, die einen auf TLS basierten und automatisierten Schlüsselaustausch nutzt. Dadurch wird eine manipulationssichere Übertragung der Zeitinformation gewährleistet.

Precision Time Protocol (PTP)

Das PTP ist definiert in IEEE 1588 bzw. IEC 61588 und erlaubt eine höhere Genauigkeit als NTP. Im Gegensatz zum NTP, bei dem die Genauigkeit in lokalen Netzen im Bereich von 200 Mikrosekunden liegt, kann mittels PTP eine Genauigkeit im Nanosekundenbereich erreicht werden. Jedoch unterstützen unter Umständen nicht alle GA-relevanten Komponenten das PTP. In dem Fall sollte geprüft werden, ob der Einsatz von PTP notwendig ist (z. B. für harte Echtzeitanforderungen in GA-Systemen) oder ob NTP für alle Komponenten als einheitliches Protokoll ausreichend ist.

INF.14.M25 Dediziertes Monitoring in der GA (S)

Um einen sicheren Betrieb der GA-relevanten Komponenten zu gewährleisten und einen möglichen Schaden durch Ausfall von Komponenten oder Diensten zu begrenzen, sollte eine geeignete Infrastruktur für das Monitoring in der GA konzipiert, implementiert und betrieben werden.

Diese Infrastruktur sollte mindestens innerhalb der GA ein Monitoring an zentraler Stelle ermöglichen. Abhängig von der individuellen Organisationsstruktur einer Institution sollte das Monitoring der GA-relevanten Komponenten auch in ein übergreifendes zentrales Monitoring der Institution eingebunden werden. Auch Mischformen sind hier denkbar. Beispielsweise können die Systeme des GA-Managements in das zentrale Monitoring der Institution eingebunden werden, während weitere wichtige GA-relevante Komponenten im GA-Monitoring überwacht werden. Mindestens sollten wichtige Informationen an das zentrale Monitoring der Institution weitergeleitet werden.

Ebenfalls sollte das Monitoring der GA mit dem Monitoring der TGA-Anlagen koordiniert bzw. gekoppelt werden, so dass wichtige Ereignisse und Statusänderungen der TGA-Anlagen auch im GA-Monitoring angezeigt werden.

Relevante Informationen aus dem Monitoring können ähnlich zu Protokollierungsdaten an das Security Monitoring, also an eine Lösung zum Security Information and Event Management (SIEM), weitergeleitet werden.

Für jeden Komponententyp sollten die zu überwachenden Parameter festgelegt werden, die dann ebenfalls kontinuierlich überwacht werden. Neben der Verfügbarkeit können hier weitere individuelle Parameter wichtig sein, beispielsweise die Auslastung der Systeme des GA-Managements.

Mindestens sollten die zentralen Komponenten der GA-Systeme sowie die Komponenten der Automatisierungsebene von wichtigen TGA-Anlagen überwacht werden. Darüber hinaus sollten alle betriebsrelevanten MSR-Komponenten, die nicht integraler Teil von TGA-Anlagen und im GA-System sichtbar sind, im Monitoring erfasst werden, um eine fehlerfreie Steuerung der TGA-Anlagen sicherzustellen.

Wichtige Netzkomponenten innerhalb von GA-Netzen sollten ebenfalls in das GA-Monitoring eingebunden werden. Dies gilt auch für Netzkomponenten, die GA-spezifische Netze wie z. B. BACnet realisieren. Die Netz- und Sicherheitskomponenten, die die Übergänge zwischen GA-Netzen und sonstigen Netzen realisieren bzw. kontrollieren, sollten ebenfalls im GA-Monitoring überwacht werden. Abhängig von der Organisation des Netzbetriebs können die Netzkomponenten auch ausschließlich oder ergänzend im übergeordneten Monitoring der Institution eingebunden und überwacht werden (siehe Bausteinschicht NET.3 *Netzkomponenten*).

Der Einsatz von nicht managebaren Komponenten, die dann auch nicht im Monitoring eingebunden werden können, sollte vermieden werden. Solche Komponenten erlauben entweder gar keine konfigurierenden Zugriffe, z. B. USB-Hubs, oder die Konfiguration kann maximal über einen lokalen Konsolenport erfolgen.

Im Rahmen des Monitorings sollten fremde bzw. neue Komponenten, z. B. unbekannte Bedienelemente, im Monitoring erkannt werden und es sollte eine entsprechende Information an das Betriebspersonal erfolgen. Darüber hinaus sollten regelmäßige Scans auf unbekannte Komponenten im GA-Netz durchgeführt werden.

Zur Beurteilung von kritischen Zuständen oder von Überlastungssituationen sollte darüber hinaus festgelegt werden, welche Komponenten mit welchen Parametern in eine Alarmierung eingebunden werden und welche Werte dieser Parameter zu einem Alarm führen. Um eine Abweichung vom Normalzustand feststellen zu können, muss dieser zunächst im Rahmen eines Baselining definiert werden. Hierfür werden die Parameter über einen längeren Zeitraum erfasst und daraus ein Normalwert bzw. ein Korridor für Normalwerte ermittelt. Die Alarme sollten regelmäßig bewertet werden, um festzustellen, ob eine Anpassung der Schwellwerte zur Alarmauslösung erforderlich ist.

Das Monitoring sollte neben der laufenden Verfügbarkeits- und Statusüberwachung von GA-relevanten Komponenten auch die Erfassung und Auswertung von sicherheitsrelevanten Ereignissen umfassen, die auch an ein zentrales Security Monitoring der Institution übermittelt werden sollten.

Über die Ereignisse oder Grenzüberschreitungen der überwachten Werte sollte das zuständige Betriebspersonal automatisch informiert bzw. alarmiert werden. Dies kann beispielsweise über E-Mail, SMS oder über Pager erfolgen. Auch ein Alarm an eine übergeordnete Managementstation, zu übergreifenden Werkzeugen im IT-Betrieb oder an einen Leitstand oder Helpdesk ist möglich. Die Meldewege und die maximal tolerierbare Verzögerung der Information sollten im Monitoring-Konzept festgelegt werden. Hierbei sollte sichergestellt sein, dass kritische Alarme dem Betriebspersonal unmittelbar angezeigt werden.

Mögliche Beispiele für solche Ereignisse und Muster innerhalb der GA sind:

- Kritische Zustände der Stromversorgung oder der Klimatisierung
- Ausfall von Systemen, z. B. von betriebsrelevanten Aktoren
- Spannungsschwankungen innerhalb der Stromversorgung
- Überschreiten von vordefinierten Werten für CPU-Last, Speicherverbrauch, Plattenplatz in GA-Managementsystemen
- Hardware-Fehler innerhalb der GA-relevanten Komponenten
- Verlust der Netzverbindung oder Überschreiten der vordefinierten Werte für Netzlast oder Broadcast-Last

Grundsätzlich sollten Status- und Ereignismeldungen nur über sichere Kommunikationswege übertragen werden. Dies können als sicher eingestufte Verbindungen innerhalb des GA-Netzes sein. Müssen im Kommunikationsweg Verbindungen genutzt werden, die als nicht ausreichend vertrauenswürdig eingestuft werden, z. B. WAN-Verbindung zwischen Gebäuden, muss der Kommunikationsweg über eine Verschlüsselung nach Stand der Technik abgesichert werden.

INF.14.M26 Protokollierung in der GA (S)

Die Protokollierung von Ereignissen (englisch Logging) dient dazu, Vorfälle und insbesondere Sicherheitsvorfälle festzustellen und zu analysieren (siehe auch OPS.1.1.5 *Protokollierung*). Daher sollten alle Ereignisse protokolliert werden, die dazu beitragen, dieses Ziel zu erreichen. Beispielsweise deuten unerlaubte Zugriffe bzw. Zugriffsversuche auf einen möglichen Angriffsversuch hin. Verfügbarkeitsschwankungen oder eine eingeschränkte Erreichbarkeit von GA-relevanten Komponenten können ein Indiz für Komponentenfehler, aber auch für eine Überlastung der Komponente durch einen Angriff sein. Die Protokollierung und Auswertung von Fehlern in automatischen und automatisierten Prozessen ist wichtig, um frühzeitig zu erkennen, dass ein Fehler aufgetreten ist, die Ursache dafür zu suchen und den Fehler dann beheben zu können.

Darüber hinaus können weitere Ereignisse protokolliert werden. Hier könnten z. B. auch Ereignisse interessant sein, die auf allgemeine Probleme mit Power over Ethernet (PoE) hindeuten. Gerade für PoE gibt es in der GA viele Nutzungsformen, z. B. Industrial Ethernet Switches, Sensoren oder

Sicherheitskameras. Auch können beispielsweise Kommunikationsprobleme bei Nutzung von Powerline (Powerline Communication, PLC) auf allgemeine Störungen der Infrastruktur oder der Stromversorgung hinweisen.

Prinzipiell erfolgt die Protokollierung auf drei Ebenen: auf Ebene der GA-relevanten Komponenten, auf Ebene des GA-Managements und übergeordnet in einer zentralen Protokollierung oder einem SIEM. Auf unterster Ebene, der Ebene der GA-relevanten Komponenten, muss festgelegt werden, was protokolliert werden soll und welche Informationen an die höheren Ebenen weitergeleitet werden sollen. Auch auf Ebene des GA-Managements muss festgelegt werden, welche Informationen an eine zentrale Protokollierung oder ein SIEM weitergegeben werden sollen (siehe Abbildung 12).

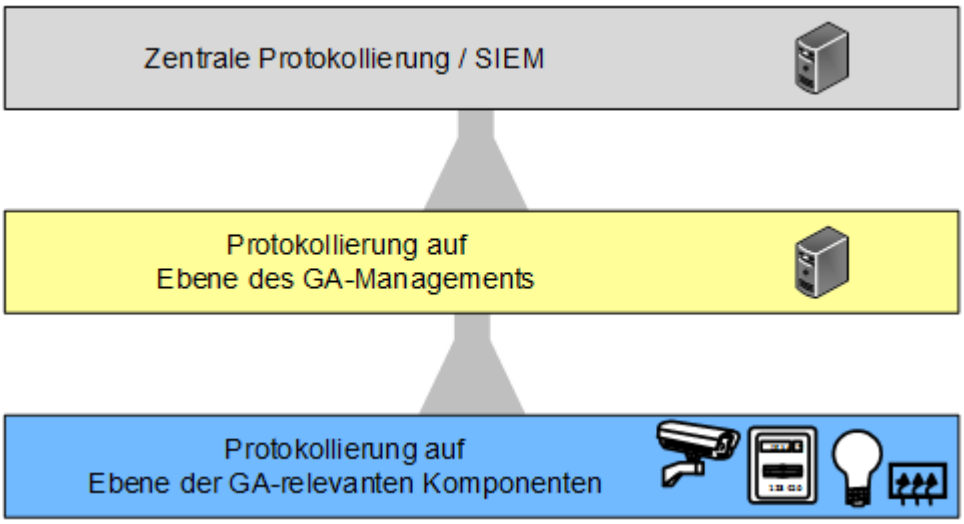

Abbildung 12: Protokollierungshierarchie

Die Protokollierung auf der Ebene der GA-relevanten Komponenten bedingt, dass Ereignismeldungen (englisch Logs) auf einer Vielzahl von Komponenten bzw. Systemen vorgehalten werden.

Die auflaufenden Meldungen sollten jedoch systematisch ausgewertet werden, damit nötigenfalls eine geeignete Reaktion ausgelöst werden kann. Bei einer überschaubaren Anzahl von GA-relevanten Komponenten kann diese Auswertung stichprobenartig und manuell erfolgen. Bei einer größeren Komponentenzahl und Ereignismeldungen sollte eine automatisierte oder zumindest teilautomatisierte Auswertung eingerichtet werden, um kritische Ereignisse zu erkennen.

Für alle Auswertungsformen sollten die Verantwortung und die Frequenz der Auswertung, z. B. wöchentlich, sowie die Ebene der Auswertung festgelegt werden. Beispielsweise können rein GA-relevante Meldungen, z. B. Steuerung der Temperatur wird von den TGA-Anlagen unzureichend umgesetzt, auf Ebene des GA-Management und Meldungen über unautorisierte Zugriffe oder Fehler bei Verschlüsselung und Entschlüsselung auf Ebene der zentralen Protokollierung analysiert werden.

Die Protokollserver auf Ebene des GA-Managements und die zentralen Protokollierungsserver sollten geeignet in das Segmentierungskonzept eingebettet werden. Abhängig von der GA-Sicherheitsrichtlinien sollten gegebenenfalls mehrere Protokollierungsserver vorgesehen werden.

Die automatisierte Auswertung von Protokollierungsdaten liefert eine Beurteilung von sicherheitskritischen Ereignissen, für die dann auch eine entsprechende Alarmierung eingerichtet werden sollte. Auch hier sollten die alarmerzeugenden Ereignisse, die Meldewege und die maximal tolerierbare Verzögerung der Information festgelegt sowie regelmäßig und ergänzend bei Bedarf angepasst werden.

INF.14.M27 Berücksichtigung von Wechselwirkungen zwischen Komponenten der GA in der Notfallplanung (S)

Notfallplanung

Die Notfallplanungen für die GA sollten mit der übergreifenden Störungs- und Notfallvorsorge, insbesondere der TGA-Anlagen und des TGM, abgestimmt werden. Eine Notfallplanung inklusive Wiederanlaufplan bezieht sich abweichend zu [BSI 200-4] in der GA immer auf den Betrieb des Gebäudes. Die Nutzbarkeit der GA innerhalb eines Gebäudes sollte durch einen Notbetrieb auf Basis eines Wiederanlaufplans und der Normalbetrieb auf Basis des Wiederherstellungsplans sichergestellt werden. Betriebsredundanzen wie Nutzung eines Ausweichstandorts sind i.d.R. im Rahmen der GA nicht möglich. Beispielsweise sind bei Ausfall einer Zutrittsanlage Ausweicharbeitsplätze nicht in jedem Fall verfügbar, jedoch könnten Sofortmaßnahmen wie Benachrichtigungen ergriffen werden.

Für die Spezifikation von Notfallplänen inklusive dem Wiederanlaufplan sollten die folgenden Punkte ergänzend zu den Festlegungen in [BSI 200-4] berücksichtigt werden, die z. B. im Rahmen einer Business Impact Analyse (BIA) festgelegt werden:

- Tolerierbare Dauer eines Komplettausfalls
    - der zentralen Komponenten von GA-Systemen
    - der Schnittstellen zu den TGA-Anlagen
    - der MSR-Komponenten innerhalb der GA
    - der Bedienelemente
    - der Zugangsmöglichkeiten auf die GA-Managementsysteme
    - der Internetanbindung inklusive Fernwartungsmöglichkeiten
- Zulässige Notbetriebsformen für alle GA-Systeme inklusive aller Komponenten (Sofortmaßnahmen und Wiederanlaufplanung)
    - Vorgaben, wann und wie Sicherheitsmaßnahmen bei einem Notfall außer Kraft gesetzt werden dürfen
    - Vorgaben, welche Funktionalitäten bei einem Notfall verzichtbar sind
    - Segmentierung bei Bearbeitung eines Notfalls, z. B. zur Isolierung von betroffenen Bereichen
    - Segmentierung von TGA-Anlagen eines GA-Systems zur Sicherstellung eines isolierten Notbetriebs von TGA-Anlagen
    - Notfallzugriffe auf GA-relevante Komponenten inkl. Netz- und Sicherheitskomponenten der GA
    - Zulässige Einschränkungen der Funktionalitäten während des Notbetriebs, z. B. nicht-redundanter Betrieb des GA-Managements oder Reduzierung von Messpunkten als Basis für die Steuerung innerhalb des GA-Systems
    - Dauer des Notbetriebs, z. B. wie lange darf eine redundant installierte Komponente nicht-redundant arbeiten
- Vorbereitungen für einen Wiederanlauf der GA eines Gebäudes
    - Verfügbarkeit von Austauschkomponenten, die für den Wiederanlauf gegebenenfalls einen geringeren Funktionsumfang haben und die auch von Betriebspersonal, das nicht über eine umfassende Systemkenntnis verfügt, getauscht und in Betrieb genommen werden können
    - Verfügbarkeit von Konfigurationssicherungen für alle GA-relevanten Komponenten, die nachweislich fehlerfrei sind, gegebenenfalls ältere Versionen, und die umgehend eingespielt werden können
    - Festlegung von Wiederanlauf-Reihenfolgen bzw. Wiederanbindung von TGA-Anlagen an GA-Systeme und typische Prüfpunkte nach Wiederanlauf

    - Festlegung der Reihenfolge von Wiederaufnahme der Kommunikation mit anderen GA-Systemen, dem TGM und sonstigen Kommunikationspartnern

Die Notfallplanungen sollten sich am allgemeinen Notfallvorsorgekonzept orientieren (siehe Baustein DER.4 *Notfallmanagement*) und es sollte sichergestellt sein, dass die Notfallplanungen und insbesondere die Handlungsanweisungen nachvollziehbar dokumentiert werden und allen betroffenen Personen in angemessener Form vorliegen, z. B. auch in Papierform.

Wechselwirkungen

Als Grundlage für das Notfallmanagement sollten innerhalb eines GA-Systems alle Wechselwirkungen aller eingebundenen Komponenten analysiert werden. Hierfür sollten alle Kommunikationsbeziehungen und Schnittstellen sowie alle Informationen, die innerhalb der Komponenten eines GA-Systems ausgetauscht werden, sowie alle durch die Informationen ausgelösten Aktionen bzw. Steuerungen erfasst und priorisiert werden. Für die ausgelösten Aktionen sollten auch die Auswirkungen auf andere Komponenten oder das gesamte GA-System bzw. die Auswirkungen von ausbleibenden Informationen und Aktionen analysiert und bewertet werden.

Wechselwirkungen mit schweren Auswirkungen sollten auf ein unumgängliches Maß reduziert werden. Gegebenenfalls müssen hierfür die Planung und das GA-Konzept angepasst werden (siehe INF.14.M1 *Planung der Gebäudeautomation* und INF.14.M9 *Entwicklung eines GA-Konzepts*), z. B. durch Vorsehen von redundanten Sensoren.

Ebenfalls sollten obige Parameter auch für die Kommunikation zwischen GA-Systemen und mit sonstigen Systemen, z. B. TGM, analysiert und minimiert werden.

Im Rahmen der Notfallplanung sollte mit dem jeweiligen TGA-Anlagenbetrieb festgelegt werden, ob Wechselwirkungen der internen Informations- und Aktionsketten der TGA-Anlage mit der Anbindung an das GA-System bestehen.

Wiederanlauf im Notbetrieb

Ergänzend zu den Festlegungen in [BSI 200-4] sollten ein Wiederanlaufplan für alle Komponenten innerhalb eines GA-Systems sowie gekoppelter GA-Systeme erstellt werden, der die Wechselwirkungen angemessen berücksichtigt (siehe auch INF.14.M2 *Festlegung eines Inbetriebnahme- und Schnittstellenmanagements für die GA*). Hierbei sollten neben den organisatorischen Schritten auch die Reihenfolge und die Priorisierung zum Wiederanlauf und zur Wiedereinbindung von Komponenten und TGA-Anlagen in das GA-System festgelegt werden. Beispielsweise sollten auch solche Komponenten oder auch TGA-Anlagen festgelegt werden, die für einen Notbetrieb entbehrlich sind.

Der Wiederanlaufplan sollte für typische Ausfallszenarien spezielle Handlungsanweisungen beinhalten, die ausreichend detailliert spezifiziert und regelmäßig erprobt werden. Die Anweisungen sollten der jeweiligen Aufgabe und dem jeweiligen Betriebspersonal angepasst sein, z. B. reiner Austausch von vorkonfigurierten MSR-Komponenten durch die Haustechnik während einer Nachtschicht.

Der Wiederanlaufplan sollte in regelmäßigen Abständen und gegebenenfalls als Ergebnis der Erprobung angepasst werden. Er sollte mindestens folgende Informationen beinhalten:

- die Schnittstellendefinition für alle Komponenten eines GA-Systems
- die Schnittstellendefinition zu anderen GA-Systemen oder sonstigen Systemen
- alle relevanten und verantwortlichen Ansprechpartner mit
    - Kontaktmöglichkeiten und -adressen
    - gegebenenfalls gestufte Berechtigungen in Notfallsituationen
- den Standort der jeweiligen Komponenten bzw. TGA-Anlage
- die Wiederanlaufreihenfolge und -priorisierung der eingebundenen Komponenten und TGA-Anlagen

- die Maßnahmen zur Sicherstellung des Notbetriebes, z. B.
    - isolierter Betrieb einer TGA-Anlage ohne Anbindung an ein GA-System oder
    - Steuerung der TGA ohne Sensoren auf Basis von Standard-Werten

Wiederherstellung des Normalbetriebs der GA im Gebäude

Auch die Wiederherstellung des Normalbetriebs der GA eines Gebäudes sollte detailliert vorbereitet und erprobt werden. Beispielsweise sollten die folgenden Punkte beachtet werden:

- Verfügbarkeit von Austauschkomponenten über eine eigene Vorratshaltung oder entsprechende Wartungsverträge
- Bereitstellung von Konfigurationssicherungen für alle GA-relevanten Komponenten
- Verfügbarkeit von fehlerfreien Software- und Firmware-Versionen, gegebenenfalls auch für ein Rollback auf eine ältere Version, auf einem eigenen Archivserver oder über einen Hersteller-Service

Analog zu INF.14.M2 *Festlegung eines Inbetriebnahme- und Schnittstellenmanagements für die GA* muss die Wieder-Inbetriebnahme der Komponenten und TGA-Anlagen eines GA-Systems aufeinander abgestimmt erfolgen. Grundsätzlich müssen die folgenden Punkte festgelegt werden:

- Reihenfolgen der Wieder-Inbetriebnahme von TGA-Anlagen
- Reihenfolge der Wiederherstellung der Anbindungen an ein GA-System (siehe 14.M3 *Sichere Anbindung von TGA-Anlagen und GA-Systemen*)
- Reihenfolge der Wiederherstellung der Anbindung von GA-Systemen an andere GA-Systeme und sonstige Systeme, z. B. TGM

Für die jeweiligen Inbetriebnahmen müssen typische Prüfpunkte festgelegt werden, die erfüllt sein müssen, bevor der nächste Schritt der Inbetriebnahme erfolgen darf.

INF.14.M28 Physische Trennung der GA (H)

Unterliegt die gesamte GA einem erhöhten Schutzbedarf, sollte das GA-Netz vom restlichen Netz physisch getrennt werden. Netzkomponenten und -leitungen sollten dediziert für die GA zur Verfügung gestellt werden. Ebenfalls sollten GA-Anwendungen wie GA-Management nicht gemeinsam mit Anwendungen, die nicht zur GA gehören, auf einem Virtualisierungs-Host realisiert werden.

Haben in der GA einzelne Bereiche einen erhöhten Schutzbedarf, so können auch GA-Bereiche, die TGA-Anlagen oder Nachfrageorganisationen umfassen, physisch vom restlichen GA-Netz getrennt werden.

Darüber hinaus sollte die GA abhängig vom Schutzbedarf als isoliertes Netz inklusive aller Netzdienste aufgebaut werden. In dem Fall sollte jegliche Kommunikation mit Netzen, die einen geringeren Schutzbedarf haben, auf das notwendige Minimum reduziert werden. Insbesondere sollte keine dauerhafte Verbindung zum Internet eingerichtet werden, auch nicht über Wartungs- und Meldeschnittstellen, die gegebenenfalls via Mobilfunk das Internet ankoppeln. Auch die Verbindung zum Büro- und OT-Netz sollte auf das notwendige Minimum, z. B. zum TGM, eingeschränkt werden.

Wird für die GA ein dedizierter Internet-Zugang bereitgestellt, so muss dieser die entsprechenden Anforderungen des Bausteins NET.1.1 *Netzarchitektur und -design* umsetzen. Der Zugang zum GA-Netz über diesen Internet-Zugang sollte auf die jeweiligen GA-relevanten Komponenten und die jeweiligen Hersteller oder Cloud-Dienste eingeschränkt werden. Wird dieser Internet-Zugang auch durch Komponenten von TGA-Anlagen genutzt, müssen auch diese Kommunikationsbeziehungen in der Internet-Firewall restriktiv reglementiert werden.

Auch für ein isoliertes GA-Netz sollten Funktionen des Network Operation Center (NOC) und Security Operation Center (SOC) umgesetzt werden, um Netzfehler und Sicherheitsvorfälle schnell erkennen zu können. Abhängig von den Sicherheitsanforderungen kann für die GA die Einrichtung eines

dedizierten NOC und gegebenenfalls sogar dedizierten SOC in Betracht gezogen werden. Hier sollte der Sicherheitsgewinn durch eventuell schnellere Alarme gegen die deutlich erhöhten Kosten und Aufwände abgewogen werden.

Falls ein isoliertes GA-Netz mit eigenen NOC- und SOC-Funktionen realisiert wird, sollte für das allgemeine NOC und SOC der Institution berücksichtigt werden, dass das GA-Netz mit allen GA-relevanten Komponenten gegebenenfalls nur als Blackbox einzubinden ist.

INF.14.M29 Trennung einzelner TGA-Anlagen (H)

Ergänzend zur Separierung der GA und der Segmentierung innerhalb der GA sollten einzelne Anlagennetze mit erhöhtem Schutzbedarf separiert werden. Die Komponenten, die die Firewall-Funktionen zur Kontrolle und Reglementierung der Kommunikation bereitstellen, sollten dann unmittelbar vor der TGA-Anlage bzw. dem Anlagennetz positioniert werden (siehe Abbildung 13). In der Regel kommen hier transparente Layer-2-Firewalls, auch Anlagen-Firewalls genannt, zum Einsatz. Diese bieten oft auch eine NAT-Funktionalität, um TGA-Anlagen mit identischen Adressbereichen konfliktfrei im GA-Netz anzubinden (siehe INF.14.M18 *Sichere Anbindung von GA-externen Systemen*). Weitere Möglichkeiten zur Mikrosegmentierung sind im Baustein NET.1.1 *Netzarchitektur und –design* thematisiert.

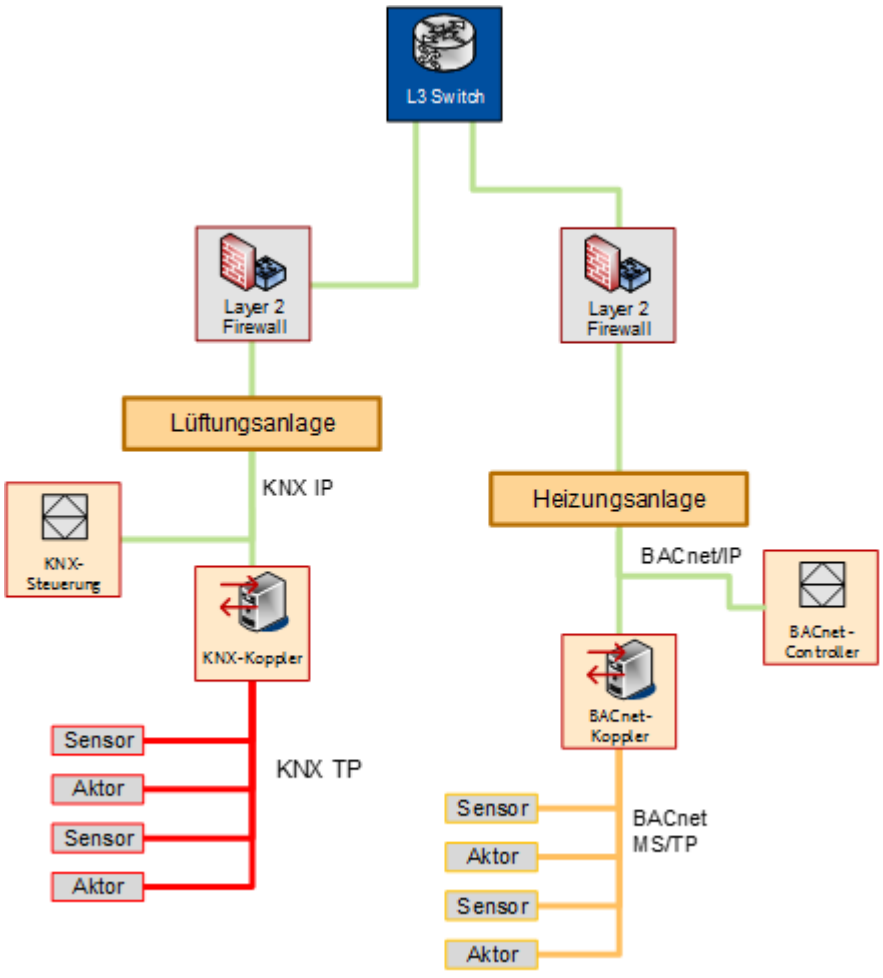

Abbildung 13: TGA-Anlagen mit vorgeschalteten L2-Firewalls

INF.14.M30 Bereitstellung eines GA-eigenen Zeitservers (H)

Bei erhöhtem Schutzbedarf sollten alle Abhängigkeiten der Zeitsynchronisation von Netzen, Diensten und Betriebseinheiten außerhalb der GA vermieden werden. Falls eine Unterbrechung zum zentralen Zeitserver der Institution für die GA insgesamt oder innerhalb von GA-Systemen nicht tolerierbar ist, sollte im GA-Netz ein dedizierter Zeitserver bereitgestellt werden, der eine direkte Kopplung an die höchste Uhreninstanz realisiert.

Abhängig von den Anforderungen an die Zeitsynchronisation sollten für einzelne GA-Systeme spezifische Zeitserver mit dedizierter Anbindung an die höchste Uhreninstanz bereitgestellt werden.

In Deutschland wird als höchste Uhreninstanz die von der Physikalisch-Technische Bundesanstalt (PTB) über den Funksender DCF-77 bereitgestellte Uhrzeit genutzt (siehe Abbildung 14). Diese Uhrzeit basiert auf mehreren, primären, synchronisierten Atomuhren. Das Funksignal realisiert am Sendeort eine Genauigkeit, die nur einen Fehler von 0,01 Milliardstel Sekunde am Tag aufweist.

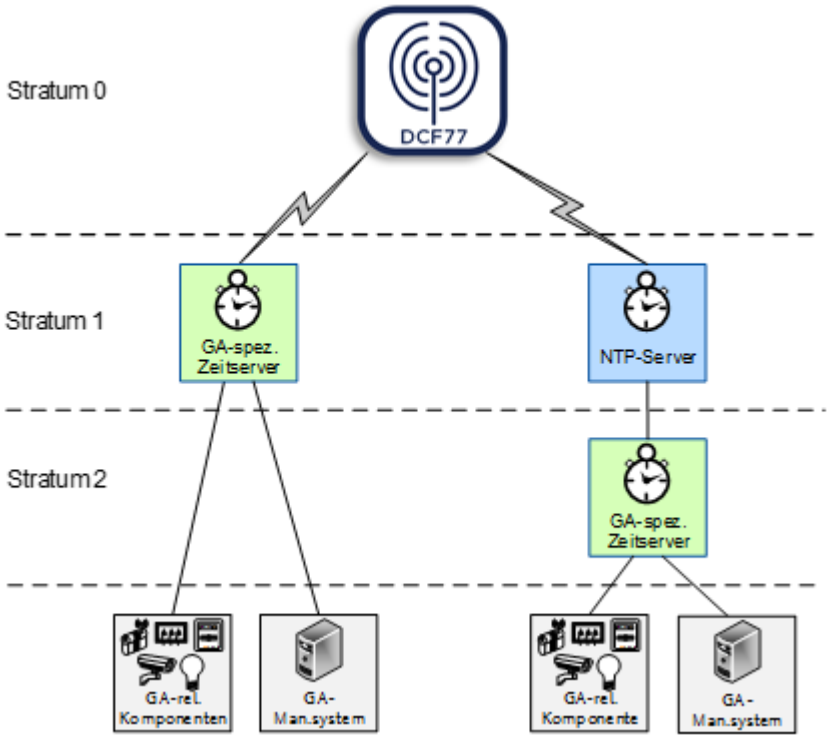

Abbildung 14: NTP-Uhrenhierarchie

3. Weiterführende Informationen

3.1. Genutzte GA-spezifische Fachbegriffe

Anlagenautomation (englisch System Automation and Control, SAC)

Die Anlagenautomation (AA) ist ein Teil eines GA-Systems und realisiert die Automation zum energieeffizienten, wirtschaftlichen und sicheren Betrieb von Anlagen der TGA. Die Anlagenautomation steuert über Aktoren die TGA-Anlage und dessen Zustandsgrößen. Diese werden wiederum durch die Sensoren der TGA-Anlage erfasst.

Bedien- und Beobachtungseinheiten (englisch Control and Display Device, CDD)

Gemäß DIN EN ISO 16484-2 umfasst der Begriff Bedien- und Beobachtungseinheiten (auch Leitstand oder Leitwarte genannt) die Summe der Einrichtungen für die Benutzer, die als Schnittstelle zu den Bedien- und Managementfunktionen eines GA-Systems fungiert.

GA-Bereich (englisch BACS Area)

Ein GA-Bereich umfasst einen oder mehrere Räume ähnlicher Nutzung, die horizontal, vertikal oder gemischt verteilt sein können und mehrere GA-Segmente umfasst.

Beispiele: ein Flur, eine Etage, ein Gebäudeflügel, eine Produktionshalle.

GA-Management (englisch Management Building Automation and Control Systems, M-BACS)

Das GA-Management (GA-M), auch als Gebäudeleittechnik bezeichnet, übernimmt als Bestandteil eines GA-Systems Aufgaben zur Informationsverarbeitung für das Management der GA, beispielhaft

Funktionen für ein übergeordnetes Energiemanagement, Wartungsmanagement, Störmanagement aber auch Raumbuchungsmanagement.

GA-Segment (englisch BACS Segment)

Ein GA-Segment bezeichnet die kleinste betrachtete räumliche Einheit, für die GA-Funktionen anwendbar sind. Ein GA-Segment ist nicht zu verwechseln mit einem Netzsegment, das über Sicherheitselemente vom restlichen Netz separiert wird.

GA-spezifische Netze (englisch BACS-specific Networks)

Ein GA-spezifisches Netz beschreibt ein Netz, das eine Verkabelung nutzt, die meist nicht auf Ethernet-Techniken basiert, z. B. KNX-Bussystem, oder das spezifische Protokolle nutzt, die nicht auf IP oder Ethernet gemäß IEEE 802.3 basiert, z. B. BACnet. Spezifische Protokolle können aufgrund von Anforderungen an eine Echtzeitkommunikation oder an einen reduzierten Protokollumfang erforderlich werden.

GA-System (englisch Building Automation and Control System, BACS)

Ein GA-System stellt gemäß VDI 3814-1 die technische Realisierung der GA dar und umfasst die folgenden Teile:

- GA-Management
- Anlagenautomation
- Raumautomation

Anlagenautomation und Raumautomation bestehen analog zur Operational Technology (OT) aus den (funktionalen) Ebenen Automationsebene (z. B. Anlagensteuerungen) und Feldebene (z. B. Aktoren und Sensoren).

Gebäudeautomation (englisch Building Automation and Control Systems, BACS)

Die Gebäudeautomation (GA) umfasst gemäß VDI 3814-1 alle Produkte und Dienstleistungen zum zielsetzungsgerichteten automatisierten Betrieb der Technischen Gebäudeausrüstung (TGA).

Gefahrenmeldeanlage (englisch Alarm System)

Gefahrenmeldeanlagen (GMA) sind TGA-Anlagen, die Gefahren wie Einbruch, Feuer und Rauch erkennen und melden können. Sie erfassen Gefahren durch Interaktion mit Sensoren oder Bedieneinheiten und erzeugen Gefahrenmeldungen, die an eine zentrale Komponente gesendet werden.

Gewerk

Im Bauwesen umfasst ein Gewerk im Allgemeinen die Arbeiten, die einem in sich geschlossenen Bauleistungsbereich zuzuordnen sind. Es handelt sich um einen Funktionsbereich, der insbesondere verschiedene TGA-Anlagen umfassen kann.

Beispiel: Raumlufttechnische Anlagen (Kostengruppe 430 in DIN 276), wozu etwa Lüftungsanlagen, Klimaanlagen und Kälteanlagen gehören.

Integration von Systemen oder Anlagen

Eine Integration von Systemen oder Anlagen bedeutet gemäß VDI 3814, dass integrierte Systeme oder Anlagen Informationen mit dem GA-Management austauschen und sich hierdurch gegenseitig beeinflussen können.

Eine Systemintegration im Rahmen der GA ist abzugrenzen von eingebetteten Systemen (englisch Embedded Systems). Diese sind intelligente Elemente, die in andere Systeme eingebettet sind und weitestgehend unsichtbar Überwachungs-, Steuerungs-, Verarbeitungs- oder Regelfunktionen innerhalb des einbindenden Systems übernehmen.

Kopplung von Systemen oder Anlagen

Eine Kopplung von Systemen und Anlagen bedeutet gemäß VDI 3814-2-2, dass die gekoppelten Systeme (Brandmeldeanlage oder Einbruchsmeldeanlage) ihre Informationen zur GA schicken, ohne dadurch ihre Autarkie einzuschränken oder zu verlieren. Eine System- oder Anlagenkopplung ist somit grundsätzlich rückwirkungsfrei.

Beispiele: Brandmeldeanlage oder Einbruchsmeldeanlage.

Leitstand (englisch Control Center)

Ein Leitstand (siehe auch Bedien- und Beobachtungseinheiten) ist ein technisches Werkzeug zur Visualisierung aktueller Abläufe, Zustände und Situationen von Prozessen, inklusive GA-Prozesse.

Liegenschaft (englisch Property)

Eine Liegenschaft umfasst gemäß VDI 3814-1 ein oder mehrere, meist lokal benachbarte Gebäude.

Lokale Vorrangbedienung (englisch Local Override, LOR)

Eine lokale Vorrangbedienung (LVB, früher auch Notbedieneinrichtung genannt) stellt gemäß VDI 3814-1 die Schnittstelle zu GA-relevanten Komponenten, die ein eingeschränktes Betreiben unabhängig von Automationseinrichtungen mit vorrangigem Anzeigen, Schalten und/oder Stellen ermöglicht. Ein Beispiel ist der manuelle vorrangige Betrieb von Ventilatoren.

Nachfrageorganisation

Eine Nachfrageorganisation ist gemäß DIN EN ISO 41011 eine Organisationseinheit innerhalb oder außerhalb der Institution, die für ihre Erfordernisse autorisiert ist, entsprechende Anforderungen an TGA, GA oder TGM zu stellen und die Kosten zur Erfüllung der Anforderungen zu übernehmen.

Beispiele: Mieter innerhalb eines Gebäudes, Eigentümer eines Gebäudes, Dienstleister innerhalb einer Institution, z. B. Kantine

Raumautomation (englisch Room Automation and Controls, RAC)

Die Raumautomation (RA) ist Bestandteil eines GA-Systems und realisiert alle Aufgaben einer anlagenübergreifenden Automation im betrachteten Raum, z. B. die Bedienung der im Raum installierten Technik.

Rückwirkungsfreiheit

Eine rückwirkungsfreie Anbindung einer TGA-Anlage an die GA bedeutet, dass die TGA-Anlage zwar Informationen an die GA liefert, von dieser jedoch auf Basis dieser Informationen nicht beeinflusst werden kann. Die Anlage bleibt weiterhin autark.

Technische Gebäudeausrüstung (englisch Building Services, BS)

Die Technische Gebäudeausrüstung (TGA) umfasst gemäß VDI 4700 Blatt 1 alle im Gebäude eingebauten und damit verbundenen technischen Einrichtungen und nutzungsspezifischen Einrichtungen sowie technische Einrichtungen in Außenanlagen und Ausstattungen. Gewisse Komponenten der GA sind ebenfalls zur TGA zuzurechnen, z. B. echtzeitfähige Industrial Ethernet Switches.

Technisches Gebäudemanagement (englisch Technical Building Management, TBM)

Das Technische Gebäudemanagement (TGM) beinhaltet gemäß DIN 32736 alle Leistungen, die zum Erhalt der technischen Funktion und Verfügbarkeit eines Gebäudes dienen. Das TGM übernimmt somit für die TGA das Betreiben, Instandhalten, Modernisieren und Dokumentieren der Komponenten und definiert alle notwendigen Prozesse.

TGA-Anlage

Eine Anlage der TGA beschreibt die Gesamtheit aller zur Erfüllung bestimmter Funktionen zusammenwirkenden technischen Komponenten. Beispiele gemäß DIN 276 „Kosten im Bauwesen“ sind Wärmeversorgungsanlagen, Lüftungsanlagen oder Beleuchtungsanlagen. Anlagen werden in der GA in ein GA-System integriert oder mit GA-Systemen gekoppelt.

3.2. Abkürzungen

Abkürzung	Bedeutung
5G	5. Generation des Mobilfunks
6LoWPAN	IPv6 over Low -Power Wireless Personal Area Networks
AA	Anlagenautomation
ACL	Access Control List
AES	Advanced Encryption Standard
AES-CCM	AES (with) Counter mode and CBC-MAC
AFH	(Bluetooth) Adaptive Frequency Hopping
ALG	Application Layer Gateway
ATEX	(französisch) ATmosphères EXplosibles
BACnet	Building Automation and Control Networks
BACnetSC	BACnet Secure Connect
BACS	Building Automation and Control Systems
BAE	Bedien- und Anzeigeeinrichtung
BIA	Business Impact Analyse
BIM	Building Information Modelling
BLE	Bluetooth Low Energy
BMA	Brandmeldeanlagen
BS	Building Services
BSI	Bundesamt für Sicherheit in der Informationstechnik
CPU	Central Processing Unit
dACL	dynamic ACL
DCF77	Deutschland, Langwellensender, Frankfurt am Main, Sendefrequenz 77,5 kHz
DDoS	Distributed DoS
DHCP	Dynamic Host Configuration Protocol
DIN	Deutsches Institut für Normung
DMZ	De-Militarized Zone
DoS	Denial of Service
EAP	Extensible Authentication Protocol
EAPoL	EAP over LAN
EMA	Einbruchmeldeanlagen
EMV	Elektromagnetische Verträglichkeit
EN	Europäische Norm
ENISA	European Network and Information Security Agency
EU	Europäische Union
FTP	File Transfer Protocol
FTPS	File Transfer Protocol Secure
GA	Gebäudeautomation
GA-M	GA-Management
GHz	Gigahertz
GMA	Gefahrenmeldeanlagen
HTTPS	HyperText Transfer Protocol Secure
IDS	Intrusion Detection System
IDPS	Intrusion Detection and Prevention System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System

Abkürzung	Bedeutung
IPsec	IP security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISO	Internationale Organisation für Normung
IT	Informationstechnologie
KNX	Konnex(-Bus)
KNX-RF	KNX - Radio Frequency
LAN	Local Area Network
LoRaWAN	Long Range Wide Area Network
LPWAN	Low Power Wide Area Network
LTE	Long Term Evolution
LVB	Lokale Vorrangbedieneinheit
MAC	Media Access Control
MBE	Management- und Bedieneinheit
MHz	Megahertz
MPLS	Multiprotocol Label Switching
MSR	Messen, Steuern, Regeln
NAC	Network Access Control
NAT	Network Address Translation
NGFW	Next Generation Firewall
NOC	Network Operation Center
NTP	Network Time Protocol
NTPsec	Network Time Protocol security
NTS	Network Time Security
OSI	Open Systems Interconnection
OT	Operational Technology
PC	Personal Computer
PLC	Powerline Communication
PoE	Power over Ethernet
PTB	Physikalisch-Technische Bundesanstalt
PTP	Precision Time Protocol
RA	Raumautomation
RADIUS	Remote Authentication Dial In User Service
RFC	Request For Comment (IETF)
SIEM	Security Incident and Event Management
SIG	(Bluetooth) Special Interest Group
SIM	Subscriber Identity Module
SLA	Service Level Agreement
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SOC	Security Operation Center
SRD	Short Range Device
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Program
TGA	Technische Gebäude-Ausstattung
TGM	Technisches Gebäude-Management
TLS	Transport Layer Security
TP	Twisted Pair
ÜMA	Überfallmeldeanlagen
USB	Universal Serial Bus
VdF	Vertrauen durch Sicherheit (VdS Schadenverhütung GmbH)

Abkürzung	Bedeutung
VdS	Verband der Sachversicherer (Herausgeber des VdS-Prüfsiegels)
VDI	Verein Deutscher Ingenieure
VDMA	Verband Deutscher Maschinen- und Anlagenbau
VLAN	Virtual LAN
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network

3.3. Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind.

Informationen zu Bluetooth Low Energy (BLE)

- Bluetooth SIG, Inc., „Bluetooth Core Specification“, Version 5.3, Juli 2021, verfügbar unter https://www.bluetooth.com/specifications/specs/core-specification/

IP500

- IP500 Alliance, siehe https://ip500.org/

Zigbee

- Zigbee Alliance, Zigbee Specification, August 2015, verfügbar unter
- https://zigbeealliance.org/wp-content/uploads/2019/11/docs-05-3474-21-0csg-zigbee-specification.pdf
- IEEE 802.15.4, IEEE Standard for Low-Rate Wireless Networks, Juli 2020, verfügbar unter https://standards.ieee.org/standard/802_15_4-2020.html

Long Range Wide Area Network (LoRaWAN)

- Informationen zu LoRaWAN verfügbar unter https://lora-alliance.org/about-lorawan/

EnOcean

- Informationen zu EnOcean verfügbar unter https://www.enocean-alliance.org/de/spezifikationen/

KNX-RF

- Informationen zu KNX und KNX-RF verfügbar unter https://www.knx.org/knx-en/for-manufacturers/development/radio-frequency/

DCF-77

- Informationen zu Zeitdiensten der Physikalisch-Technische Bundesanstalt (PTB) sind unter https://www.ptb.de/cms/ptb/fachabteilungen/abt4/fb-44/fragenzurzeit/fragenzurzeit12.html verfügbar.

Elektromagnetische Verträglichkeit

- DIN EN IEC 61000-6 „Elektromagnetische Verträglichkeit (EMV)“, November 2019,
- DIN EN 50310 „Telekommunikationstechnische Potentialausgleichsanlagen für Gebäude und andere Strukturen“, Juli 2020 sowie
- DIN EN 50174-2 „Informationstechnik – Installation von Kommunikationsverkabelung“, Oktober 2018,

- alle verfügbar im Beuth-Verlag

Enisa, EU Toolbox for 5G Security, Januar 2020, verfügbar unter https://www.enisa.europa.eu/news/enisa-news/5g

Weitere sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne unter grundschutz@bsi.bund.de entgegen.

3.4. Quellenverweise

[BSI 200-4] Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 200-4 - Business Continuity Management, Januar 2021, Community Draft

[IEC61588] IEC 61588 – Precision clock synchronization protocol for networked measurement and control systems, Februar 2009

[IEEE1588] IEEE 1588 – IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems, November 2019, verfügbar unter https://standards.ieee.org/standard/1588-2019.html

[RFC5905] IETF, RFC 5905 – Network Time Protocol Version 4: Protocol and Algorithms Specification, Proposed Standard, Juni 2010, verfügbar unter https://tools.ietf.org/html/rfc5905

[RFC8915] IETF, RFC 8915 – Network Time Security for the Network Time Protocol, Proposed Standard, September 2020, verfügbar unter https://tools.ietf.org/html/rfc8915

[VDI3814-1] VDI 3814 Blatt 1 – Gebäudeautomation (GA) – Grundlagen, Verein Deutscher Ingenieure e.V., Januar 2019, verfügbar im Beuth-Verlag

[VDI3814-2] VDI 3814 Blatt 2.x – Gebäudeautomation (GA) – Planung, Verein Deutscher Ingenieure e.V., Januar 2019, verfügbar im Beuth-Verlag

- VDI 3814 Blatt 2.1 –Bedarfsplanung
- VDI 3814 Blatt 2.2 –Planungsinhalte, Systemintegration und Schnittstellen
- VDI 3814 Blatt 2.3 –Bedienkonzept und Benutzeroberflächen