



INF.13 Technisches Gebäudemanagement

1. Beschreibung

1.1. Einleitung

Das Gebäudemanagement (GM), auch Facility Management genannt, ist für alle Leistungen zuständig, die in der Planungs- und Nutzungsphase von Gebäuden, Gebäudekomplexen, Liegenschaften oder Liegenschaftsportfolios anfallen. Im Folgenden wird hierfür einheitlich der Begriff Gebäude genutzt. Ausnahmen hiervon werden explizit genannt.

Das GM ist standort- sowie objektbezogen ausgerichtet. Es lässt sich in technisches, infrastrukturelles und kaufmännisches GM untergliedern.

Das technische Gebäudemanagement (TGM) umfasst gemäß DIN 32736 alle Leistungen, die die technische Funktion und Verfügbarkeit eines Gebäudes erhalten. Zu diesen Leistungen gehören unter anderem:

- Betreiben
- Dokumentieren
- Energie- und Umweltmanagement
- Informationsmanagement
- Modernisieren
- Sanieren
- Umbauen
- Verfolgen der technischen Gewährleistung

Wesentliche technische Funktionen eines Gebäudes werden durch die technische Gebäudeausrüstung (TGA) bereitgestellt, die durch das TGM betrieben, gepflegt und weiterentwickelt wird. Die TGA umfasst dabei gemäß VDI 4700 Blatt 1 alle im Bauwerk eingebauten und damit verbundenen technischen und nutzungsspezifischen Einrichtungen sowie technische Einrichtungen in Außenanlagen und Ausstattungen (siehe auch Kapitel 4.1 *Genutzte TGM-spezifische Fachbegriffe*). Falls die TGA automatisiert und gewerkübergreifend betrieben werden soll, wird zusätzliche technische Infrastruktur zur Gebäudeautomation (GA, engl. Building Automation and Control Systems, BACS) eingesetzt. Somit ist die GA ein zentrales Werkzeug des TGM. Ein Gebäude kann durch TGM auch ohne

GA betrieben werden, GA hingegen ist immer durch TGM flankiert. Gewisse Komponenten der GA sind dabei auch der TGA zuzurechnen, wie z. B. echtzeitfähige Industrial Ethernet Switches.

Während die TGA in der Vergangenheit meist unabhängig von der IT und der Prozessleit- und Automatisierungstechnik (Operational Technology, OT) betrieben wurde, werden heute zunehmend Netzübergänge zu diesen Bereichen etabliert. Hinzu kommt, dass Teile der TGA rund um die Uhr genutzt werden. Daher müssen Änderungen oft parallel zur produktiven Nutzung durchgeführt werden.

Auch im TGM müssen die Grundwerte der Informationssicherheit berücksichtigt werden, denn der Verlust von Verfügbarkeit, Vertraulichkeit und Integrität von Systemen kann im TGM weitreichende Auswirkungen bis hin zur Gefährdung von Leib und Leben nach sich ziehen.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, die Informationssicherheit als integralen Bestandteil bei Planung, Umsetzung und Betrieb im Rahmen des TGM zu etablieren.

1.3. Abgrenzung und Modellierung

Der Baustein INF.13 *Technisches Gebäudemanagement* ist auf das TGM einer Institution anzuwenden, sobald Gebäude mit TGA geplant, gebaut oder betrieben werden.

Dieser Baustein behandelt das TGM, somit die Aufgaben und Prozesse, die für die Planung und den Betrieb der TGA-Anlagen (siehe Kapitel 4.1 Genutzte TGM-spezifische Fachbegriffe) eines Gebäudes erforderlich sind. Die technische Infrastruktur für den automatisierten Betrieb von Gebäuden wird im Baustein INF.14 *Gebäudeautomation* behandelt. Letzterer muss zusätzlich zum Baustein INF.13 *Technisches Gebäudemanagement* angewendet werden, wenn die zu betreibende TGA automatisiert und anlagenübergreifend gesteuert wird. In diesem Sinne umfasst das TGM auch die Prozesse der GA.

Weiterhin ist es möglich, dass zu den zu verwaltenden Systemen auch solche gehören, die durch Bausteine aus den Schichten IND *Industrielle IT* und SYS *IT-Systeme* modelliert werden, z. B. IND.2.1 *Allgemeine ICS-Komponente* oder auch SYS.4.4 *Allgemeines IoT-Gerät*. Darüber hinaus müssen die für das TGM relevanten Aspekte der Schichten ORP und OPS beachtet werden, insbesondere die Teilschichten OPS.1 *Eigener Betrieb* und OPS.2 *Betrieb von Dritten* sowie die Bausteine ORP.2 *Personal* und ORP.4 *Identitäts- und Berechtigungsmanagement*. Werden für das TGM Cloud-Dienste eingesetzt, muss für die Auswahl dieser Dienste der Baustein OPS.2.2 *Cloud-Nutzung* berücksichtigt werden.

Zur Absicherung von Fernzugängen im TGM sind die Bausteine OPS.1.2.5 *Fernwartung* und IND.3.2 *Fernwartung im industriellen Umfeld* anzuwenden.

Der Baustein INF.13 *Technisches Gebäudemanagement* behandelt nicht die physische Sicherheit von Gebäuden, diese wird in dem Baustein INF.1 *Allgemeines Gebäude* behandelt. Ebenso spielt der Aspekt der Safety in diesem Baustein keine hervorgehobene Rolle, sondern wird im Baustein IND.2.7 *Safety Instrumented Systems* behandelt.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein INF.13 *Technisches Gebäudemanagement* von besonderer Bedeutung.

2.1. Fehlende Grundlagen für die Planung des TGM

Wenn beim Bau eines Gebäudes die Nachfrageorganisationen (siehe Kapitel 4.1 Genutzte TGM-spezifische Fachbegriffe) noch nicht feststehen, fehlen Ansprechpartner, Zielsetzung und Bedarfe für

das TGM. Das kann dazu führen, dass das TGM im Betrieb nicht dem tatsächlichen Bedarf entspricht, weil dieser zum Zeitpunkt der Planung und Umsetzung nicht abgefragt werden konnte.

2.2. Mangelnde Dokumentation beim TGM

In das TGM ist häufig eine Vielzahl von Dienstleistern involviert. Ist die Dokumentation der Zuständigkeiten mit Ansprechpartnern und zugehörigen SLAs unvollständig oder nicht zugänglich, führt dies im Ernstfall, wenn wichtige Systeme ausfallen, zu vermeidbaren Verzögerungen, die gegebenenfalls sogar Personenschaden zur Folge haben können.

Eine fehlende Dokumentation von Sicherheitszertifizierungen der TGA-Anlagen inklusive Terminen für notwendige Erneuerung kann dazu führen, dass abgelaufene Zertifizierungen nicht rechtzeitig erneuert werden. Dadurch kann gegen Gesetze verstoßen werden, je nach TGA-Anlage Gefahr für Leib und Leben entstehen und ein entstandener Schaden nicht über entsprechende Versicherungen abgewickelt werden.

2.3. Kompromittierung der Schnittstellen mit TGM

Das TGM hat technische Schnittstellen zu besonders schützenswerten Bereichen, z. B. Safety Instrumented Systems (SIS), Sicherheitsdienst und Brandmeldeanlagen. Wenn diese Schnittstellen bewusst oder unbewusst durch Fehler im TGM kompromittiert werden, dann kann dies einen Verstoß gegen Gesetze sowie Gefahr für Leib und Leben zur Folge haben.

Wird z. B. bei einem Feueralarm in einem Rechenzentrum die optische oder akustische Warnung außer Kraft gesetzt, können im Raum befindliche Personen diesen nicht rechtzeitig verlassen, bevor der Raum mit Löschgas geflutet wird. Ebenso kann ein vorgetäuschter Feueralarm dazu führen, dass Fluchttüren geöffnet werden und dadurch unberechtigter Zugang erlangt wird oder Türen geschlossen und gegebenenfalls Personen eingeschlossen werden.

2.4. Unzureichendes Monitoring der TGA

Wenn die TGA nur unzureichend durch ein entsprechendes Monitoring überwacht wird, dann werden sicherheitsrelevante Ereignisse, wie z. B. relevante Fehlfunktionen in der TGA, unter Umständen nicht oder zu spät erkannt. Dies kann je nach Ereignis zu weiteren Schäden führen oder Gefahr für Leib und Leben bedeuten.

Wird z. B. der Ausfall der Heizung bei Außentemperaturen im Minusbereich nicht gemeldet, kühlen die Räume erst stark aus, bevor der Ausfall bemerkt wird und eine Behebung eingeleitet werden kann.

2.5. Unzureichendes Rollen- und Berechtigungsmanagement

Wenn das TGM oder einzelne seiner Teile von der restlichen IT der Institution physisch getrennt werden, dann wird in der Regel auch ein dediziertes Benutzer- und Berechtigungsmanagement eingerichtet. Wenn dieses unzureichend konzipiert und umgesetzt wird, dann kann nicht ausgeschlossen werden, dass mehrere Mitarbeiter dasselbe Benutzerkonto nutzen oder Berechtigungen von ausgeschiedenen internen oder externen Mitarbeitern oder Dienstleistern nicht gelöscht wurden. Als Folge kann auf das TGM unberechtigt zugegriffen werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins INF.13 *Technisches Gebäudemanagement* aufgeführt. Der ISB ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der ISB stets einzubeziehen.

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

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

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

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

INF.13.A1 Beurteilung des Ist-Zustands bei der Übernahme bestehender Gebäude (B)

Bei der Übernahme von bestehenden Gebäuden MÜSSEN die im Gebäude installierten TGA-Anlagen, die Bausubstanz und Einrichtungen sowie vorhandene Dokumentation erfasst und hinsichtlich ihres Zustands (Alter, Supportstatus, Zukunftsfähigkeit, Vollständigkeit der Dokumentation etc.) beurteilt werden.

INF.13.A2 Regelung und Dokumentation von Verantwortlichkeiten und Zuständigkeiten im Gebäude [Institutionsleitung, Planer] (B)

Da es in einem Gebäude meist unterschiedliche Verantwortlichkeiten und Zuständigkeiten für verschiedene Bereiche gibt, MÜSSEN die entsprechenden Rechte, Pflichten, Aufgaben, Kompetenzen und zugehörigen Prozesse geregelt und dokumentiert werden.

Hierbei MÜSSEN auch die organisatorischen Strukturen im Gebäude berücksichtigt und dokumentiert werden. Insbesondere MÜSSEN alle Nachfrage- und Betreiberorganisationen erfasst werden. Erfolgt das TGM durch eine externe Betreiberorganisation, MÜSSEN die zugehörigen Rechte, Pflichten, Aufgaben und Kompetenzen gemäß Baustein OPS 2.1 *Outsourcing für Kunden* vertraglich festgehalten werden.

Weiterhin MÜSSEN die Schnittstellen und Meldewege inklusive Eskalation zwischen allen Beteiligten festgelegt und dokumentiert werden. Auch die Koordination verschiedener Betreiberorganisationen MUSS geregelt und dokumentiert werden.

Der Zugriff auf die Dokumentation MUSS geregelt werden. Die gesamte Dokumentation inklusive der zugehörigen Kontaktinformationen MUSS immer aktuell und verfügbar sein.

INF.13.A3 Dokumentation von Gebäudeeinrichtungen (B)

Alle Gebäudeeinrichtungen der TGA inklusive GA MÜSSEN dokumentiert werden. Hierbei MUSS alle gegebenenfalls schon vorhandene Dokumentation zusammengeführt, aus dem Blickwinkel des TGM organisiert und um TGM-spezifische Angaben ergänzt werden.

Der Zugriff auf die Dokumentation MUSS geregelt werden. Die gesamte Dokumentation inklusive der zugehörigen Kontaktinformationen MUSS immer aktuell und verfügbar sein.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

INF.13.A4 Erstellung einer Sicherheitsrichtlinie für TGM (S)

Ausgehend von der allgemeinen Sicherheitsleitlinie der Institution SOLLTE eine übergeordnete Sicherheitsrichtlinie für TGM erstellt sowie nachvollziehbar umgesetzt werden. Aus dieser übergeordneten Sicherheitsrichtlinie SOLLTEN spezifische Sicherheitsrichtlinien für die verschiedenen Themenbereiche des TGM abgeleitet werden. In der Sicherheitsrichtlinie für das TGM SOLLTEN nachvollziehbar Anforderungen und Vorgaben beschrieben werden, wie das TGM umgesetzt wird. Die Sicherheitsrichtlinie SOLLTE regelmäßig und zusätzlich bei Bedarf geprüft und gegebenenfalls aktualisiert werden, um dem aktuellen Stand der Technik zu entsprechen und auch neueste Erkenntnisse abdecken zu können. Sie SOLLTE allen im Bereich TGM zuständigen Mitarbeitern bekannt und grundlegend für ihre Arbeit sein.

INF.13.A5 Planung des TGM (S) [Planer]

Das TGM, die zugrundeliegende Infrastruktur und die zugehörigen Prozesse SOLLTEN geeignet geplant werden. Die Planung SOLLTE dabei mindestens eine detaillierte Anforderungsanalyse, eine ausreichende Grobkonzeptionierung und eine Fein- und Umsetzungsplanung umfassen.

Im Rahmen der Anforderungsanalyse SOLLTEN Anforderungen an TGM-Infrastruktur und TGM-Prozesse spezifiziert werden. Dabei SOLLTEN alle wesentlichen Elemente für das TGM berücksichtigt werden. Auch SOLLTE die Sicherheitsrichtlinie für das TGM beachtet werden. Steht die Nachfrageorganisation zum Zeitpunkt der Planung noch nicht fest, SOLLTEN im Rahmen einer universellen Planung zumindest grundlegende Anforderungen erfasst werden, die dem Stand der Technik entsprechen.

Für die Anforderungsspezifikation SOLLTEN auch die Schnittstellen der zu verwaltenden Systeme dokumentiert werden, z. B. um die Kompatibilität von TGM-Lösung und zu verwaltenden Systemen zu gewährleisten.

Außerdem SOLLTEN vor der Beauftragung von Dienstleistern oder der Anschaffung von Hard- oder Software der durch das TGM zu verwaltenden Systeme die Anforderungen des TGM in einem Lastenheft des TGM spezifiziert werden. In diesem Lastenheft SOLLTE auch die Durchführung von Tests berücksichtigt werden (siehe auch INF.13.A22 *Durchführung von Systemtests im TGM*).

Wenn im TGM Funktionen der Künstlichen Intelligenz (KI) eingesetzt werden, SOLLTE bei dem zuständigen Hersteller angefragt werden, ob und wie die Informationssicherheit hier angemessen berücksichtigt wird.

Die Grobkonzeptionierung SOLLTE gemäß INF.13.A6 *Erstellung eines TGM-Konzepts* erfolgen.

In der Fein- und Umsetzungsplanung für das TGM SOLLTEN alle in der Sicherheitsrichtlinie und im TGM-Konzept adressierten Punkte berücksichtigt werden.

INF.13.A6 Erstellung eines TGM-Konzepts (S) [Planer]

Ausgehend von der Sicherheitsrichtlinie für das TGM SOLLTE ein TGM-Konzept erstellt und gepflegt werden. Dabei SOLLTEN mindestens folgende Aspekte bedarfsgerecht berücksichtigt werden:

- Methoden, Techniken und Werkzeuge für das TGM
- Absicherung des Zugangs und der Kommunikation
- Absicherung auf Ebene des Netzes, insbesondere Zuordnung von TGM-Komponenten zu Netzsegmenten
- Umfang des Monitorings und der Alarmierung
- Protokollierung von Ereignissen und administrativen Zugriffen
- Meldekettens bei Störungen und Sicherheitsvorfällen
- benötigte Prozesse für das TGM
- Bereitstellung von TGM-Informationen für andere Betriebsbereiche

- Einbindung des TGM in die Notfallplanung

Das TGM-Konzept SOLLTE regelmäßig und zusätzlich bei Bedarf geprüft und gegebenenfalls aktualisiert werden, um dem aktuellen Stand der Technik zu entsprechen und auch neue Erkenntnisse abdecken zu können.

Außerdem SOLLTE regelmäßig ein Soll-Ist-Vergleich zwischen den Vorgaben des Konzepts und dem aktuellen Zustand durchgeführt werden. Dabei SOLLTE insbesondere geprüft werden, ob die Systeme gemäß den Vorgaben konfiguriert sind. Die Ergebnisse SOLLTEN nachvollziehbar dokumentiert werden. Abweichungen SOLLTEN behoben werden.

INF.13.A7 Erstellung eines Funkfrequenzkatasters (S)

Um Funkfrequenzen weitestgehend störungsfrei nutzen zu können, SOLLTE ein Funkfrequenzkataster erstellt werden, dass die Systeme und Nutzer des Frequenzspektrums an den Standorten der Institution listet. Dabei SOLLTE bei einer potentiellen Nutzung von Frequenzen durch unterschiedliche Systeme und Nutzer festgelegt werden, wer auf welchen Frequenzen der Primärnutzer ist. Dabei SOLLTE auch eine Abstimmung zwischen IT und TGM erfolgen. Wird in den Gebäuden OT eingesetzt, SOLLTE auch hier eine Abstimmung erfolgen.

Das Funkfrequenzkataster SOLLTE regelmäßig und zusätzlich bei Bedarf geprüft und gegebenenfalls aktualisiert werden.

INF.13.A8 Erstellung und Pflege eines Inventars für das TGM (S) [Planer]

Für die Dokumentation von Systemen, die durch das TGM verwaltet werden, SOLLTE ein Inventar erstellt und gepflegt werden. Das Inventar SOLLTE vollständig und aktuell gehalten werden. Aus dem Inventar SOLLTEN für alle Systeme Verantwortlichkeiten und Zuständigkeiten ersichtlich sein.

Auch die Elemente der TGM-Infrastruktur selbst SOLLTEN dokumentiert werden.

INF.13.A9 Regelung des Einsatzes von Computer-Aided Facility Management (S) [Planer]

Wird ein Computer-Aided Facility Management-System (CAFM-System) eingesetzt, SOLLTE dieser Einsatz umfassend geplant und konzeptioniert werden. Werden im CAFM Prozesse abgebildet und unterstützt, SOLLTEN entsprechende Rollen- und Berechtigungen definiert werden, insbesondere wenn externe Dienstleister an den Prozessen beteiligt sind.

INF.13.A10 Regelung des Einsatzes von Building Information Modeling (S) [Planer]

Soweit möglich SOLLTE Building Information Modeling (BIM) zur digitalen Modellierung aller relevanten Gebäudedaten eingesetzt werden. Bei der Verwendung von BIM SOLLTE der BIM-Projektentwicklungsplan spezifiziert werden.

Weiterhin SOLLTE die BIM-Architektur umfassend geplant und konzeptioniert werden. Auch für die BIM-Werkzeuge SOLLTE die Informationssicherheit angemessen gewährleistet werden.

INF.13.A11 Angemessene Härtung von Systemen im TGM (S)

Alle Systeme des TGM sowie die Systeme, die durch das TGM betrieben werden, SOLLTEN angemessen gehärtet werden. Die Härtungsmaßnahmen SOLLTEN dokumentiert, regelmäßig und zusätzlich bei Bedarf überprüft und, falls erforderlich, angepasst werden.

Für alle Systeme des TGM sowie die Systeme, die durch das TGM betrieben werden, SOLLTE bei der Beschaffung sichergestellt werden, dass diese angemessen gehärtet werden können und insbesondere sicherheitsrelevante Updates für die geplante Nutzungsdauer bereitgestellt werden.

Systeme, für die keine sicherheitsrelevanten Updates verfügbar sind, SOLLTEN nach Bekanntwerden von Schwachstellen nicht mehr genutzt werden. Wenn dies nicht möglich ist, SOLLTEN die

betroffenen Systeme mit den Mitteln der Netzsegmentierung separiert und die Kommunikation kontrolliert und reglementiert werden.

INF.13.A12 Sichere Konfiguration der TGM-Systeme (S)

Alle Systeme des TGM sowie die Systeme, die durch das TGM betrieben werden, SOLLTEN sicher konfiguriert werden.

Die Konfiguration SOLLTE mindestens vor Inbetriebnahme eines Systems getestet werden. Konfigurationsänderungen während des Produktivbetriebs SOLLTEN vor Aktivierung auf einer Testinstanz getestet oder nur im Vier-Augen-Prinzip durchgeführt werden.

Die Konfiguration von Systemen SOLLTE gesichert werden, um ein schnelles Wiedereinspielen einer fehlerfreien Version zu ermöglichen (Rollback). Rollback-Tests SOLLTEN auf einem Testsystem eingerichtet oder während Wartungsfenstern durchgeführt werden. Die Konfigurationen SOLLTEN zentral gespeichert werden.

Für gleichartige Systeme, inklusive der Geräte der Automations- und Feldebene (siehe Kapitel 4.1 Genutzte TGM-spezifische Fachbegriffe), SOLLTE eine automatisierte Verteilung von Software-Updates und Konfigurationen eingerichtet werden.

Konfigurationsänderungen SOLLTEN allen Beteiligten an Betriebs- und Serviceprozessen (Entstörung, Rufbereitschaft, Wartungen etc.) bekannt gemacht werden, insbesondere

- Änderungen der Zugangsmechanismen oder der Passwörter sowie
- Änderungen an Kommunikations- und Steuerparametern für die eingebundenen Systeme.

Es SOLLTE sichergestellt werden, dass im Störfall beispielsweise ein Wartungstechniker das System bedienen bzw. parametrieren kann.

Außerdem SOLLTE regelmäßig und zusätzlich bei Bedarf geprüft werden, ob die Systeme gemäß den Vorgaben konfiguriert sind. Die Ergebnisse SOLLTEN nachvollziehbar dokumentiert werden. Abweichungen von den Vorgaben SOLLTEN behoben werden.

INF.13.A13 Sichere Anbindung von eingeschränkt vertrauenswürdigen Systemen im TGM (S) [Planer]

Eingeschränkt vertrauenswürdige Systeme, die aus wichtigen betrieblichen Gründen im TGM eingebunden werden müssen, SOLLTEN über ein System angebunden werden, das die Kommunikation mit Hilfe von Firewall-Funktionen kontrolliert und reglementiert. Dieses System SOLLTE in der Verantwortlichkeit des TGM liegen.

INF.13.A14 Berücksichtigung spezieller Rollen und Berechtigungen im TGM (S)

Im Rollen- und Berechtigungskonzept hinsichtlich des TGM SOLLTEN sowohl Nachfrageorganisationen als auch Betreiberorganisationen der TGM-Systeme und der TGA-Systeme berücksichtigt werden. Dies SOLLTE insbesondere dann sorgfältig geplant werden, wenn das TGM institutionsübergreifend bereitgestellt wird.

INF.13.A15 Schutz vor Schadsoftware im TGM (S)

Können auf einem System keine Virenschutzprogramme gemäß Baustein OPS.1.1.4 *Schutz vor Schadprogrammen* ausgeführt werden, beispielsweise aufgrund von knappen Ressourcen oder aufgrund von Echtzeitanforderungen, SOLLTEN geeignete alternative Schutzverfahren eingesetzt werden.

Jedes externe System und jeder externe Datenträger SOLLTE vor der Verbindung mit einem TGM-System und vor der Datenübertragung auf Schadsoftware geprüft werden.

INF.13.A16 Prozess für Änderungen im TGM (S)

Änderungen SOLLTEN immer angekündigt und mit allen beteiligten Gewerken (siehe Kapitel 4.1 Genutzte TGM-spezifische Fachbegriffe), Betreiber- und Nachfrageorganisationen abgestimmt werden. Außerdem SOLLTEN Regelungen für den Fall getroffen werden, dass ein Rückbau von Änderungen mit fehlerhaftem Ergebnis nicht oder nur mit hohem Aufwand möglich ist. Daher sollten im Änderungsmanagement vor Ausführung der Änderung Tests durchgeführt werden, die auch die Fähigkeit des Rückbaus beinhalten. Für die verschiedenen Typen von Änderungen SOLLTE die jeweilige Testtiefe festgelegt werden. Bei der Einführung neuer Systeme und bei großen Änderungen an bestehenden Systemen SOLLTE eine entsprechend hohe Testtiefe vorgesehen werden (siehe INF.13.A22 *Durchführung von Systemtests im TGM*).

INF.13.A17 Regelung von Wartungs- und Reparaturarbeiten im TGM (S)

Gebäudeeinrichtungen SOLLTEN regelmäßig gewartet werden. Hierfür SOLLTE ein Wartungsplan erstellt werden. Es SOLLTE geregelt sein, welche Sicherheitsaspekte bei Wartungs- und Reparaturarbeiten zu beachten sind. Dabei SOLLTEN auch die Abhängigkeiten der verschiedenen Gewerke berücksichtigt werden. Darüber hinaus SOLLTE festgelegt werden, wer für die Wartung oder Reparatur von Einrichtungen zuständig ist. Durchgeführte Wartungsarbeiten SOLLTEN dokumentiert werden.

Es SOLLTE zu jedem Zeitpunkt gewährleistet werden, dass Wartungs- und Reparaturarbeiten, die durch Dritte ausgeführt werden, kontrolliert, ausschließlich abgestimmt durchgeführt und abgenommen werden. Hierfür SOLLTEN interne Mitarbeiter der Haustechnik bestimmt werden, die solche Wartungs- und Reparaturarbeiten autorisieren, beobachten, gegebenenfalls unterstützen und abnehmen.

INF.13.A18 Proaktive Instandhaltung im TGM (S) [Planer]

Für Systeme, die durch das TGM verwaltet werden, SOLLTE eine angemessene proaktive Instandhaltung durchgeführt werden. Hierfür SOLLTEN die regelmäßigen Wartungsintervalle je System festgelegt werden. Zusätzlich SOLLTE je System abgewogen werden, ob ergänzend zur regelmäßigen Instandhaltung eine vorausschauende Instandhaltung (engl. Predictive Maintenance) genutzt werden kann und in welchem Umfang hierdurch die regelmäßigen Wartungsintervalle verlängert werden können.

INF.13.A19 Konzeptionierung und Durchführung des Monitorings im TGM (S) [Planer]

Es SOLLTE ein Konzept für das Monitoring im TGM erstellt und umgesetzt werden. Darin SOLLTE spezifiziert werden, wie die durch das TGM zu verwaltenden Systeme in ein möglichst einheitliches Monitoring eingebunden werden können und welche Werte überwacht werden sollten. Hierfür SOLLTEN schon bei der Anforderungsanalyse erforderliche Schnittstellen für das Monitoring wichtiger Zustände von Systemen spezifiziert werden, die durch das TGM verwaltet werden. Außerdem SOLLTEN auch die für das TGM genutzten Systeme in das Monitoring eingebunden werden.

Das Konzept SOLLTE regelmäßig und zusätzlich bei Bedarf geprüft und gegebenenfalls aktualisiert werden, um dem aktuellen Stand der Technik zu entsprechen und auch neueste Erkenntnisse abdecken zu können.

Statusmeldungen und Monitoringdaten SOLLTEN NUR über sichere Kommunikationswege übertragen werden.

INF.13.A20 Regelung des Ereignismanagements im TGM (S) [Planer]

Im TGM auftretende Ereignisse SOLLTEN hinsichtlich ihrer Bedeutung und ihres Einflusses kategorisiert, gefiltert und klassifiziert werden (englisch Event Management). Für die Ereignisse SOLLTEN Schwellwerte definiert werden, die eine automatisierte Einstufung von Ereignissen ermöglichen. Je nach Klassifizierung der Ereignisse SOLLTEN entsprechende Maßnahmen für

Monitoring, Alarmierung und Meldewege (Eskalation) sowie Maßnahmen zur Protokollierung bestimmt werden.

INF.13.A21 Protokollierung im TGM (S)

Ereignisse, die im Ereignismanagement entsprechend klassifiziert wurden, SOLLTEN protokolliert werden. Außerdem SOLLTEN für die Systeme sicherheitsrelevante Ereignisse protokolliert werden.

Alle Konfigurationszugriffe sowie alle manuellen und automatisierten Steuerungszugriffe SOLLTEN protokolliert werden. Abhängig vom Schutzbedarf SOLLTE eine vollumfängliche Protokollierung inklusive Metadaten und Inhalt der Änderungen erfolgen.

Die Protokollierung SOLLTE auf einer zentralen Protokollierungsinstanz zusammengeführt werden.

Protokollierungsdaten SOLLTEN NUR über sichere Kommunikationswege übertragen werden.

Bei sicherheitskritischen Ereignissen SOLLTE automatisch alarmiert werden.

INF.13.A22 Durchführung von Systemtests im TGM (S) [Planer]

Systeme des TGM und Systeme, die durch das TGM verwaltet werden, SOLLTEN vor der Inbetriebnahme und bei großen Systemänderungen hinsichtlich ihrer funktionalen und nicht-funktionalen Anforderungen getestet werden. Dabei SOLLTE auch das Soll- und Ist-Verhalten von Funktionen und Einstellungen geprüft werden. Bei den nicht-funktionalen Anforderungen SOLLTEN auch Anforderungen der Informationssicherheit getestet sowie zusätzlich bei Bedarf auch Lasttests durchgeführt werden. Für die Tests SOLLTE eine Testspezifikation erstellt werden, die eine Beschreibung der Testumgebung, der Testtiefe und der Testfälle inklusive der Kriterien für eine erfolgreiche Testdurchführung enthält. Die Testdurchführung SOLLTE in einem Testbericht dokumentiert werden.

Testspezifikationen SOLLTEN regelmäßig und zusätzlich bei Bedarf geprüft und gegebenenfalls aktualisiert werden, um dem aktuellen Stand der Technik zu entsprechen und auch neueste Erkenntnisse abdecken zu können.

INF.13.A23 Integration des TGM in das Schwachstellenmanagement (S)

Systeme des TGM und die durch das TGM verwalteten Systeme SOLLTEN fortlaufend hinsichtlich möglicher Schwachstellen überwacht werden.

Hierfür SOLLTEN regelmäßig Informationen über bekanntgewordene Schwachstellen eingeholt und entsprechend berücksichtigt werden. Hierbei SOLLTE auch die Konfiguration der Systeme dahingehend überprüft werden, ob sie bekannt gewordene Schwachstellen begünstigt.

Weiterhin SOLLTE entschieden werden, für welche Systeme regelmäßig oder zumindest bei Inbetriebnahme und bei großen Systemänderungen Schwachstellen-Scans durchgeführt werden. Für Schwachstellen-Scans SOLLTE die Scan-Tiefe festgelegt werden. Außerdem SOLLTE festgelegt werden, ob ein passiver oder ein aktiver Scan durchgeführt wird. In Produktivumgebungen SOLLTEN passive Scans bevorzugt werden. Aktive Scans SOLLTEN in Produktivumgebungen nur durchgeführt werden, wenn sie notwendig sind und Personal hinzugezogen wird, das durch den Scan bedingte, eventuell auftretende Fehler oder Ausfälle beheben kann.

INF.13.A24 Sicherstellung der Kontrolle über die Prozesse bei Cloud-Nutzung für das TGM (S) [Planer]

Werden im TGM Cloud-basierte Dienste genutzt, SOLLTE die Kontrolle über alle TGM-Prozesse im TGM verbleiben. Dies SOLLTE bei Nutzung eines Cloud-Dienstes bei einem Cloud-Anbieter vertraglich festgelegt werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

INF.13.A25 Aufbau einer Testumgebung für das TGM (H) [Planer]

Bei erhöhtem Schutzbedarf SOLLTE für Systeme des TGM und für Systeme, die durch das TGM verwaltet werden, eine Testumgebung eingerichtet werden, damit Hard- und Software vor der Inbetriebnahme und bei Änderungen getestet und Fehler im produktiven Betrieb reduziert werden können. Außerdem SOLLTEN Regelungen für den Umgang mit Systemen spezifiziert werden, für die keine Testumgebung aufgebaut werden kann.

INF.13.A26 Absicherung von BIM (H) [Planer]

Werden in BIM auch sicherheitskritische Informationen erfasst, SOLLTEN sowohl auf Ebene der BIM-Architektur als auch für Implementierung und Betrieb der BIM-Lösung entsprechende Sicherheits- und Härungsmaßnahmen vorgesehen werden. Die Absicherung SOLLTE ein verschärftes Rollen- und Berechtigungskonzept sowie weitergehende Schutzmaßnahmen wie Verschlüsselung, Segmentierung und höherwertige Authentisierungsmechanismen, insbesondere eine 2-Faktor-Authentisierung beinhalten.

INF.13.A27 Einrichtung einer Private Cloud für das TGM (H) [Planer]

Bei erhöhtem Schutzbedarf SOLLTEN Cloud-Dienste zum TGM in einer Private Cloud On-Premises oder einer Private Cloud bei einem vertrauenswürdigen Cloud-Anbieter positioniert werden. Der Einsatz einer Public Cloud SOLLTE vermieden werden.

INF.13.A28 Sichere Nutzung von Künstlicher Intelligenz im TGM (H)

Werden bei erhöhtem Schutzbedarf im TGM Funktionen der Künstlichen Intelligenz (KI) genutzt, SOLLTE nur eine KI genutzt werden, die nachweislich sicher ist. Mindestens SOLLTE darauf geachtet werden, dass keine Daten in Netze geleitet werden, die nicht zur eigenen Institution gehören oder nicht vertrauenswürdig sind.

Für Cloud-basierte KI-Dienste SOLLTEN über die Anforderungen des Bausteins OPS.2.2 *Cloud-Nutzung* hinaus auch die Kriterien des AI Cloud Service Compliance Criteria Catalogue (AIC4) des BSI berücksichtigt werden.

INF.13.A29 Integration des TGM in ein SIEM (H) [IT-Betrieb]

Wird ein System für das Security Information and Event Management (SIEM) genutzt, SOLLTEN die Systeme des TGM und soweit möglich auch die durch das TGM verwalteten Systeme entsprechend eingebunden werden, um system- und anwendungsübergreifende sicherheitsrelevante Vorfälle erkennen und analysieren zu können.

INF.13.A30 Durchführung von Penetrationstests im TGM (H)

Um Systeme des TGM und Systeme, die durch das TGM verwaltet werden, entsprechend abzusichern, SOLLTEN bedarfsorientiert Penetrationstests durchgeführt werden. Mindestens SOLLTEN vor der Inbetriebnahme und bei großen Systemänderungen in einer Testumgebung Penetrationstests durchgeführt werden.

Werden im TGM Funktionen der KI genutzt, SOLLTEN diese in die Penetrationstests einbezogen werden.

4. Weiterführende Informationen

4.1. Genutzte TGM-spezifische Fachbegriffe

Automationsebene

Die Automationsebene befindet sich in der Automatisierungspyramide zwischen der Feldebene und der Managementebene. Sie führt die von der Feldebene gelieferten Daten sowie die von der Managementebene übermittelten Vorgaben zusammen. Hier erfolgt die Steuerung und Regelung der TGA-Anlagen, aber auch die Überwachung von Grenzwerten, Schaltzuständen oder Zählerständen.

Building Information Modeling (BIM)

Gemäß VDI 2552 Blatt 2 ist BIM eine Methodik zur Planung, zur Ausführung und zum Betrieb von Bauwerken mit einem kollaborativen Ansatz auf Grundlage eines digitalen Informationsmodells des Bauwerks zur gemeinschaftlichen Nutzung.

Computer-Aided Facility Management (CAFM)

Gemäß VDI 3814 Blatt 2.1 dient CAFM als Werkzeug zur Erfassung, Verarbeitung, Aufbereitung und Archivierung von Daten und Informationen mit dem Ziel, die Leistungsprozesse und Aufgaben in der Betriebsphase eines Gebäudes zu unterstützen.

Feldebene

Die Feldebene stellt die unterste Ebene der Automatisierungspyramide dar und umfasst unterschiedliche Komponenten der GA oder OT. In der Regel werden hier Sensoren und Aktoren betrieben. Sensoren erfassen Informationen (z. B. Bewegung, Helligkeit, Temperatur) und senden diese an die Automationsebene. Aktoren empfangen Steuerinformationen und setzen diese in Schaltsignale um, z. B. für die Beleuchtungs-, Heizungs-, Klima- und Lüftungsanlage.

Gebäude

Der Begriff Gebäude wird im Baustein INF.13 *Technisches Gebäudemanagement* und in den zugehörigen Umsetzungshinweisen synonym für Gebäude, Gebäudekomplex, Liegenschaft und Liegenschaftsportfolio genutzt. Außerdem beschreibt der Begriff Gebäude nicht nur Häuser und Hallen, sondern auch beispielsweise einen Fernsehturm oder eine Bohrinself.

Gebäudeautomation (englisch Building Automation and Control Systems, BACS)

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

Gebäudekomplex

Ein Gebäudekomplex ist eine Gruppe von Gebäuden, die baulich miteinander verbunden sind und als Gesamteinheit wahrgenommen 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: Raumlufthtechnische Anlagen (Kostengruppe 430 in DIN 276), wozu etwa Lüftungsanlagen, Klimaanlage und Kälteanlagen gehören.

Leitstand (englisch Control Center)

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

Liegenschaft

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.

Liegenschaftsportfolio

Als Liegenschaftsportfolio wird die Gesamtheit der Liegenschaften im Besitzstand bezeichnet.

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.

System

Der Begriff System adressiert im Baustein INF.13 *Technisches Gebäudemanagement* und in den zugehörigen Umsetzungshinweisen nicht nur ein IT-System im klassischen Sinn (vgl. Bausteine der Schicht SYS), sondern umfasst auch alle Komponenten der TGA einschließlich aller Komponenten der Feldebene, wie Sensoren, Aktoren usw.

Technische Gebäudeausrüstung (englisch Building Services, BS)

Die Technische Gebäudeausrüstung (TGA) umfasst gemäß VDI 4700 Blatt 1 alle im Bauwerk eingebauten und damit verbundenen technischen Einrichtungen und nutzungsspezifischen Einrichtungen sowie technische Einrichtungen in Außenanlagen und Ausstattungen. Gewisse Komponenten der Gebäudeautomation 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.

4.2. Abkürzungen

Abkürzung	Bedeutung
AI	Artificial Intelligence
AIC4	AI Cloud Service Compliance Criteria Catalogue
BACS	Building Automation and Control Systems
BIM	Building Information Modelling
BS	Building Services
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAFM	Computer-Aided Facility Management
DIN	Deutsches Institut für Normung
GA	Gebäudeautomation
GM	Gebäudemanagement
ICS	Industrial Control System
ISB	Informationssicherheitsbeauftragter
IT	Informationstechnik

Abkürzung	Bedeutung
KI	Künstliche Intelligenz
KRT	Kreuzreferenztablette
OT	Operational Technology
SIEM	Security Information and Event Management
SIS	Safety Instrumented Systems
SLA	Service Level Agreement
TBM	Technical Building Management
TGA	Technische Gebäude-Ausstattung
TGM	Technisches Gebäude-Management
VDI	Verein Deutscher Ingenieure e.V.

4.3. Wissenswertes

Genannte Normen und Dokumente:

- AI Cloud Service Compliance Criteria Catalogue (AIC4), Bundesamt für Sicherheit in der Informationstechnik, Februar 2021, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/AIC4/AI-Cloud-Service-Compliance-Criteria-Catalogue_AIC4.html
- BSI-CS 108 - Fernwartung im industriellen Umfeld, BSI Veröffentlichung zur Cyber-Sicherheit, Juli 2018, aufrufbar über https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_108.pdf
- DIN 276 – Kosten im Bauwesen, Deutsches Institut für Normung e.V., Dezember 2018, verfügbar im Beuth-Verlag
- DIN 32736 – Gebäudemanagement – Begriffe und Leistungen, Deutsches Institut für Normung, August 2000, verfügbar im Beuth-Verlag
- VDI 4700 Blatt 1 – Begriffe der Bau- und Gebäudetechnik, Verein Deutscher Ingenieure e.V., Oktober 2015, verfügbar im Beuth-Verlag

5. Anlage: Kreuzreferenztablette zu elementaren Gefährdungen

Aus jeder Anforderung (A) in diesem Baustein können Sicherheitsmaßnahmen abgeleitet werden. Die Umsetzung dieser Maßnahmen wirkt denjenigen elementaren Gefährdungen (G0) entgegen, die für das Thema bzw. Zielobjekt relevant sind. In der Kreuzreferenztablette (KRT) zu diesem Baustein sind jeder Anforderung die entsprechenden elementaren Gefährdungen zugeordnet.

Anhand der KRT lässt sich ermitteln, welche elementaren Gefährdungen durch welche Anforderungen abgedeckt sind. Die Buchstaben in der zweiten Spalte zeigen an, welche Grundwerte der Informationssicherheit durch die Anforderung vorrangig geschützt werden. Diese Grundwerte sind Confidentiality (C) für Vertraulichkeit, Integrity (I) für Integrität sowie Availability (A) für Verfügbarkeit.

Die folgenden elementaren Gefährdungen sind für den Baustein INF.13 *Technisches Gebäudemanagement* von Bedeutung:

G 0.9 Ausfall oder Störung von Kommunikationsnetzen

G 0.10 Ausfall oder Störung von Versorgungsnetzen

G 0.14 Ausspähen von Informationen (Spionage)

G 0.15 Abhören

- G 0.18 Fehlplanung oder fehlende Anpassung
- G 0.19 Offenlegung schützenswerter Informationen
- G 0.21 Manipulation von Hard- oder Software
- G 0.22 Manipulation von Informationen
- G 0.23 Unbefugtes Eindringen in IT-Systeme
- G 0.24 Zerstörung von Geräten oder Datenträgern
- G 0.25 Ausfall von Geräten oder Systemen
- G 0.26 Fehlfunktion von Geräten oder Systemen
- G 0.27 Ressourcenmangel
- G 0.28 Software-Schwachstellen oder -Fehler
- G 0.29 Verstoß gegen Gesetze oder Regelungen
- G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen
- G 0.32 Missbrauch von Berechtigungen
- G 0.33 Personalausfall
- G 0.37 Abstreiten von Handlungen
- G 0.39 Schadprogramme
- G 0.41 Sabotage
- G 0.43 Einspielen von Nachrichten
- G 0.44 Unbefugtes Eindringen in Räumlichkeiten
- G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe