ZUKUNFT BAU
FORSCHUNGSFÖRDERUNG

Bundesinstitut
für Bau-, Stadt- und
Raumforschung
im Bundesamt für Bauwesen
und Raumordnung

BBSR-
Online-Publikation
24/2023

Open-BIM-Unterstützung für sichere Smart Buildings

von

Arne Wall
Björn Butzin
Dr.-Ing. Michael Rethfeldt
Prof. Dr.-Ing. Dirk Timmermann

Open-BIM-Unterstützung für sichere Smart Buildings

Modellbasierte, sichere Kommissionierung und Konfiguration
für Gebäudeautomation und Smart Home

Gefördert durch:

Bundesministerium
für Wohnen, Stadtentwicklung
und Bauwesen

aufgrund eines Beschlusses
des Deutschen Bundestages

ZUKUNFT BAU
FORSCHUNGSFÖRDERUNG

Dieses Projekt wurde gefördert vom Bundesinstitut für Bau-, Stadt- und Raumforschung (BBSR) im Auftrag des Bundesministeriums für Wohnen, Stadtentwicklung und Bauwesen (BMWSB) aus Mitteln des Innovationsprogramms Zukunft Bau.
Aktenzeichen: 10.08.18.7-18.37
Projektlaufzeit: 01.2019 bis 12.2021

IMPRESSUM

Herausgeber
Bundesinstitut für Bau-, Stadt- und Raumforschung (BBSR)
im Bundesamt für Bauwesen und Raumordnung (BBR)
Deichmanns Aue 31–37
53179 Bonn

Fachbetreuer
Steffen Kisseler, Brüggemann Kisseler Ingenieure
im Auftrag des BBSR, Referat WB 3 „Forschung und Innovation im Bauwesen“
zb@bbr.bund.de

Autoren
Universität Rostock, Institut für Angewandte Mikroelektronik und Datentechnik
Prof. Dr.-Ing. Dirk Timmermann (Projektleitung)
dirk.timmermann@uni-rostock.de

Arne Wall, M. Sc.
arne.wall@uni-rostock.de

Björn Butzin, M. Sc.
bjoern.butzin@uni-rostock.de

Dr.-Ing. Michael Rethfeldt
michael.rethfeldt@uni-rostock.de

Lektorat/Korrektorat
Universität Rostock, Institut für Angewandte Mikroelektronik und Datentechnik
Dr.-Ing. Michael Rethfeldt

Stand
Februar 2022

Gestaltung
Universität Rostock, Institut für Angewandte Mikroelektronik und Datentechnik
Dr.-Ing. Michael Rethfeldt

Bildnachweis
Titelbild: Universität Rostock, Institut für Angewandte Mikroelektronik und Datentechnik

Vervielfältigung
Alle Rechte vorbehalten

Der Herausgeber übernimmt keine Gewähr für die Richtigkeit, die Genauigkeit und Vollständigkeit der Angaben sowie für die Beachtung privater Rechte Dritter. Die geäußerten Ansichten und Meinungen müssen nicht mit denen des Herausgebers übereinstimmen.

Zitierweise
Wall, Arne; Butzin, Björn; Rethfeldt, Michael; Timmermann, Dirk: Open-BIM-Unterstützung für sichere Smart Buildings: Modellbasierte, sichere Kommissionierung und Konfiguration für Gebäudeautomation und Smart Home. BBSR-Online-Publikation 24/2023, Bonn.

ISSN 1868-0097 Bonn 2023

Inhaltsverzeichnis

Kurzfassung 5

Abstract 7

Einführung und Problemstellung 9

Schwerpunkt 1: Middleware für die Gebäudeautomation 10
Einheitliches Vokabular für die abstrakte Beschreibung von GA-Komponenten 10
Finden von konkreten Instanzen auf Basis von abstrakten Beschreibungen und Informationszugriff 13

Schwerpunkt 2: Sicherheitsarchitektur für die Gebäudeautomation 15
Security-Bedrohungen und grundlegender Lösungsansatz 16
Gerätekonfiguration durch Nutzer zur Laufzeit 34
Dezentrale Speicherung von Log-Daten 35
Abgeleitete Sicherheitsvorteile 36

Ergebnisverwertung 38

Fazit 41

Mitwirkende 42
Autorinnen und Autoren 42

Verzeichnisse 43
Abbildungsverzeichnis 45
Tabellenverzeichnis 46

Kurzfassung

Heutige Gebäudeautomations (GA)- Anwendungen müssen für jedes Gebäude individuell konfiguriert werden, was deren Inbetriebnahme aufwendig und teuer macht. Für eine breite Anwendung von etwa Ambient Assisted Living oder Continuous Commissioning ist daher eine universellere Herangehensweise erforderlich. Ein Ansatz hierfür ist die Verwendung maschinell lesbarer Geräte-, Daten- und Funktions-Beschreibungen anstelle der dominierenden Datenpunkt-Adressierung (z. B. Gerät 7, Klemme 4). Diese Abstrahierung von technischen Details vereinfacht die Inbetriebnahme und Wiederverwendung von Anwendungen maßgeblich. Derzeit existieren einige Ansätze der Modellierung für derartige Systeme, ein einheitliches Modell existiert jedoch nicht. Im ersten Schwerpunkt des Projektes wurden daher Methoden entwickelt, um die bestehenden Teilmodelle zu einem Gesamtmodell zusammenzufügen. Open-BIM und IFC können mit diesem Gesamtmodell um funktionale Aspekte der GA erweitert werden. Im zweiten Schwerpunkt wurde ein Konzept für Smart Home entwickelt, das die zusätzlichen Informationen zur Realisierung höherwertiger Dienste für Sicherheits- und Komfortfunktionen verwendet. Die Ergebnisse aus unseren bisherigen BBSR-Projekten wurden zusammengeführt um die verbliebenen Schutzziele der Informationssicherheit, Verfügbarkeit und Zurechenbarkeit hinzuzufügen. Dies wird durch einen verteilten Ansatz zur Gerätekonfiguration und -steuerung erreicht, der die Prüfung auf Konfigurationskonflikte ermöglicht und deren Auftreten möglichst vermeidet. Da sichere Geräte nicht auch ein sicheres Gesamtsystem zur Folge haben, ist ein ganzheitlicher Ansatz notwendig.

Der erste Schwerpunkt basiert auf der Beschreibung von Geräten, Daten und Funktionen, sodass diese maschinell gesucht werden können. Grundvoraussetzung dafür ist ein einheitliches Modell und eine geeignete Abfragesprache, welche jedoch derzeit weder für GA- noch Smart Home-Geräte, deren Prozessdaten oder Funktionen existieren. Forschungsansätze, welche auf ein bestimmtes Ziel hin entwickelt wurden (z. B. Fehlerdetektion), zeigen vielversprechende Resultate, stellen aber individuelle Lösungen dar. Daher wurden Methoden entwickelt und evaluiert, um bestehende Modelle miteinander zu verknüpfen und somit die Grundlage für eine inhaltliche Datenvermittlung in der Praxis zu schaffen. Insbesondere fehlerhafte und inkompatible Teilmodelle müssen dabei berücksichtigt werden. Für die Abfrage und Vermittlung der Informationen wurde eine Schnittstelle implementiert, welche ausschließlich offene Internettechnologien mit dem Fokus auf eine lose Kopplung der Systemteilnehmer verwendet. Dabei ist die Integration in den Bestand eine zusätzliche Herausforderung, um eine zügige Etablierung dieser Technik zu ermöglichen. Zudem wurden die Beschreibungen mit Elementen aus Open-BIM-Modellen verknüpf, um etwa die Realisierung intelligenter Energiesparfunktionen zu ermöglichen. So können etwa die thermischen Eigenschaften von Wänden genutzt werden, um die Heizungssteuerung automatisch zu optimieren.

Im zweiten Schwerpunkt wurde eine Sicherheitsarchitektur für Gebäudeautomationssysteme unter Verwendung des Open-BIM-Ansatzes ausgearbeitet. Ein zentraler Security Controller, der auf zertifizierter Hardware beruht, kommuniziert über den im Schwerpunkt 1 entwickelten Broker mit den Geräten und der Netzwerkinfrastruktur. Damit die Kommunikation vereinheitlicht und portabel gestaltet werden kann, wird die Ontologie durch ein entsprechendes Vokabular für Security- und Netzwerkkonfigurationen erweitert. Der Aspekt, die Ontologie durch entsprechende Konfigurationselemente anzureichern (Erweiterung des Vokabulars), um protokollunabhängig mit den Geräten zu kommunizieren, war im ursprünglichen Antrag grob skizziert. Während der ersten Laufzeithälfte konnte diese Schnittstelle zwischen beiden Schwerpunkten näher spezifiziert werden. Durch die Annotation von Geräten an das Open-BIM-Modell kann die örtliche Verteilung der Geräte im Gebäude beschrieben werden. Der Security Controller erhält durch dieses globale Netzwerkwissen die Fähigkeit, Security-Konfigurationen zu generieren und das Netzwerk samt Geräten zu konfigurieren. Des Weiteren lag im zweiten Schwerpunkt der Fokus auf der Konfigurierbarkeit von Geräten und Funktionen durch den Nutzer. Dabei wurde berücksichtig, dass die individuelle, sichere Konfiguration einzelner Geräte im Gesamtsystem dennoch zu einem Fehlverhalten führen kann, welches sich z. B. von Hackern ausnutzen lässt. Die Problemstellung bestand folglich aus einer geeigneten Zusammenführung und Analyse der Konfiguration des Gesamtsystems zur Erkennung und Vermeidung von Konfigurationskonflikten. Im Laufe der Arbeiten hat sich herauskristallisiert, dass es sinnvoll ist, Anwendungskonfigurationen einmalig durch den vorgeschlagenen Security Controller zu prüfen. Anschließend werden die Geräte, die zusammen eine Anwendung bilden, durch eine Trust Zone isoliert. Neben den resultierenden Security-Vorteilen (Abschottung zu potentiell

bösartigen Netzwerkteilnehmern und Geräten) können keine Kollisionen auf Anwendungsebene stattfinden. Eine Kollision beschreibt das Steuern eines Aktors mit widersprüchlichen Steueranweisungen (z. B. gleichzeitige Fenstersteuerung auf und zu). Weiterhin wurden Konzepte zur Vermeidung eines Single Point of Failure bei der sicheren Protokollierung von Vorgängen, wie z. B. Nutzungsaktivitäten oder Hacker-Attacken, erarbeitet. Dazu wurden verschiedene Lösungsansätze, wie zum Beispiel Blockchains, untersucht. Ergebnis der Untersuchung: Da sich alle Geräte einer Anwendung in einer geschützten Trust Zone befinden, werden die Log-Daten dezentral innerhalb der isolierten Zone gespeichert. Nach der von uns vorgeschlagenen Kommissionierung erhält jedes Gerät Schlüsselmaterial, um mithilfe von digitalen Signaturen eigene Log-Daten zu signieren und sie anschließend redundant im Netzwerk zu speichern. Blockchain-Technologien, die auf dem Proof-of-Work-Prinzip zur Erstellung neuer Einträge bestehen, sind für den Einsatz in einer Gebäudeautomation oder einem Smart Home nicht anwendbar, da sie aufgrund der Ressourcenauslastung auf eingebetteten Systemen nicht geeignet sind. Stattdessen ist es vielversprechender, P2P-basierte Verteilungsansätze zur redundanten Speicherung zu wählen.

Das Forschungsprojekt konnte zeigen, dass sich Anwendungen für Gebäudeautomationssysteme allgemeingültig formulieren und auf eine reale Installation abbilden lassen. Dazu werden Modelle inklusive dem BIM geschickt miteinander verknüpft, um maschinell lesbare Geräte-, Daten- und Funktions-Beschreibungen zu schaffen, die von gebäudespezifischen Datenpunkten abstrahieren. Die Konzepte wurden in Form eines Demonstrators implementiert. Reale BACnet- und CoAP-Geräte, die an ein exemplarisches IFC-Modell annotiert worden sind, lassen sich von einer Weboberfläche ansteuern. Die Interfaces zwischen den entwickelten Komponenten des Demonstrators basieren auf dem offenen HTTP-Standard, sodass eine modulare Erweiterung/Anpassung möglich ist. Des Weiteren haben die Arbeiten gezeigt, wie globales Wissen über die Gebäudeautomationsanlage genutzt werden kann, um einen verbesserten Schutz gegen Computersabotage zu erzielen. Wichtige Informationen über die Gebäudestruktur (BIM) in Kombination mit universellen Sicherheitsrichtlinien dienen als Grundlage für einen Partitionierungsalgorithmus, der jedes Gerät in einen geschützten Netzwerkbereich gruppiert. Innerhalb eines solchen Bereichs (Trust Zone) können die eigentlichen Anwendungen ausgeführt und Daten redundant gesichert gespeichert werden. Neben den sicherheitskritischen Entscheidungen des Partitionierungsalgorithmus werden formal beschriebene Anwendungsgraphen auf ihre Korrektheit verifiziert und an jedes Endgerät über einen abgesicherten Kanal (Vertraulichkeit, Integrität und Authentizität) übertragen. In Form einer praktischen Realisierung wurde der geringe Implementierungsaufwand für zusätzliche Gerätefunktionalitäten gezeigt.

Abstract

Today's building automation applications have to be configured individually for each building, which makes them complex and expensive to commission. A more universal approach is therefore required to achieve a broad prevalence of, for example, Ambient Assisted Living or Continuous Commissioning. One approach to this is to use machine-readable device, data, and function descriptions instead of the dominant data point addressing (e.g., device 7, clamp 4). This abstraction of technical details significantly simplifies the commissioning and reuse of applications. Currently, some approaches of modeling for such systems exist, but a unified model is still missing. Therefore, in the first research area of the project, methods were developed to combine existing partial models into an overall model. Open-BIM and IFC can be extended with this overall model to include functional aspects of building automation. In the second research area, a concept for Smart Home was developed that uses the additional information to realize higher-value services for security and comfort functions. The results from our previous BBSR projects were merged to add the remaining protection goals of information security, availability, and accountability. This is achieved through a distributed approach to device configuration and control, which enables testing for configuration conflicts and avoids their occurrence whenever possible. Since secure devices do not also result in a secure overall system, a holistic approach is necessary.

The first research area focuses on the description of devices, data, and functions so that they become machine-readable and searchable. The basic prerequisite for this is a uniform model and a suitable query language, which, however, do not currently exist for either building automation or smart home devices, their process data, or functions. Research approaches, which were developed with a specific goal in mind (e.g., fault detection), show promising results, but represent individual solutions. Therefore, methods have been developed and evaluated to link existing models and thus create the basis for a content-centric data dissemination in practice. In particular, erroneous and incompatible sub-models must be taken into account. For querying and delivering the information, an interface was implemented that exclusively uses open Internet technologies with focus on a loose coupling of the system participants. Thereby, the integration into existing installations is an additional challenge to enable a rapid establishment of this technology. In addition, the descriptions were linked with elements from Open-BIM models, e.g., to enable the realization of intelligent energy-saving functions. For example, the thermal properties of walls could be used to automatically optimize heating control.

In the second research area, a security architecture for building automation systems was developed using the Open-BIM approach. A central security controller based on certified hardware communicates with the devices and the network infrastructure via the middleware developed in research area 1. In order to make the communication unified and portable, the ontology is extended by a corresponding vocabulary for security and network configurations. The aspect of enriching the ontology with appropriate configuration elements (extending the vocabulary) to communicate with the devices in a protocol-independent way was roughly outlined in the original proposal. During the first half of the project runtime, this interface between the two research areas could be specified in more detail. By annotating devices to the Open-BIM model, the location and distribution of devices in the building can be described. This global network knowledge gives the security controller the ability to generate security configurations and to configure the network infrastructure and end devices.

Furthermore, the second research focus was on the configurability of devices and functions by the user. It was taken into account that, despite a secure configuration of individual devices, there might still be misbehavior in the overall system that can be exploited, e.g., by hackers. Consequently, the challenge consisted of a suitable consolidation and analysis of the configuration of the overall system to detect and avoid configuration conflicts. During the course of the work, it became apparent that it makes sense to check application configurations once through the proposed security controller. Subsequently, the devices that together form an application are isolated by a trust zone. In addition to the resulting security benefits (isolation from potentially malicious network participants and devices), no conflicts can occur at the application level. A conflict describes the control of an actuator with contradictory control instructions (e.g., simultaneous window control open and close). Furthermore, concepts for avoiding a single point of failure in the secure logging of operations, such as usage activities or hacker attacks, were developed. For this purpose, various solution approaches, such as Blockchains, were investigated. Result of the investigation: since all

devices of an application are located in a protected trust zone, the log data is stored in a decentralized manner within the isolated zone. After our proposed commissioning step, each device receives key material to sign its own log data using digital signatures and then store it redundantly on the network. Blockchain technologies that insist on the proof-of-work principle to create new entries are not suitable for use in a building automation or smart home scenario due to resource utilization on embedded systems. Contrarily, P2P-based distribution approaches for redundant storage can be adopted.

The research project was able to show that applications for building automation systems can be described in a uniform way and mapped to a real installation. For this purpose, models including the BIM are linked in a suitable way to create machine-readable device, data and function descriptions that abstract from building-specific data points. The concepts were implemented in the form of a demonstrator. Real BACnet and CoAP devices, which have been annotated to an exemplary IFC model, can be controlled from a web interface. The interfaces between the developed components of the demonstrator are based on the open HTTP standard, so that a modular extension/adaptation is possible. Furthermore, the work has shown how global knowledge about the building automation system can be used to achieve improved protection against computer sabotage. Key information about the building structure (BIM) combined with universal security policies serve as the basis for a partitioning algorithm that groups each device into a protected network area. Within such an area (trust zone), the actual applications can be executed and data can be stored in a redundant manner. In addition to the security-critical decisions of the partitioning algorithm, formally described application graphs are verified for correctness and transmitted to each end device via a secured channel (confidentiality, integrity, and authenticity). In the form of a practical realization, the low implementation effort for integrating additional device functionalities was demonstrated.

Einführung und Problemstellung

Heutige Gebäudeautomations (GA)-Anwendungen müssen für jedes Gebäude individuell konfiguriert werden, was deren Inbetriebnahme aufwendig und teuer macht. Für eine breite Anwendung von intelligenten GA-Technologien ist daher eine universellere Herangehensweise erforderlich. Ein Ansatz hierfür ist die Verwendung maschinell lesbarer Geräte-, Daten- und Funktions-Beschreibungen, anstelle der dominierenden Datenpunkt-Adressierung (z. B. Gerät 7, Klemme 4). Diese Abstrahierung von technischen Details vereinfacht die Inbetriebnahme und Wiederverwendung von Anwendungen maßgeblich. So ist beispielsweise das Konzept einer Klimaanlage gebäudeübergreifend nutzbar. Derzeit existieren einige Ansätze der Modellierung für derartige Systeme, ein einheitliches Modell existiert jedoch nicht. Ziel dieses Projektes war es daher, die Modellierung von GA-Systemen zu vereinfachen und zu vereinheitlichen. Dadurch werden die Verwendung und Planbarkeit dieser Systeme befördert und wirtschaftlicher gestaltet. Bisher gab es vor allem Einzelansätze im Bereich Smart Home, die keine einheitlichen Datenmodelle zur Beschreibung von Komponenten und deren Zusammenhang berücksichtigen. Eine Anknüpfung an Open-BIM (Building Information Modeling) und dazugehörige Standards verbreitern das Anwendungsfeld und ermöglichen es, die jeweiligen Informationen in beide Richtungen als Mehrwert zu nutzen. Ein zweiter Schwerpunkt behandelte die sichere Auslegung und Konfiguration des Gesamtsystems. Dazu wurde ein ganzheitliches Kommissionierungskonzept entwickelt, das GA-Netzwerke modellgestützt und anwendungsgetrieben in sichere Vertrauensbereiche partitioniert und die verteilten Gerätekonfigurationen im Gesamtkontext überprüft, um sicherheitsrelevante Schwachstellen und kritische Punkte im System zu identifizieren und zu vermeiden.

Im ersten Schwerpunkt des Projektes wurden Methoden entwickelt, um bestehende Teilmodelle zu einem Gesamtmodell zusammenzufügen. Open-BIM und IFC (Industry Foundation Classes) können auf diese Weise um funktionale Aspekte der GA erweitert werden. Um die definierten Ziele zu erreichen, wurde eine umfangreiche, theoretisch-analytische Herangehensweise gewählt. Vorhandene Informationsmodelle und Begriffssammlungen (Ontologien) wurden analysiert und als Teilmodelle so aufbereitet, dass ein definiertes und logisch durchsuchbares Gesamtmodell entsteht. Hier wurde eine geeignete Schnittstellendefinition gefunden, um Komponenten möglichst neutral und damit hersteller- und systemunabhängig beschreibbar und auffindbar zu machen. Die für die Abfrage und Vermittlung der Informationen entwickelte Schnittstelle verwendet ausschließlich offene Internettechnologien mit dem Fokus auf eine lose Kopplung der Systemteilnehmer sowie semantische Interoperabilität. Folglich verringert sich der Implementierungsaufwand für darüber liegende GA-Anwendungen erheblich und diese müssen keine spezifischen Gebäudeautomationsprotokolle mehr beherrschen oder zwischen Geräten unterschiedlicher Protokolle unterscheiden können.

Im zweiten Schwerpunkt wurde ein Konzept entwickelt, das die zusätzlichen GA-Informationen, welche durch die im ersten Schwerpunkt entwickelte Schnittstelle bereitgestellt werden, zur Realisierung höherwertiger Dienste für Sicherheits- und Komfortfunktionen verwendet. Um die Sicherheit des Gesamtsystems zu gewährleisten, wurden die Ergebnisse aus unseren früheren BBSR-Projekten zusammengeführt und die bisherigen Schutzziele um die Aspekte der Informationssicherheit, sicheren Anwendungsisolation und logischen Überprüfbarkeit von Konfigurationen erweitert. Dies wird durch einen verteilten Ansatz zur Gerätekonfiguration und -steuerung erreicht, der die Prüfung auf Konfigurationskonflikte ermöglicht und deren Auftreten möglichst vermeidet. Da sichere Geräte nicht notwendigerweise auch ein sicheres Gesamtsystem zur Folge haben, ist ein ganzheitlicher Ansatz notwendig. Der Einfluss von Konfigurationsvorgängen an verschiedenen Stellen auf das Gesamtsystem („verteiltes System“) wird damit vorhersehbar und sicher berücksichtigt. Wichtige Informationen über die Gebäudestruktur in Kombination mit universellen Sicherheitsrichtlinien dienen zudem als Grundlage für einen Partitionierungsalgorithmus, der Geräte in geschützten Netzwerkbereichen gruppiert. Innerhalb eines solchen Bereichs können die eigentlichen Anwendungen ausgeführt und Daten redundant gesichert gespeichert werden.

Schwerpunkt 1: Middleware für die Gebäudeautomation

Der erste Schwerpunkt basiert auf der Beschreibung von Geräten, Daten und Funktionen, sodass diese maschinell gesucht werden können. Grundvoraussetzung dafür sind ein einheitliches Modell und eine geeignete Abfragesprache, welche jedoch derzeit weder für GA- noch Smart Home-Geräte, deren Prozessdaten oder Funktionen existiert. Forschungsansätze, welche auf ein bestimmtes Ziel hin entwickelt wurden (z. B. Fehlerdetektion), zeigen vielversprechende Resultate, stellen aber individuelle Lösungen dar. Daher wurden Methoden entwickelt und evaluiert, um bestehende Modelle miteinander zu verknüpfen und somit die Grundlage für eine inhaltliche Datenvermittlung in der Praxis zu schaffen. Insbesondere fehlerhafte und inkompatible Teilmodelle müssen dabei berücksichtigt werden. Für die Abfrage und Vermittlung der Informationen wurde eine Schnittstelle implementiert, welche ausschließlich offene Internettechnologien mit dem Fokus auf eine lose Kopplung der Systemteilnehmer verwendet. Dabei ist die Integration in den Bestand eine zusätzliche Herausforderung, um eine zügige Etablierung dieser Technik zu ermöglichen. Zudem wurden die Beschreibungen mit Elementen aus Open-BIM-Modellen verknüpft, um etwa die Realisierung intelligenter Energiesparfunktionen zu ermöglichen. So können etwa die thermischen Eigenschaften von Wänden genutzt werden, um die Heizungssteuerung automatisch zu optimieren.

Die Motivation für die Arbeiten in Schwerpunkt 1 ist, Anwendungen für Gebäude so entwickeln zu können, dass diese ohne erheblichen Konfigurationsaufwand in verschiedenen Gebäuden genutzt werden können. Der Ansatz für unsere Arbeiten ist die Idee, statt installationsspezifischer Adressen (IP-Adressen, Bus-Adressen, usw.) abstrakte, domänenspezifische und maschinenlesbare Beschreibungen zu verwenden. Der Vorteil der abstrakteren Beschreibung liegt in der Wiederverwendbarkeit. So ist das Konzept einer Klimaanlage gebäudeübergreifend nutzbar. Hingegen ist eine konkrete Adresse nur in jeweils einer Installation gültig. Hinzu kommt, dass durch die Heterogenität von Protokollen im Umfeld der Gebäudeautomation die gleiche Funktionalität in einer Installation etwa mit KNX, in einer anderen Installation aber mit BACnet realisiert wurde. Eine Anwendung wird also auch durch die Protokollauswahl in ihrer Wiederverwendbarkeit eingeschränkt.

Um portable Anwendungen realisieren zu können, sind daher drei wesentliche Punkte von Bedeutung:

1. Es wird ein einheitliches Vokabular für die abstrakte Beschreibung benötigt.
2. Konkrete Adressen müssen anhand der Beschreibungen zur Laufzeit gefunden werden können.
3. Für die Anwendung ist der Zugriff auf die Informationen unabhängig vom Protokoll der Informationsquelle.

Einheitliches Vokabular für die abstrakte Beschreibung von GA-Komponenten

In der Praxis haben sich Ontologien als eine technische Lösung für einheitliche, maschinenlesbare Vokabularien etabliert. Diese bestehen aus Konzepten (etwa „Lichtaktor“, „Sensor“, „Raum“), welche einerseits in Hierarchien geordnet sind („Lichtaktor“ ist eine Spezialform von „Aktor“ und ein „dimmbarer Lichtaktor“ wiederum eine Spezialform des „Lichtaktors“) und andererseits über Relationen miteinander verknüpft sein können (etwa „Lichtaktor“ „befindet sich in“ „Raum“). Hinzu kommen Regeln, um mögliche Zusammenhänge zu fordern oder einzuschränken (etwa „jeder Raum hat mindestens eine Tür“). Zusammengenommen bilden diese das Vokabular. Beschreiben wir nun Dinge (im Folgenden “Entitäten” genannt) mit diesem Vokabular, spricht man von Instanzen (beispielsweise <BACnet Gerät:15 BinaryValue:3> ist eine Instanz des Konzeptes „Lichtaktor“). Für den Prozess, eine Entität als Instanz eines Konzeptes zu deklarieren und Relationen zwischen Instanzen zu definieren, benutzen wir im Folgenden den Begriff „annotieren“.

Wie im Antrag erwähnt existieren zahlreiche Ontologien für die Gebäudeautomation, das Smart-Home und das Internet der Dinge, welche im Rahmen der jeweiligen Projekte unabhängig von jeweils anderen entwickelt wurden. Daher ist ein Ziel des Projektes die Verknüpfung zwischen diesen Projekten. In Vorbereitung auf die mögliche Zusammenführung wurde im Berichtszeitraum untersucht, inwieweit bereits Verknüpfungen bestehen. Unter einer Vielzahl an Projekten wurden insbesondere die folgenden Ontologien genauer untersucht: IoT-Lite [1], SAREF [2], SAREF4BLD [3], SOSA & SSN [4], SEAS [5], BRICK [6], ThinkHome [7], IfcOWL [8], DogOnt [9], HTO (Haystack Tagging

Ontology) [10], Colibri [11], BOnSAI & CoDaMoS [12]. Hierbei wurde ermittelt, welche Ontologien auf den gleichen grundlegenden Ontologien und Schemata aufsetzen und inwiefern bereits Mappings zwischen Ontologien verschiedener Projekte existieren. Dazu wurden rekursiv die Abhängigkeiten der Modelle analysiert und auf Gemeinsamkeiten hin untersucht. Bislang zeichneten sich hier einige Gemeinsamkeiten in Randbereichen ab, etwa in der Modellierung von Zeit oder geographischen Positionen.

Abbildung 1 zeigt eine detaillierte Übersicht aller im Projektzeitraum untersuchten Ontologien inklusive deren farblicher Gruppierung in funktionale Themenfelder (siehe Legende: Einheiten & Zeit, Sensoren, GA & Smart Home, Gebäudeplanung). Neben den Ontologien sind zudem Formatstandards und Protokolle aufgeführt, die in einigen der Ontologien Berücksichtigung finden. Alle Elemente sind von oben nach unten nach ihrem Erscheinungsdatum aufsteigend sortiert. Die durchgezogenen Pfeile verdeutlichen, dass Ontologien aufeinander aufbauen oder Weiterführungen bzw. Erweiterungen voneinander darstellen. Die gestrichelten Linien geben wiederum an, dass sich Ontologien referenzieren, wobei einige wenige Ontologien auch eine Auswahl von anderen Ontologien verschiedener Bereiche verknüpfen.

Im Ergebnis wurde unsere Vermutung bestätigt, dass bislang nur wenige Ontologien aktiv mit anderen in Beziehung gesetzt werden (gestrichelte Verbindungen in Abbildung 1). Erst in derzeitig laufenden Arbeiten spielt diese projektübergreifende Verknüpfung eine stärkere Rolle. Insbesondere ist hierbei das Projekt Building Topology Ontology (BOT) [1] zu nennen, welches aktiv Verknüpfungen für Ontologien im Bereich Gebäudeautomation und Smart Home anbietet. Hinzu kommt das neu bekannt gewordene Projekt RealEstateCore [2], welches eine Ontologie für Gebäudeeigner, -betreiber und -nutzer entworfen hat und versucht, diese mit existierenden Ontologien zu verknüpfen. Die Ergebnisse beider Projekte bieten einen Ausgangspunkt, um initiale Verknüpfungen zu extrahieren bzw. diese miteinander zu vergleichen.

Insbesondere mangelt es jedoch weiterhin an einer Verknüpfung von Modellen des Bauwesens und der Gebäudeplanung (BIM/IFC bzw. deren Ontologie-Darstellung IfcOWL) mit Daten- und Domänenmodellen der Gebäudeautomation & Smart Home (wie z. B. ThinkHome, BRICK, DogOnt etc.) sowie einer geeigneten Zuordnung von technologie- und gerätespezifischen Informationen (u. a. Adressinformationen der konkreten GA-Protokolle) der individuellen GA-Endgeräte im laufenden Gebäudebetrieb. Die im Rahmen von Schwerpunkt 1 des Projektes entwickelte Middleware-Architektur widmet sich dieser Problemstellung, indem sie BIM/IFC- und GA-Ontologie-Informationen innerhalb einer Zwischenschicht miteinander verbindet und die Übersetzung zwischen abstrahierter Anwendungsebene und spezifischer GA-Technologie an Gateway-Komponenten delegiert. Technologiespezifische Informationen können hierbei als Selbstbeschreibung direkt durch Geräte bzw. deren Gateways geliefert werden und lassen sich mit der Ontologie-Wissensbasis der Middleware in Beziehung setzen. Die entwickelte Lösung wird im Abschnitt „Finden von konkreten Instanzen auf Basis von abstrakten Beschreibungen und Informationszugriff“ im Detail beschrieben.

Um neben der Verwendung existierender Ontologie-Verknüpfungen auch neue finden zu können, wurde im Projektzeitraum eine Evaluierung verschiedener Werkzeuge durchgeführt, die sich für diese Aufgabe eignen könnten. Es wurden verschiedene Open-Source-Werkzeuge betrachtet, wobei sich die Software-Projekte OpenII Harmony [3] und AgreementMaker [4] als vergleichsweise vielversprechende Kandidaten herausstellten.

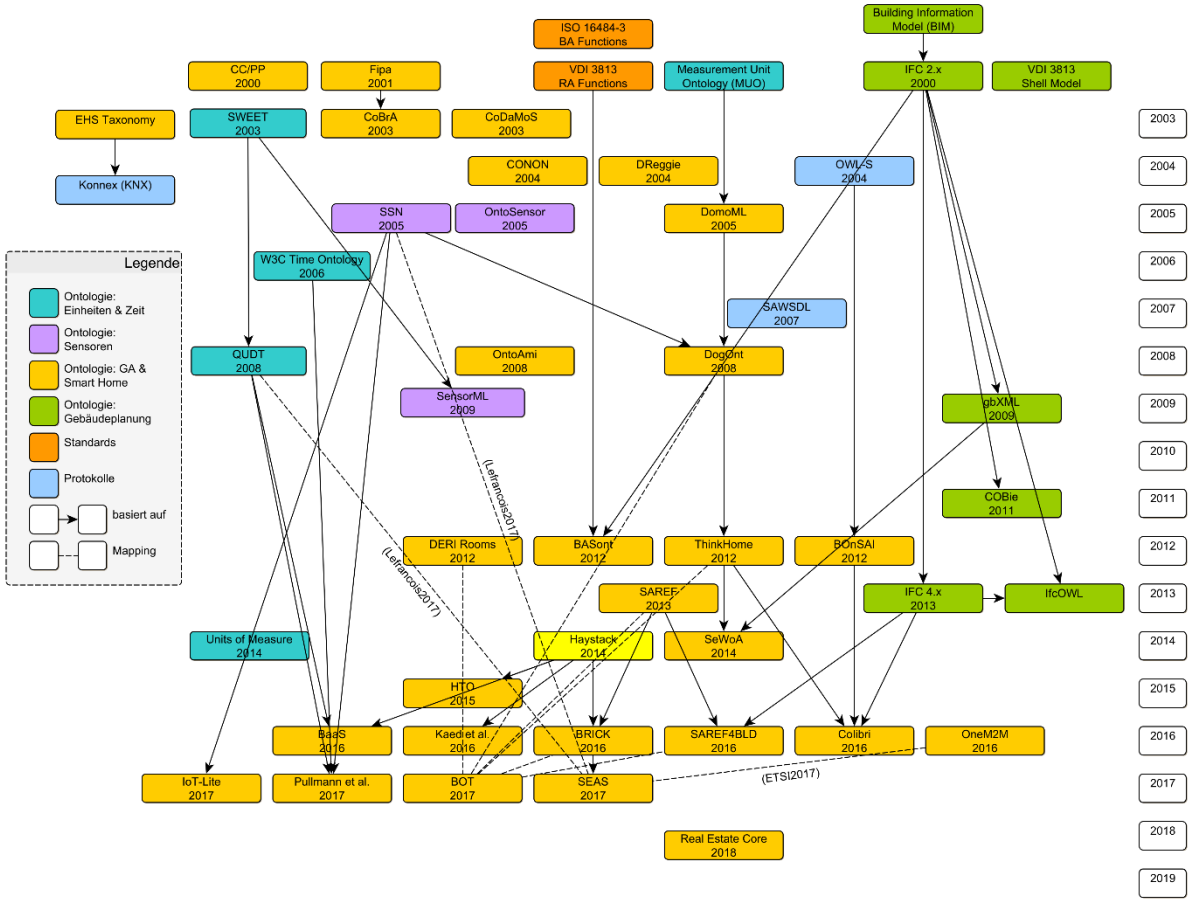
1 https://w3c-lbd-cg.github.io/bot/

2 http://www.realestatecore.io

3 http://openii.sourceforge.net/

4 https://github.com/agreementmaker/agreementmaker

Abbildung 1: Übersicht bestehender Ontologien und deren Abhängigkeiten



Quelle: IMD, Universität Rostock

Die Methoden der Werkzeuge unterscheiden sich teilweise stark. Im Allgemeinen können aber drei Grundformen identifiziert werden, welche zum Teil kombiniert werden: manuelle Verknüpfung, Verknüpfung auf linguistischer Basis und Verknüpfung auf Basis der Graphstruktur. Keiner der beiden letzten Ansätze bietet eine vollständig automatisierte Lösung. Der linguistische Ansatz basiert dabei auf Ähnlichkeiten von Konzeptnamen, etwa einem gleichen Wortstamm oder Synonymen. Da Konzepte mit gleichem Namen jedoch nicht zwangsläufig exakt das Gleiche bedeuten oder Konzepte mit gleicher Bedeutung nicht notwendigerweise eine identische Bezeichnung haben, kann diese Methode nur Vorschläge für eine Verknüpfung bieten. Der graphbasierte Ansatz nutzt hingegen Relationen zwischen Konzepten und vergleicht diese mit den Strukturen in anderen Ontologien. Auch hier ist es möglich, dass gleiche Strukturen vorkommen, ohne dass diese zwangläufig die gleiche Bedeutung haben. Letztendlich bleibt nur ein manuelles Verfahren, welches durch die anderen Verfahren unterstützt werden kann (Vorschlagsfunktion). Von den untersuchten Werkzeugen hat keines vollständig überzeugen können, da diese teilweise nicht verfügbar sind bzw. die Skripte zum Bauen der Applikationen nicht funktionieren, das Ausgabeformat proprietär ist, die Bedienung sehr unhandlich ist oder die erzielten Ergebnisse nicht überzeugen. Hinzu kommt, dass diese Werkzeuge ausschließlich auf das Verknüpfen von zwei Ontologien ausgelegt sind und nicht auf die Verknüpfung einer größeren Anzahl an Ontologien gleichzeitig.

Perspektivisch ist mit den derzeitigen Entwicklungen im Bereich des maschinellen Lernens denkbar, auch die textuellen Beschreibungen in Ontologien für eine Vorschlagsfunktion heranzuziehen. Da dieser Ansatz Textverständnis erfordert, ist die Umsetzung und insbesondere das Training einer solchen künstlichen Intelligenz in unserem Rahmen aber nicht leistbar.

Finden von konkreten Instanzen auf Basis von abstrakten Beschreibungen und Informationszugriff

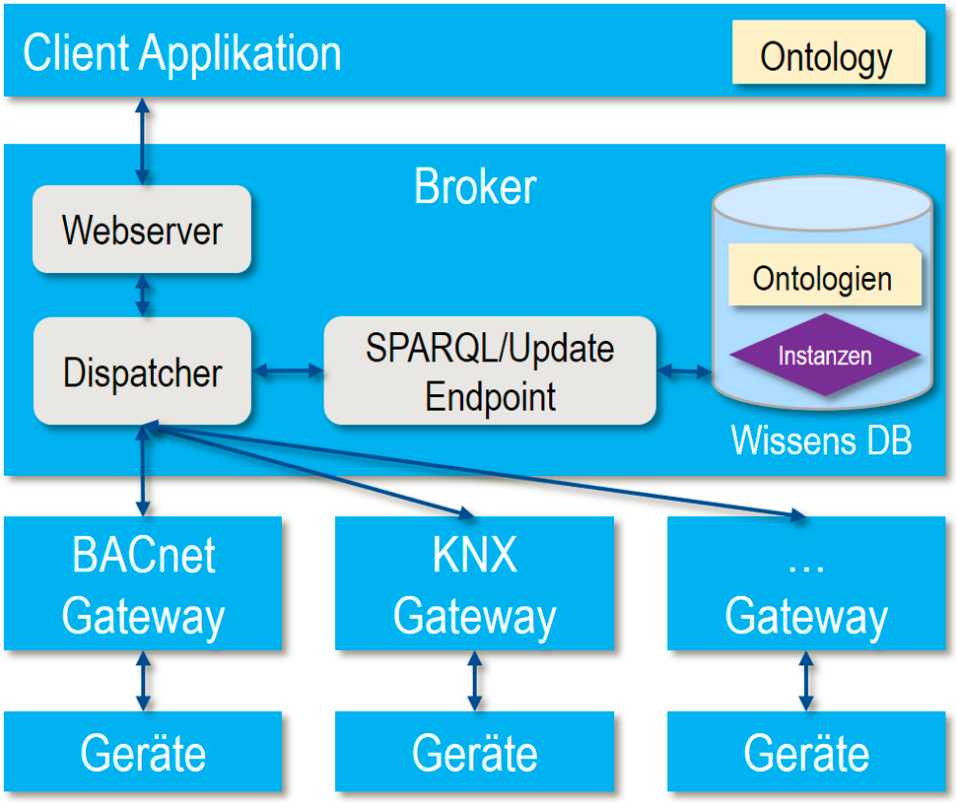
Um über die Beschreibungen die konkreten Instanzen in einem Gebäude finden zu können, wurde im Berichtszeitraum die Grundarchitektur einer Middleware für semantische Interoperabilität in GA-Netzwerken, dargestellt in Abbildung 2, im Detail entwickelt und prototypisch implementiert. Dabei konnte in ersten Versuchen gezeigt werden, dass der Ansatz funktioniert und in der Lage ist, Daten gleichzeitig über Ontologien verschiedener Projekte zu annotieren. Um dies zu erreichen, wurde explizit ein Ansatz gewählt, der nicht, wie in anderen Projekten, ein festes einheitliches Datenschema vorgibt und die Daten aller Technologien in dieses Schema presst. Stattdessen wurde für jede Technologie ein eigenes Schema entworfen, das alle adressierbaren Daten als eine annotierbare Entität darstellt. Auf diese Weise gehen keine Informationen verloren. Weiterhin können technologieinhärente Beziehungen zwischen Daten (etwa des Wertes und der zugehörigen Einheit) einfacher und zum großen Teil automatisiert abgebildet werden. Derzeit wurden prototypische Schemata für KNX, BACnet, DPWS, EnOcean, LONTalk, MQTT, CoAP, oBIX, OPC-UA, ZigBee und zWave entwickelt. In einem weiteren, zurzeit noch manuellen Prozess werden diese Entitäten mit Klassen und Relationen aus externen Ontologien (bislang unter Nutzung der Ontologie DogOnt, siehe Abbildung 1) annotiert und insbesondere auch im BIM-Modell verortet.

Da jede annotierbare Entität beliebig oft und mit Konzepten und Relationen diverser Ontologien annotiert werden kann, bietet sich die Möglichkeit, die gleichen Daten simultan aus verschiedenen Perspektiven zu betrachten. So kann etwa ein und dieselbe Entität einerseits als Lichtaktor annotiert und somit für die Lichtsteuerung verwendet werden und andererseits auch als elektrischer Verbraucher mit einer aktuellen Last, etwa für die Verbrauchserfassung.

Um mithilfe dieser Beschreibungen konkrete Instanzen zu finden, nutzen wir SPARQL (**S**PARQL **P**rotocol **A**nd **R**DF **Q**uery **L**anguage). Es erlaubt uns, etwa nach Instanzen bestimmter Konzepte zu suchen oder Relationen zwischen Instanzen auszuwerten. Jede Instanz ist mit einer HTTP-Adresse verknüpft, welche der Broker/Dispatcher nutzen kann, um über Gateways die Daten abzurufen. Somit können Anwendungen Daten finden, ohne installationsspezifisches Wissen zu benötigen, und diese Daten auch unabhängig vom Protokoll des liefernden Gerätes lesen und (mit Einschränkungen) schreiben.

Aus Sicht der Anwendungen wird ausschließlich HTTP als Kommunikationsprotokoll genutzt. Hinzu kommt die Verwendung von RDF (**R**esource **D**escription **F**ramework) zur Wissensrepräsentation (Ontologien und Instanzen), der Abfragesprache SPARQL, um Daten zu finden und abzufragen, und JSON als Austauschformat. Die Anwendung muss keine spezifischen Gebäudeautomationsprotokolle beherrschen oder zwischen Geräten unterschiedlicher Protokolle unterscheiden können. Dennoch kann bei Bedarf die Applikation erfahren, welche Technologie eingesetzt wird und (eine passende Netzwerkverbindung zum Gerät vorausgesetzt) theoretisch auch über das native Protokoll mit den Geräten kommunizieren.

Abbildung 2: Middleware-Architektur für GA-Netzwerke



Quelle: IMD, Universität Rostock

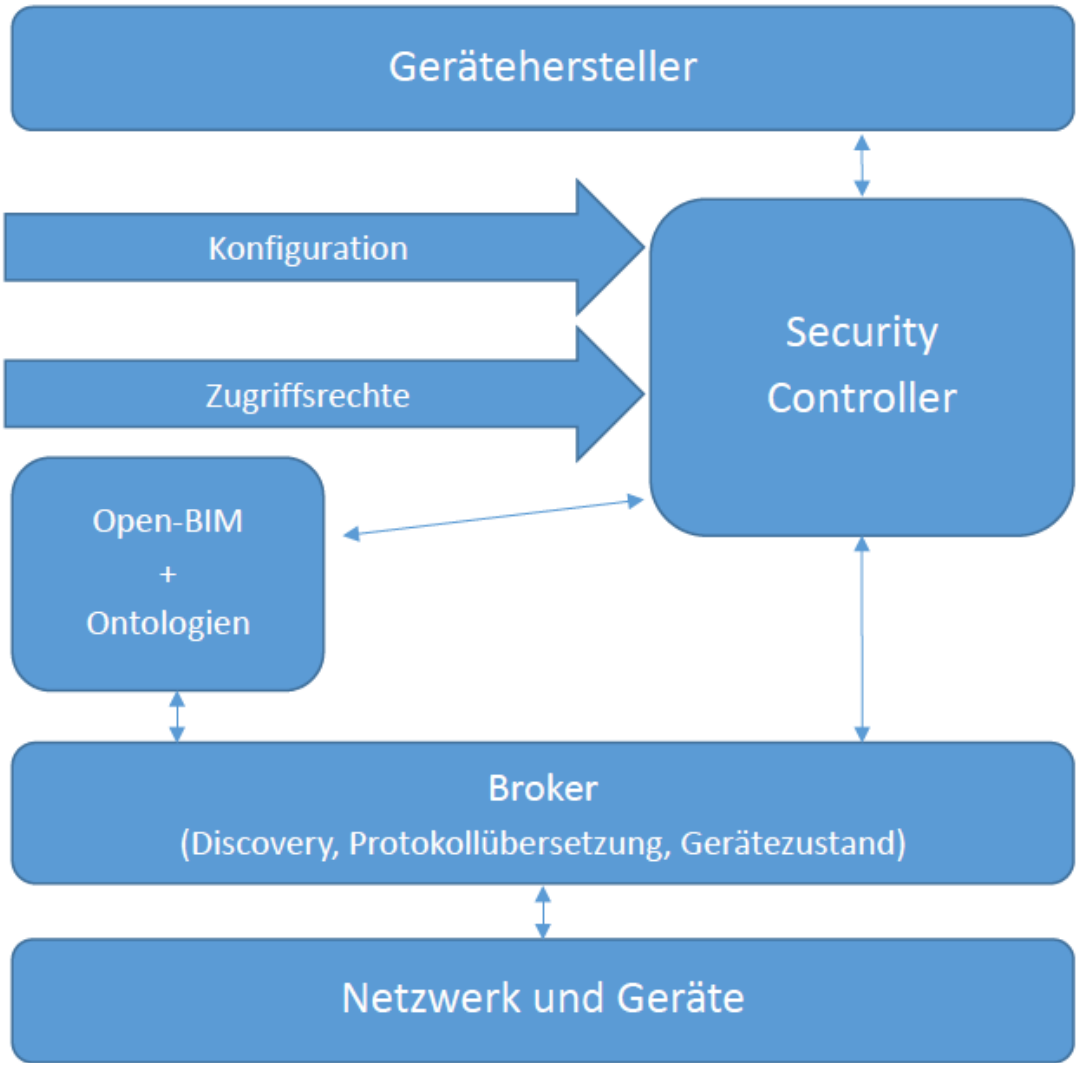
Auf Seiten der Feldgeräte ist in unserem Ansatz keinerlei Modifikation notwendig. Dadurch können Bestandsgeräte problemlos integriert werden. In einigen Fällen, wie etwa BACnet, können die meisten Informationen vom Gateway dynamisch zur Laufzeit erfasst werden. Hinzu kommt in BACnet etwa das StructuredView-Objekt, welches bereits Annotationen nach dem Haystack-Schema enthalten kann. Bei anderen Technologien, wie etwa KNX, sind wir in einem Stadium, in dem die annotierbaren Elemente nicht allein aus Laufzeitdaten generiert werden können. Stattdessen wurde die Idee entwickelt, hierfür auf Planungsdaten zurückzugreifen, welche etwa vom Planungs- und Konfigurationstool ETS (De-Facto-Standard für KNX) generiert werden. In beiden genannten Fällen ist für die Umformung also kein zusätzlicher manueller Aufwand erforderlich. Beide Technologien stehen stellvertretend für weitere Protokolle. So können auch in DPWS, oBIX oder CoAP dynamisch Daten zur Laufzeit erfasst werden. EnOcean, ZigBee und zWave hingegen setzen wie KNX auf vordefinierte Geräteprofile. Entsprechend gehen wir derzeit von einer Übertragbarkeit der Ergebnisse aus.

Zusammengefasst sind somit die drei wesentlichen Anforderungen für portable Anwendungen durch unsere Plattform adressiert. Daten können annotiert, gefunden und abgefragt werden. Für die Zusammenführung existierender Ontologien wurden wichtige Vorarbeiten geleistet. Unsere Plattform stellt die Grundlage für die Arbeit von Schwerpunkt 2 dar.

Schwerpunkt 2: Sicherheitsarchitektur für die Gebäudeautomation

Im zweiten Schwerpunkt wurde eine Sicherheitsarchitektur für Gebäudeautomationssysteme unter Verwendung des Open-BIM-Ansatzes ausgearbeitet, die in Abbildung 3 dargestellt ist. Ein zentraler Security Controller, der auf zertifizierter Hardware beruht, kommuniziert über die im Schwerpunkt 1 entwickelte Middleware (Broker) mit den Geräten und der Netzwerkinfrastruktur. Damit die Kommunikation vereinheitlicht und portabel gestaltet werden kann, wird die Ontologie um ein Vokabular für Security- und Netzwerkkonfigurationen erweitert. Durch die Annotation von Geräten an das BIM kann deren örtliche Verteilung im Gebäude beschrieben werden. Der Security Controller erhält durch das globale Netzwerkwissen die Fähigkeit, Security-Konfigurationen zu generieren und das Netzwerk samt Endgeräten abzusichern. Weiterhin sieht die erarbeitete Sicherheitsarchitektur eine Schnittstelle für Gerätehersteller vor, um ein Updatemanagement der Firmware zu realisieren.

Abbildung 3: Sicherheitsarchitektur aus Schwerpunkt 2



Quelle: IMD, Universität Rostock

Auf Basis der entwickelten Sicherheitsarchitektur aus Abbildung 3 wurden die einzelnen Phasen der Gerätekommissionierung, Konfiguration und Wartung definiert und verfeinert. Neben der Ausarbeitung von Ablaufplänen und Protokollen wurden zudem erste Skalierbarkeitsuntersuchungen für eine modell- und richtlinienbasierte Bildung sogenannter „Trust Zones“ durchgeführt. Durch diese lassen sich Geräte unabhängiger GA-Anwendungen im Zuge ihrer Kommissionierung in separaten Teilnetzen isolieren und somit die Angriffsfläche für Sicherheitsbedrohungen reduzieren.

Ein weiterer Fokus im zweiten Schwerpunkt lag auf der Konfigurierbarkeit von Geräten und Funktionen durch den Nutzer. Dabei wurde berücksichtigt, dass die individuelle, sichere Konfiguration einzelner Geräte im Gesamtsystem dennoch zu einem Fehlverhalten führen kann, welches sich z. B. von Hackern ausnutzen lässt. Die Problemstellung bestand folglich auch aus einer geeigneten Zusammenführung und Analyse der Konfiguration des Gesamtsystems zur Erkennung und Vermeidung von Konfigurationskonflikten. Weiterhin wurden dezentrale Konzepte zur Vermeidung eines zentralen Ausfallpunktes (Single Point of Failure) sowie zur sicheren Protokollierung von Vorgängen, wie z. B. Konfigurationsaktivitäten oder Hacker-Attacken, erarbeitet. Dazu wurden verschiedene Lösungsansätze betrachtet, wie etwa Blockchains und P2P-basierte Speicherungsprotokolle.

Die Grundlage der Entwicklung der Sicherheitsarchitektur bildete eine umfangreiche Literatur-recherche und -analyse bezüglich der Sicherheitsanforderungen und Bedrohungen. Die Ergebnisse der Untersuchungen und das vorgestellte Konzept wurden auf der IEEE Global Conference on Internet of Things (GCIoT) 2019 in Dubai vorgestellt und stehen im Online-Katalog des IEEE zur Verfügung [13].

Die Forschungsinhalte aus Schwerpunkt 2 sind in die Dissertation mit dem Titel “Modellbasierte, sichere Service- und Netzwerkkonfiguration in der Gebäudeautomation” [14] eingeflossen. Die nachfolgenden Abschnitte sind der Dissertation entnommen. Zunächst folgt eine Beschreibung des grundlegenden Lösungsansatzes. Anschließend werden die einzelnen Phasen zur sicheren Kommissionierung und Konfiguration des GA-Netzwerks in Detail erläutert. Nachfolgend werden weitere Aspekte des Konzepts zur Gerätekonfiguration und verteilten Protokollierung von Log-Daten diskutiert. Abschließend werden die sich ergebenden Sicherheitsvorteile der Architektur aus Schwerpunkt 2 noch einmal zusammengefasst.

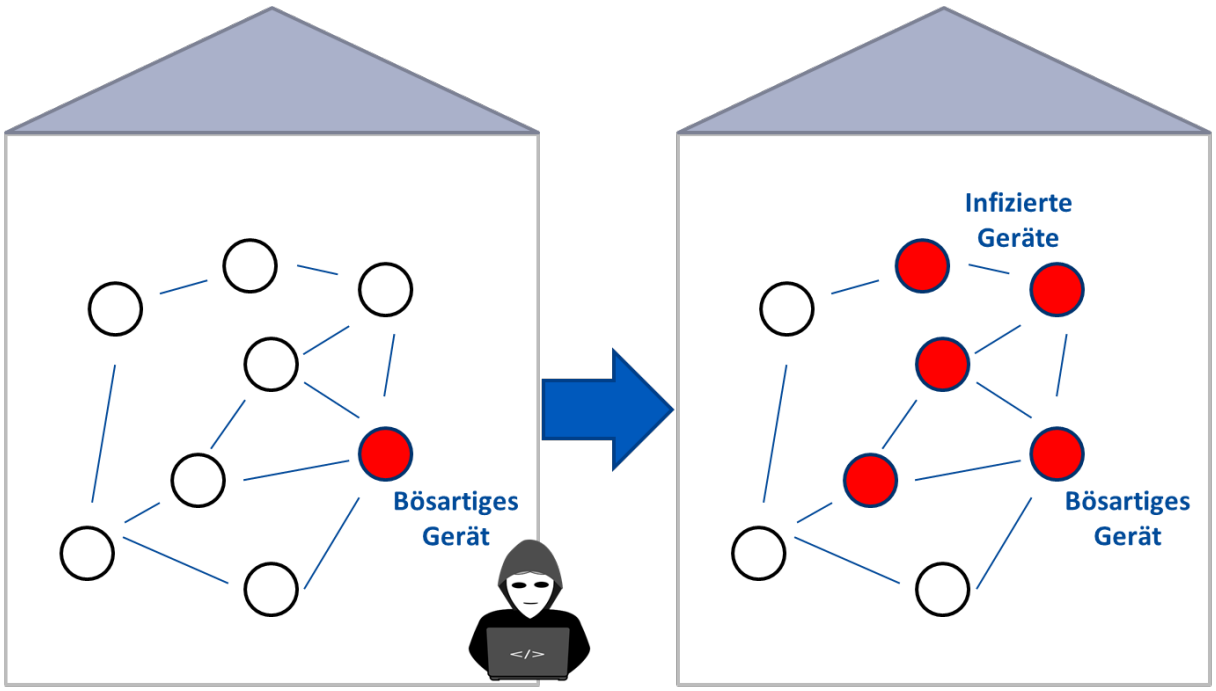
Security-Bedrohungen und grundlegender Lösungsansatz

In den letzten Jahren ist der Grad der Vernetzung zwischen smarten Geräten rasant gestiegen. Während traditionelle GA-Systeme auf Steuergeräten basieren, die über einen Feldbus Sensordaten auswerten und Aktorik steuern, basieren moderne Ansätze auf Webtechnologien. Dabei bieten eingebettete Systeme (Sensorik, Aktorik und Steuergeräte) ihre Funktionalitäten in Form von Webservices an. Durch die Anbindung an ein paketvermitteltes Netzwerk (IPv4 bzw. IPv6) können die Geräte miteinander kommunizieren und Anwendungen realisieren. Zu den Anwendungen gehören bspw. Regelkreise der Klimatechnik oder die Verknüpfung von Bedienpanelen oder Wandschaltern mit der Beleuchtung.

Der moderne Ansatz, Geräte über lokale IP-basierte Netzwerke und Webtechnologien miteinander zu verbinden, birgt jedoch die Gefahr von Hackerangriffen. Durch die gestiegene Anzahl an vernetzten Geräten innerhalb eines GA-Systems steigt die Wahrscheinlichkeit, dass mindestens ein Gerät durch einen Angreifer kompromittiert wurde, um weitere Angriffe innerhalb des Netzwerks zu starten. Dabei haben es Angreifer in der Regel auf das Abgreifen sensibler Daten bzw. das Steuern von Aktorik abgesehen. Außerdem muss in den nächsten Jahren von einer erhöhten Bedrohung durch sogenannte Ransomware ausgegangen werden. Ransomware zielt darauf ab, persönliche/wichtige Daten durch Verschlüsselung temporär unbrauchbar zu machen. Erst nach Zahlung eines Lösegelds werden die Daten wieder freigegeben. Ransomware, die darauf abzielt, Funktionalitäten von eingebetteten Systemen einzuschränken, ist für Angreifer ebenfalls ein attraktives Ziel. Der verursachte wirtschaftliche Schaden wäre im Falle einer Sabotage groß. Die Hürde, einen Angriff erfolgreich durchzuführen, sinkt, da sich immer mehr Geräte, die zum Teil nicht mit Firmware-Updates versorgt werden, in einem Gebäude befinden.

Hinzu kommt das Problem, dass sich manche Geräte in öffentlich zugänglichen Gebäudeteilen befinden. Ein Angreifer hätte die Möglichkeit, durch physischen Zugang zu Geräten selbige durch Anwenden eines Exploits[5] zu übernehmen und schädlichen Code auszuführen. Steht nach erfolgreicher Anwendung eines Exploits ein Gerät unter der Kontrolle des Angreifers, so kann es missbraucht werden, um weitere Geräte im Gebäude zu infizieren (siehe Abbildung 4).

Abbildung 4: Ausweitung eines Angriffs auf weitere verwundbare Geräte

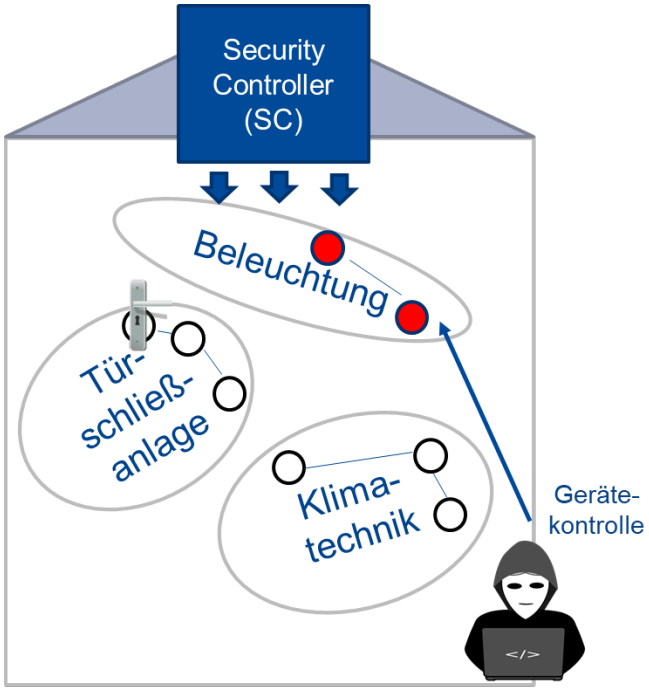


Quelle: IMD, Universität Rostock

Das in Scherpunkt 2 entwickelte Lösungskonzept setzt an dieser Stelle an. Durch die Abschottung von Geräten, die nicht miteinander kommunizieren müssen, da sie z. B. unterschiedlichen Anwendungsdomänen zugeordnet sind, lässt sich die Ausweitung eines Angriffs eindämmen (siehe Abbildung 5. Das Konzept zur Kommissionierung des GA-Netzwerks beinhaltet daher einen Schritt zur Einteilung der Geräte in sogenannte „Trust Zones“. Diese netzwerktechnische Abschottung in isolierte Teilnetze findet auf der MAC-Ebene des ISO/OSI-Referenzmodells statt. Die grundlegende Eignung des Ansatzes zur Erhöhung der Sicherheit konnte in unseren Publikationen [15], [16] bereits unter Beweis gestellt werden. Der Algorithmus zur Trust-Zone-Bildung wird von einem vertrauenswürdigen Gerät ausgeführt, dem sogenannten Security Controller (SC), wie er in der Übersicht der Sicherheitsarchitektur in Abbildung 3 oberhalb der Middleware dargestellt ist. Mathematisch betrachtet handelt es sich um einen Entscheidungsalgorithmus, da jedes Gerät basierend auf Geräteattributen einer oder mehreren Trust Zones zugeordnet werden kann. Im Projekt wurde untersucht, inwiefern sich der Installationsstandort, die Firmware-Version und die Anwendungs-Zugehörigkeit von Geräten als Attribute für einen Partitionierungsalgorithmus verwenden lassen. Umsetzung und Evaluation des Algorithmus werden im Abschnitt „*Policy-basierte Bildung von Trust Zones*“ im Detail erläutert.

[5] Ein Exploit beschreibt inhaltlich den Vorgang, eine Schwachstelle eines Gerätes auszunutzen, um technische Schutzmaßnahmen zu umgehen. Der Angreifer kann durch erfolgreiches Anwenden eines Exploits beispielsweise eigenen Code ausführen, die Nutzer-Authentifikation umgehen, Administratorprivilegien erlangen (engl.: Privilege Escalation) oder sensible/vertrauliche Daten auslesen. Eine besondere Form des Exploits ist der sogenannte „Zero-day Exploit“. Gegen ihn existiert kein Gegenmittel in Form eines Updates (Firmware-Update, Mikrocode-Update, Hardwaremodifikation). Nachdem die Existenz eines Zero-day Exploits bekannt wurde, muss der Gerätehersteller ein passendes Update an das betroffene Gerät ausliefern, um die vom Exploit ausgenutzte Schwachstelle zu beheben.

Abbildung 5: Angriff auf einzelne Trust Zone beschränkt



Quelle: IMD, Universität Rostock

Auf Basis der zuvor in Abbildung 3 dargestellten grundlegenden Sicherheitsarchitektur wurde ein Konzept zur Kommissionierung und Konfiguration von GA-Netzwerken durch den Security Controller (SC) erarbeitet. Zur Übersicht werden die einzelnen Phasen des Sicherheitskonzeptes in **Fehler! Verweisquelle konnte nicht gefunden werden.** kurz erläutert. Anschließend werden die Phasen 1—5 im Detail diskutiert.

Tabelle 1: Übersicht der Phasen des Konzeptes zur Kommissionierung und Konfiguration von GA-Netzwerk und -Geräten

Phase	Ablauf und Bedeutung
1) Kommissionierung von Endgeräten	Während der Kommissionierungsphase wird jedes Endgerät durch einen Techniker zunächst mit einem Konfigurationsnetz verbunden. Zusätzlich zu den über einen separaten Kanal (out-of-band) übertragenen Zugangsdaten erhält jedes Gerät vom SC ein Schlüsselpaar (öffentlicher und privater Schlüssel). Durch die so entstandene Public-Key-Infrastruktur ist es während der Konfiguration und des Betriebs des GA-Systems möglich, Nachrichtenauthentizität und -integrität zu gewährleisten. Der SC speichert jedes Gerät in einer lokalen, geschützten Datenbank. Neben dem öffentlichen Schlüssel werden der Installationsort und der Gerätetyp durch einen Techniker eingetragen bzw. verifiziert. Diese im SC gespeicherten Daten werden als Ground Truth bezeichnet. Auf Basis dieser gesicherten Informationen ist es möglich, automatisiert Anwendungen und das Netzwerk zu planen.

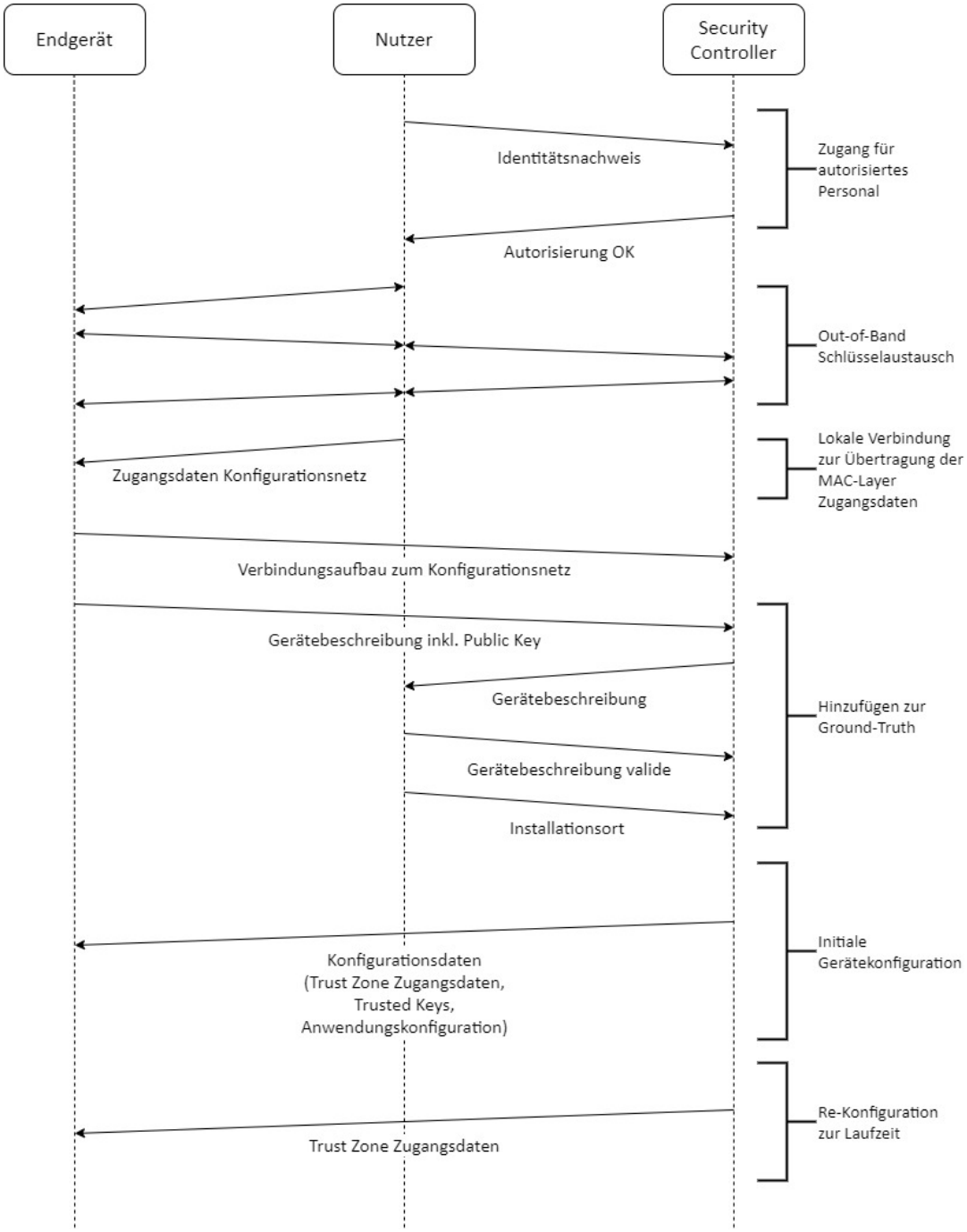
Phase	Ablauf und Bedeutung
2) Sammlung von Informationen der Netzwerkebene	Nachdem alle Geräte installiert und zur Ground-Truth-Datenbank hinzugefügt wurden, sammelt der SC globales Wissen zur Netzwerktopologie. Dazu gehören Informationen zur Geräte-Konnektivität via Ethernet und/oder Mesh-WLAN. Der SC erhält Ortsinformationen zu Ethernet-Leitungen und angeschlossenen Ethernet Switches. Weiterhin ruft der SC die Link-Liste und Routing-Tabelle jedes WLAN-Mesh-Gerätes ab, um einen Netzwerkgraphen zu erstellen.
3) Erstellung und Verifikation der Anwendungsebene	Um die Sensoren und Aktoren einer GA zu verknüpfen, werden IFTTT-Regeln („if-this-then-that“) erstellt. Jede Regel wird als gerichteter, azyklischer Anwendungsgraph modelliert. Logische Fehler innerhalb einzelner Regeln und zwischen verschiedenen Regeln werden durch formale Verifikation ausgeschlossen.
4) Abbildung der Anwendungen auf Geräte	Nachdem die Korrektheit der Regeln gewährleistet ist, werden die Knoten der korrespondierenden Anwendungsgraphen auf reale Geräte der Ground-Truth-Datenbank abgebildet. Alle Geräte eines Anwendungsgraphen werden zu einer Trust Zone (isoliertes Teilnetz) hinzugefügt.
5) Policy-basierte Bildung von Trust Zones	Sollten die Geräte eines Anwendungsgraphen keine netzwerktechnische Konnektivität aufweisen, müssen die fehlenden Kanten des Graphen durch weitere Netzwerkinfrastruktur realisiert werden. Ein Algorithmus fügt WLAN-Mesh-Geräte als verbindende Infrastrukturknoten einer Trust Zone hinzu. Dabei werden der Installationsort (Verknüpfung mit BIM) und eine allgemeingültige Sicherheitsrichtlinie (Policy) berücksichtigt.

Kommissionierung von Endgeräten

Während der ersten Phase werden die Endgeräte mit einem allgemeinen Konfigurationsnetzwerk verbunden. Dabei vermittelt ein legitimierter Nutzer per Smartphone zwischen dem Endgerät und dem Security Controller (SC), um eine Public-Key-Infrastruktur (PKI) zu errichten, Geräte-Metadaten auszutauschen und den Gerätestandort festzulegen.

Der Ablauf der Kommunikation zwischen Endgerät, Nutzer und SC ist in Abbildung 6 als Sequenzdiagramm dargestellt und wird in den nachfolgenden Abschnitten erläutert. Die vom SC ausgeführte Programmlogik zur Kommissionierung von Geräten verschiedener Netzwerktypen (Ethernet, WLAN) ist in Abbildung 9 durch einen Programmablaufplan dargestellt.

Abbildung 6: Ablauf der Kommissionierung eines Gerätes durch eine/n Nutzer/in (z. B. Techniker/in)



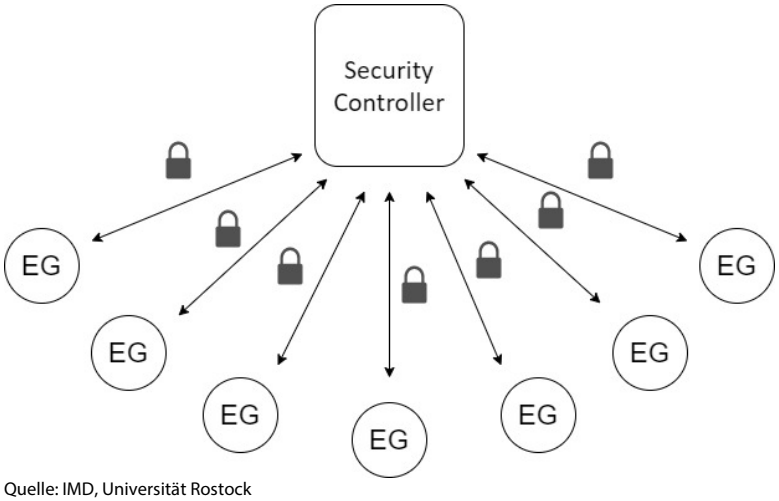
Quelle: IMD, Universität Rostock

Folgende Annahmen werden getroffen:

1. Der SC verfügt über eine Liste mit Nutzern samt ihren Zugangsdaten. Diese Nutzer sind autorisiert, Endgeräte zu kommissionieren.
2. Das Smartphone und der SC verfügen über Schlüsselmaterial, um eine geschützte Verbindung miteinander aufzubauen.
3. Es wird ein sicheres Authentifizierungsverfahren verwendet, um den Nutzer zu identifizieren und den Kommissionierungsprozess zu starten.
4. Das Smartphone zur Mensch-Maschine-Interaktion wird als vertrauenswürdig und sicher angenommen. Die auf dem Smartphone ausgeführte Software implementiert die in [17] vorgeschlagenen Mechanismen sowie die in diesem Projekt entwickelten Konzepte korrekt.
5. Die Erzeugung von Schlüsselpaaren (privater und öffentlicher Schlüssel) durch den SC kann nicht von Angreifern manipuliert werden.
6. Private Schlüssel werden sicher auf Endgeräten gespeichert.
7. Es werden sichere asymmetrische Verschlüsselungsverfahren eingesetzt.
8. Das eingesetzte Verfahren zur Aushandlung von Shared Keys zwischen zwei Geräten auf Basis der PKI ist sicher und korrekt implementiert.

Der SC verfügt über eine Liste mit Nutzern, die autorisiert sind, neue Geräte hinzuzufügen. Um Geräte hinzufügen zu können, meldet sich der Nutzer per Smartphone am SC an. Nach erfolgreichem Login-Vorgang wird Schlüsselmaterial zwischen Endgerät und SC ausgehandelt. Das technische Problem besteht darin, dass ein Gerät dieses Schlüsselmaterial bzw. Daten für eine Schlüsselaushandlung über einen gesicherten Übertragungsweg erhalten muss. Dieser ist jedoch zu Beginn der Kommissionierung noch nicht vorhanden. Da es sich bei den Endgeräten der GA um eingebettete Systeme mit limitierten Ein- und Ausgabemöglichkeiten handelt, können Schlüssel oder Shared Secrets nicht oder nur umständlich vom Nutzer gesetzt werden. Im Falle eines Gerätes mit nur einem Taster (Lichtschalter oder Sensor) müsste ein menschlicher Bediener einen 256-bit langen AES-Schlüssel (bzw. ein 256-bit langes Pre-shared Secret) „out-of-band" per Drücken des Tasters eingeben. Eine benutzerfreundliche Codierung ist nicht möglich. Als Verfahren zur sicheren Schlüsselaushandlung (symmetrischer Schlüssel) wird auf das in [17] beschriebene Verfahren zurückgegriffen, das auf einem authentifiziertem Diffie-Hellman-Schlüsselaustausch nach [18] beruht. Abbildung 7 zeigt schematisch die sternförmige Vertrauensbeziehung zwischen dem Security Controller und den Endgeräten.

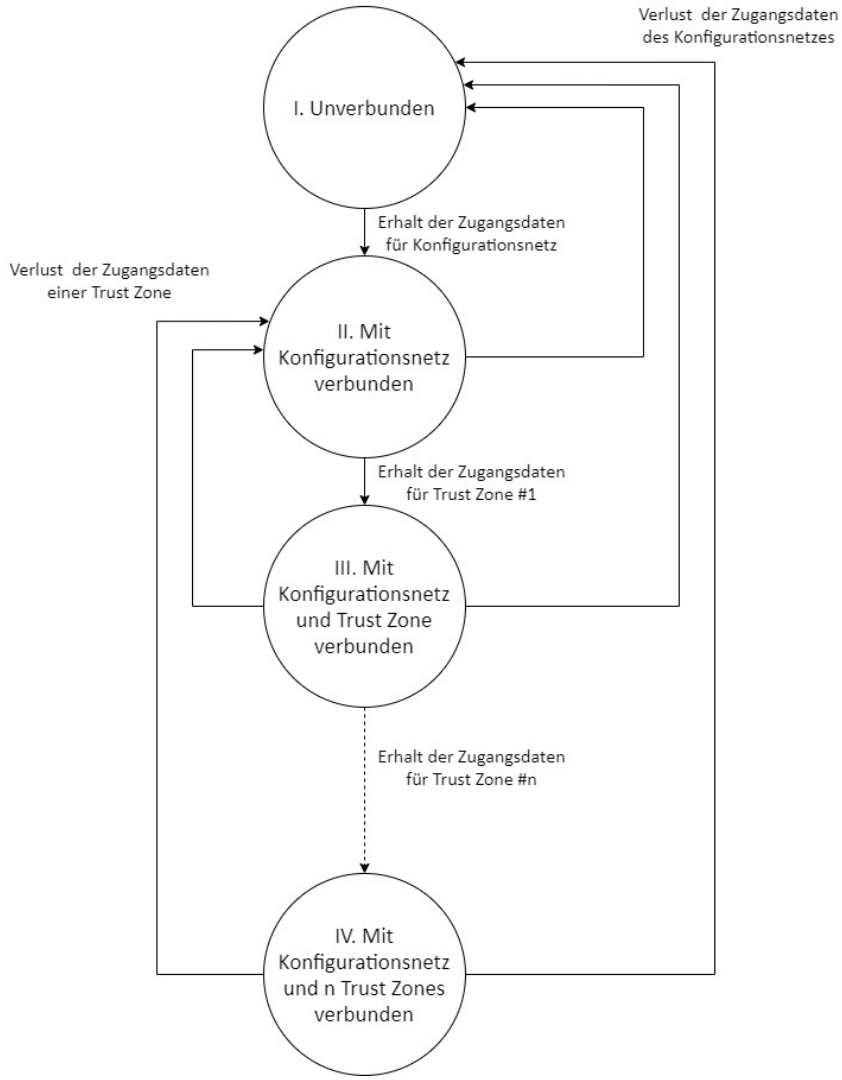
Abbildung 7: Ende-zu-Ende Sicherheit im Konfigurationsnetz zwischen Security Controller und Endgeräten



Quelle: IMD, Universität Rostock

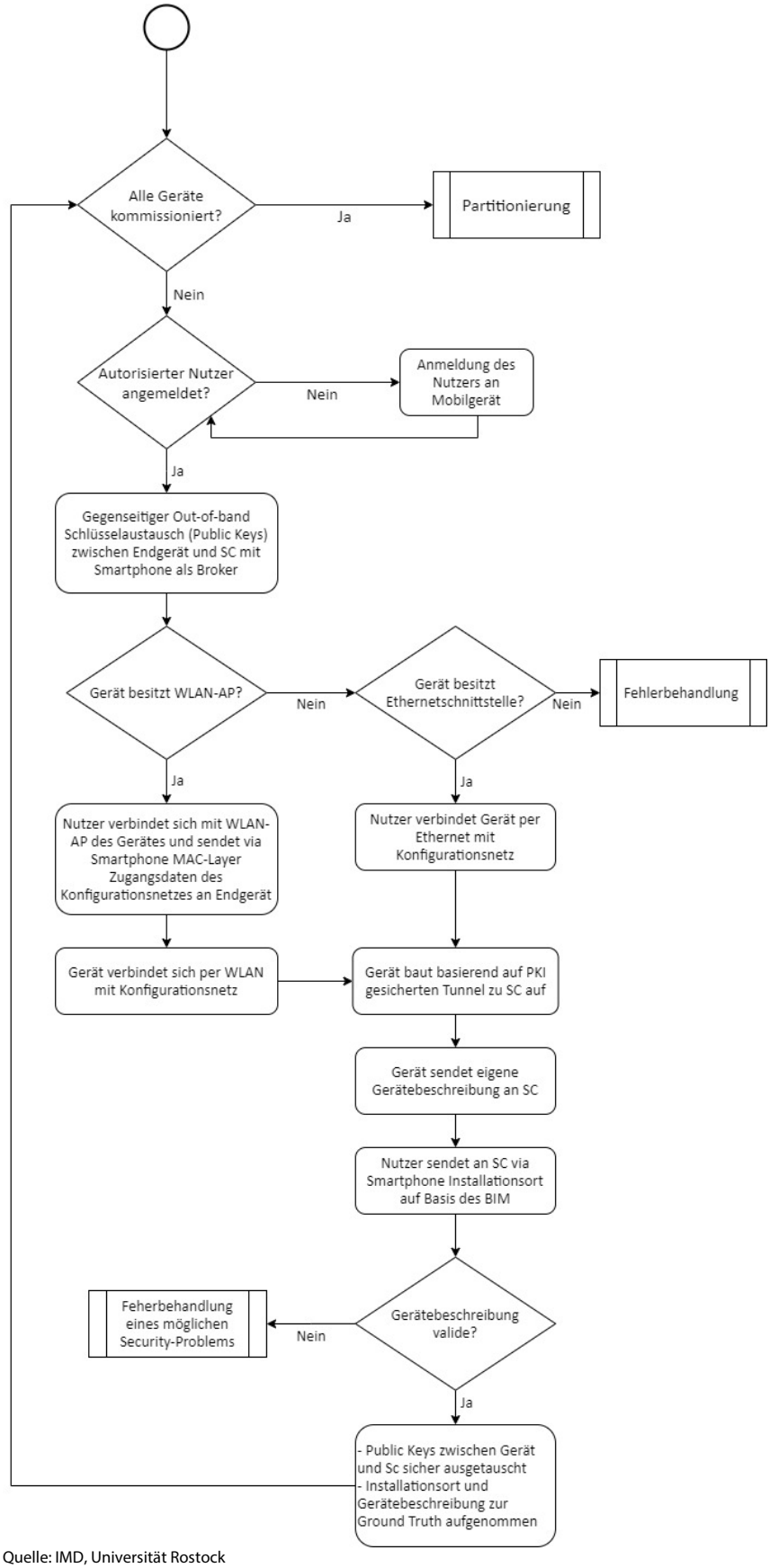
Abbildung 8 zeigt das Verhalten eines Endgerätes beim Netzwerkbeitritt (Beitritt in Konfigurationsnetz und Trust Zone(s)) in Form eines Zustandsautomaten. Abbildung 9 stellt wiederum den Kommissionierungsablauf verschiedener Gerätetypen (drahtlos/drahtgebunden) samt Aufnahme des Gerätes in die Ground-Truth-Datenbank dar.

Abbildung 8: Zustandsautomat eines Endgeräts



Quelle: IMD, Universität Rostock

Abbildung 9: Vom Security Controller ausgeführtes Programm zur Kommissionierung verschiedener Gerätetypen



Quelle: IMD, Universität Rostock

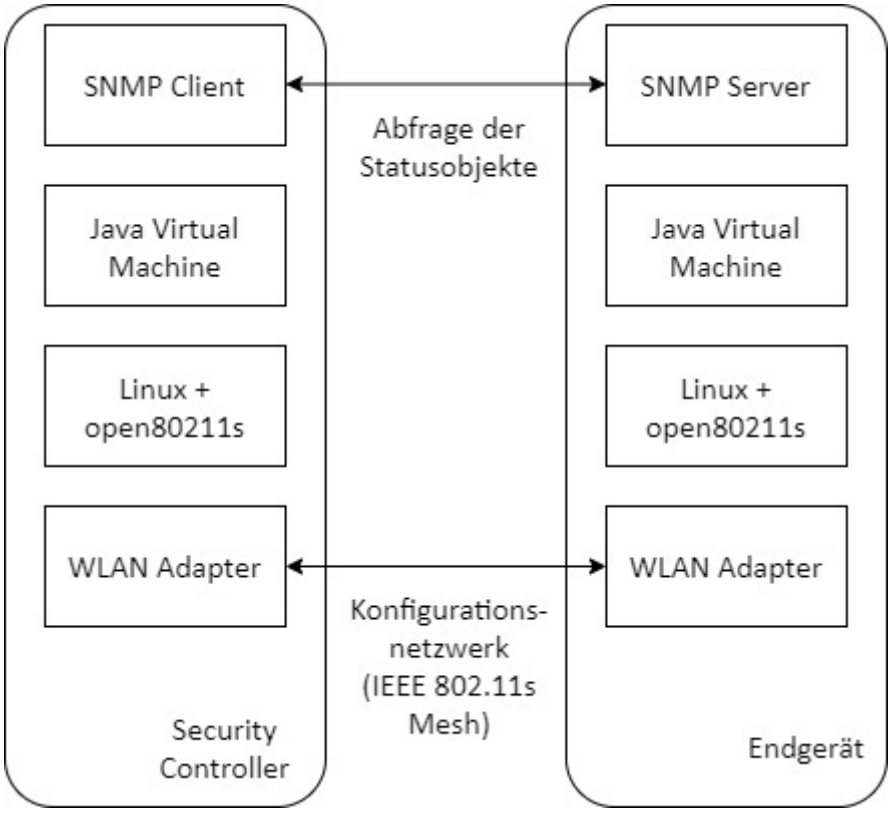
Damit nach erfolgreichem Schlüsselaustausch Endgerät und SC sicher (verschlüsselt und signiert) miteinander kommunizieren können, muss das Endgerät dem Konfigurationsnetz beitreten. Dieses basiert auf Ethernet und WLAN-Mesh gemäß der Spezifikation IEEE 802.11s, um Geräte verschiedener Netzwerktechnologien zu unterstützen. Die Sicherheit des Konfigurationsnetzes basiert im Falle von Ethernet auf IEEE 802.1AE [19]. Dieser Standard, der auch unter dem Namen „MACsec" bekannt ist, dient der Network Access Control (NAC). Die benötigten Zugangsdaten werden vom Nutzer per Smartphone an das Endgerät übertragen. Das WLAN-Mesh-basierte Konfigurationsnetz verwendet das Authentisierungs- und Verschlüsselungsverfahren SAE (Simultaneous Authentication of Equals) zur Absicherung der MAC-Schicht. Die Zugangsdaten für SAE bestehen aus der Kennung des Mesh-Netzwerks (Mesh-SSID) und dem Pre-shared Secret. Nach Erhalt dieser Daten führt das Endgerät mit einem beliebigen anderen Endgerät, das bereits Teil des Konfigurationsnetzes ist, per SAE einen Schlüsselaustausch durch, um dem gesicherten WLAN-Mesh-Netzwerk beizutreten. Im nachfolgenden Schritt wird die Gerätebeschreibung des Endgeräts vom SC abgerufen. Der Nutzer verifiziert den Gerätetyp, sodass dieser Teil der Ground Truth wird.

Weiterhin ist der Installationsort zum Zeitpunkt der Kommissionierung bekannt. Dieser wird durch den Nutzer via grafischer Oberfläche (GUI) auf einem Smartphone der Ground-Truth-Datenbank des SC hinzugefügt. Das in der Middleware verknüpfte Gebäudemodell (BIM) enthält Daten, um das Gebäude-Layout zu visualisieren. Somit ist es möglich, eine entsprechende Nutzeroberfläche zu entwerfen, um den Standort zu annotieren. Gängige Lokalisierungsverfahren eignen sich hier weniger, da die eingeschränkte Lokalisierungsgenauigkeit oft fehlerhafte Standortdaten liefert. Nachdem alle Geräte in die PKI eingebunden wurden und eine Konnektivität zum Konfigurationsnetzwerk erhalten haben, folgt das Einholen von Informationen der Netzwerkebene.

Sammlung von Informationen der Netzwerkebene

Um eine Netzwerkpartitionierung unter Berücksichtigung der netzwerktechnischen Distanz durchführen zu können, benötigt der SC Informationen über die einzelnen Verbindungen jedes Endgeräts. Dabei wird zwischen Ethernet- und WLAN-Mesh-Verbindungen unterschieden. Ethernet-Kabelverbindungen von jedem Endgerät werden vom Nutzer manuell via Smartphone GUI an das BIM annotiert. WLAN-basierte Links zwischen Endgeräten des Konfigurationsnetzes werden mit einem automatisierten Verfahren gesammelt. Das Konzept, WLAN-Mesh-Statusinformationen per SNMP (Simple Network Management Protocol) [20] von einem zentralen Knoten, dem „Mesh Manager", abzurufen und innerhalb von Anwendungen zu nutzen, wurde in [21] prototypisch für Linux-Umgebungen vorgestellt. Die Rolle des Mesh Managers wird in der Sicherheitsarchitektur durch den SC übernommen, der Statusinformationen der einzelnen Endgeräte verwaltet. In Abbildung 10 sind SC und Endgerät schematisch dargestellt. Beide Geräte kommunizieren über das IEEE-802.11s-basierte Mesh-Konfigurationsnetz. Das Linux-Kernelmodul mac80211 implementiert dabei die 802.11s-Funktionen. Das Endgerät führt einen SNMP-Server aus, der in Java implementiert ist. Durch Aufrufen des Kommandozeilentools *iw* aus der Java Virtual Machine (JVM) heraus wird die Mesh-Routingtabelle samt Pfadkosten-Metriken ausgelesen. SNMP unterstützt das Abfragen von Statusinformationen, die als Statusobjekte von einem Server angeboten werden. Die ausgelesenen Routingtabelleneinträge werden daher in Form von SNMP-Statusobjekten dargestellt. Jedes Statusobjekt wird per GET-Operation vom Server abgefragt, der auf jedem Endgerät auf dem Konfigurationsnetz-Interface auf eingehende Anfragen vom SC wartet.

Abbildung 10: Abfrage der Routingtabelle eines Endgerätes durch den Security Controller



Quelle: IMD, Universität Rostock

Das HWMP (Hybrid Wireless Mesh Protocol) wird von jedem WLAN-Mesh-Knoten, auch Mesh Point (MP) genannt, standardmäßig unterstützt, um als einheitliches Profil das Routing im Mesh-Netzwerk zu definieren [22]. Die ALM (Airtime Link Metric) dient dabei als Metrik zur Bewertung von Pfadkosten zwischen zwei MPs. Das Routingprotokoll nutzt die ALM, um die netzwerktechnische Distanz zwischen Quelle und Ziel eines Frames abzuschätzen. Bei der ALM handelt es sich um die akkumulierten Übertragungszeitkosten aller Links, aus denen eine Multi-Hop-Übertragungsstrecke besteht. Die *Airtime Cost* c_a eines Links zwischen zwei Mesh Peers beschreibt die geschätzte Übertragungszeit einer Nachricht. Sie berechnet sich nach der folgenden Formel:

$$c_a = \left[O_{ca} + O_p + \frac{B_t}{r}\right] * \frac{1}{1 + e_{fr}}$$

Die Variablen $\mathcal{O}_{ca}$ (Kanalzugriffszeit) und $\mathcal{O}_p$ (MAC-Protokoll-Overhead) sind technologieabhängige Konstanten. $\mathcal{B}_t$ beschreibt die Größe eines Test-Frames. Der Standardwert ist mit 8192bit beziffert. „r" steht für die Datenrate in Mbit/s, mit welcher der Test-Frame übertragen wird. Da durch fehlerhafte Frame-Übertragungen erneute Sendeversuche nötig sind, erhöht sich die mittlere Kanalzugriffszeit. Daher wird in der Airtime-Cost-Formel die Fehlerrate e_{fr} berücksichtigt. Nach dem IEEE 802.11s Standard werden die konkrete Implementierung der Schätzungen der Fehlerrate e_{fr} sowie die Konstanten $\mathcal{O}_{ca}$ und $\mathcal{O}_p$ nicht vorgegeben, dies ist dem Hersteller überlassen [23].

Erstellung und Verifikation der Anwendungsebene

Die Geräteverknüpfungen auf Anwendungsebene basieren auf dem in [24] publizierten Konzept. Traditionell werden Geräte der Feldebene auf Steuerungsebene durch Speicher-Programmierbare Steuerungen (SPS) verknüpft. SPS-Anlagen werden fest mit den einzelnen Geräten verbunden, um eine Kommunikation zum Lesen von Sensorwerten und zum Steuern von Aktorik zu ermöglichen. Die logischen Funktionen können von der Administration der

Gebäudeleittechnik frei definiert werden. Dazu wird die von der SPS-Anlage ausgeführte Software modifiziert. Da dieser zentralisierte Ansatz anfällig für Ausfälle der Steuerungsanlage ist und es daher zu einem Ausfall aller Funktionen innerhalb der GA kommen kann, eignen sich dezentrale Ansätze zur Steuerung.

Das in [24] beschriebene Konzept führt einen Konfigurationsservice ein, der generisch für eingebettete Systeme implementiert werden kann. Das Interface des Konfigurationsservices bietet die in Tabelle 2 aufgeführten Funktionen. Im Gegensatz zu [24] werden die einzelnen Funktionen nicht in Form eines Web Services nach DPWS (Devices Profile for Web Services) sondern durch eine RESTful API im Netzwerk angeboten.

Tabelle 2: RESTful API des Konfigurationsservices

Ressource	**Beispieldaten**
/config/getSupportedInterfaces	Motion Detector
/config/connectDevice	Null
/config/getConnectedDevices	[Motion Detector ID]
/config/setRule	Null
/config/getRule	[Anwendungsgraph]

Die von einem Gerät unterstützten Interfaces können somit abgefragt werden. Bezeichnungen für entsprechende Geräte-Interfaces (z. B.: Sensor::Bewegungsmelder, Sensor::Temperaturfühler, Sensor::Helligkeitssensor, Aktor::Fenstersteuerung und Aktor::Beleuchtung) müssen samt Datenmodell herstellerübergreifend spezifiziert sein. Die Open Mobile Alliance [25] löst das Problem durch öffentlich einsehbare Standards. Der Konfigurationsservice nimmt unterstützte Geräte entgegen. Dabei werden folgende Daten vom SC übermittelt:

- IP-Adresse
- Protokoll-Stack
- Pre-shared Key (PSK)

Damit ein Gerät, das den Konfigurationsservice ausführt, Sensoren und Aktoren abfragen bzw. steuern kann, müssen neben der IP-Adresse der zu verwendende Protokoll-Stack samt Schlüsselmaterial (PSK) vom SC übermittelt werden. Dieses Konzept ist somit auf alle Protokolle übertragbar, die einen PSK zur kryptographischen Absicherung der Kommunikation unterstützen. Dazu zählen beispielsweise DTLS, TLS und OSCORE. Je nach Protokoll werden Pre-shared Secrets unterstützt, um einen Sitzungsschlüssel zwischen beiden Kommunikationspartnern auszuhandeln. Die unterstützten Protokoll-Stacks müssen durch eine Selbstbeschreibung jedes Endgeräts abrufbar sein, damit der SC entsprechende Pre-shared Secrets bzw. Pre-shared Keys individuell zuordnen kann.

Formale Beschreibung von Konfigurationsregeln

Die Konfiguration von Anwendungen auf Endgeräten kann durch Regeln beschrieben werden. Jede Regel besteht aus einzelnen Bedingungen (4), die durch Boole'sche Operatoren (5) miteinander verknüpft sind. Jede Bedingung nach (4) (mathematischer Term) beschreibt eine physikalische Größe (Parameter), die durch eine Operation (2) mit einem Schwellenwert (Element der ganzen Zahlen) verglichen wird. Eine sogenannte Messfunktion (3) bildet jeden Parameter auf eine ganze Zahl ab, sodass ein Vergleich mit einem Schwellenwert möglich ist:

$$OPERATION := \{=, \neq, >, \geq, <, \leq\} \quad (2)$$

$$f: PARAMETER \rightarrow \mathbb{Z} \quad (3)$$

$$BEDINGUNG := \{PARAMETER \times OPERATION \times \mathbb{Z}\} \quad (4)$$

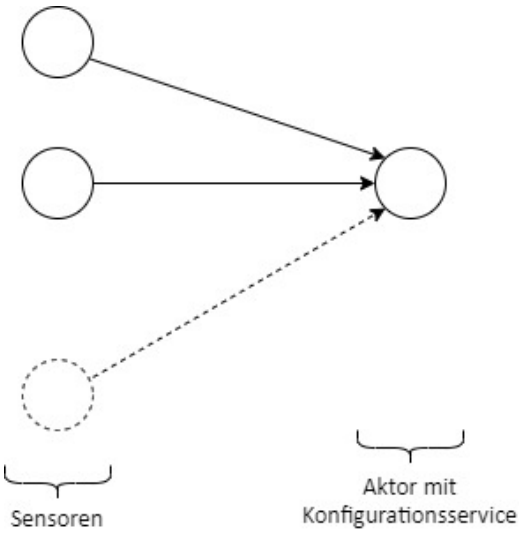
$$BOOL\ OPERATOR := \{AND, OR, NAND, NOR, XOR, XNOR\} \quad (5)$$

$$REGELN := \mathcal{P}(BEDINGUNG) \times BOOL\ OPERATOR \quad (6)$$

Ein Beispiel für eine Fenstersteuerung lässt sich in folgender Form beschreiben: „Fenster öffnen WENN (Außentemperatur < Sollwert) UND (Innentemperatur > Sollwert)".

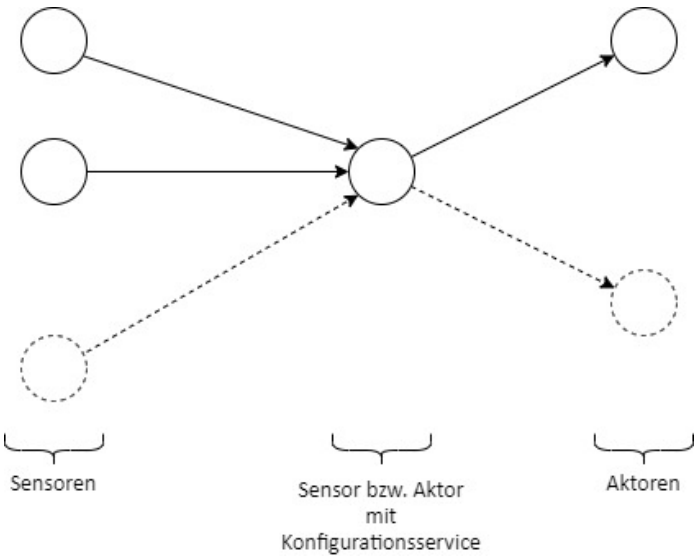
In einem realen Anwendungsfall wird der Konfigurationsservice nach Tabelle 2 auf einem Aktor ausgeführt, da Sensorknoten für diese Aufgabe aufgrund von Energieversorgungsproblemen oft nicht geeignet sind. Insbesondere verbringen batteriebetriebene Mikrocontrollerplattformen die meiste Betriebszeit im Schlafzustand (engl.: deep sleep), um Energie zu sparen. In diesem Zustand wäre der Konfigurationsservice nicht erreichbar. Ein Aktor zur Ausführung von Konfigurationsregeln kann durch beliebig viele Sensoren mit Daten gespeist werden. Dabei entsteht ein zweistufiger Anwendungsgraph nach Abbildung 11. Im Fall, dass ein weiterer Aktor / weitere Aktoren durch eine Regel angesteuert werden, entsteht ein dreistufiger Anwendungsgraph nach Abbildung 12.

Abbildung 11: Zweistufige Sensor-Aktor-Beziehung



Quelle: IMD, Universität Rostock

Abbildung 12: Dreistufige Sensor-Aktor-Beziehung



Quelle: IMD, Universität Rostock

Verifikation von Konfigurationsregeln

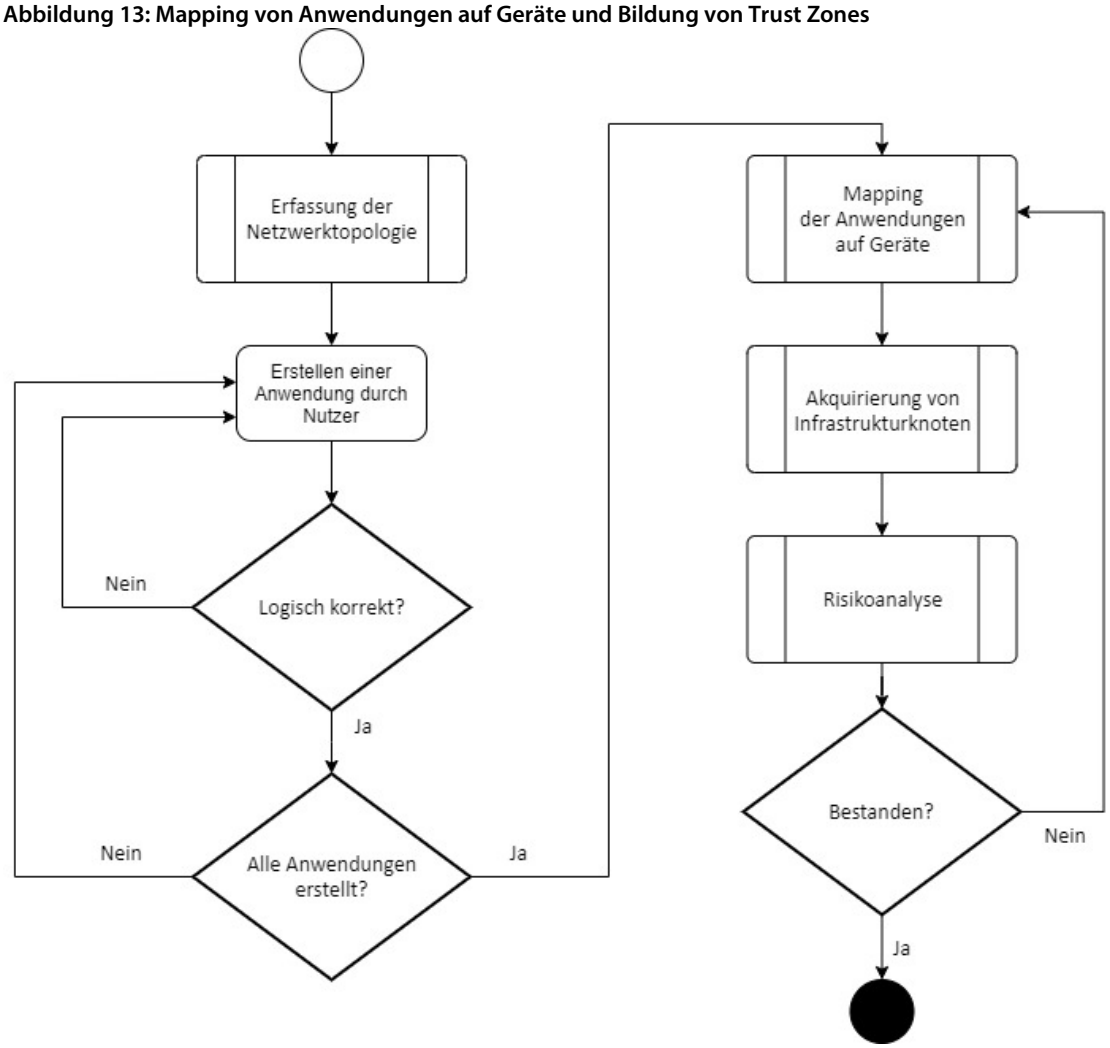
In [26] wurde ein formales Verfahren zur Verifikation der Anwendungslogik vorgestellt. Dabei kommen binäre Entscheidungsdiagramme (BDD, Binary Decision Diagram) zum Einsatz. Sie repräsentieren Boole'sche Funktionen. Jeder Knoten stellt eine Variable dar. Da jede Variable zwei Zustände (wahr - durchgezogene Linie und falsch - gestrichelte Linie) annehmen kann, gehen von jedem Knoten zwei Kanten ab. Die Blätter des Graphen repräsentieren die Funktionswerte der Boole'schen Funktion. Wird die Reihenfolge der Variablen berücksichtigt, so spricht man von einem geordneten binären Entscheidungsbaum (OBDD, Ordered Binary Decision Diagram). OBDDs lassen sich miteinander verknüpfen und vereinfachen.

Die Konfigurationsregeln lassen sich durch Substitution der Terme mit Vergleichsoperator in Boole'sche Funktionen überführen. Damit lässt sich jede Regel mit einem BDD modellieren. Wenn zwei oder mehr Regeln dieselbe Aktorik steuern, treten potentiell Kollisionen auf. Die einzelnen Boole'schen Funktionen liefern bei einer bestimmten Eingangsvariablenbelegung verschiedene Werte, sodass ein Widerspruch entsteht. Wenn zwei BDDs dieselbe Variablenreihenfolge besitzen, lassen sie sich mit zwei OBDDs beschreiben, sodass eine Verknüpfung beider Graphen miteinander möglich ist. Wenn beide Funktionen mittels XOR (exklusiv oder) verknüpft werden und mindestens ein Blattknoten wahr ist, so existiert mindestens eine Eingangsvariablenbelegung, die zu einem Konflikt führt. Sogenannte SAT-Solver können angewendet werden, um entsprechende Variablenbelegungen zu identifizieren. Im Gegensatz dazu kann das Fehlen von Fehlerzuständen bewiesen werden, wenn alle Blätter falsch sind. Durch Substitution der Variablen mit den Vergleichstermen kann der Fehlerfall eingegrenzt werden. Logische Konfigurationsfehler lassen sich während der Inbetriebnahme der GA identifizieren. Weiterhin können angepasste Regel-Logiken zur Laufzeit mit dem vorgestellten Verfahren formal verifiziert werden. Da die Konfigurationsregeln in einer GA keine große Tiefe (wenige Variablen) aufweisen, sind keine besonderen Komplexitätsbetrachtungen nötig.

Abbildung der Anwendungen auf reale Geräte

Nach Erstellung und Validierung aller Anwendungsgraphen erfolgt deren Abbildung auf reale Geräte. Dazu führt der Security Controller einen heuristischen Ansatz aus (siehe Abbildung 13). Ein Anwendungsgraph wird nach Schwerpunkt 1 auf einer abstrakten Ebene beschrieben. Die im ersten Teil des Forschungsprojektes vorgestellte Lösung kann zu mehreren gültigen Geräten führen. Soll beispielsweise die Zimmertemperatur eines speziellen Raumes abgefragt werden, um als Eingabewert für eine Regel zu dienen, kann die SPARQL-Abfrage mehr als einen Temperatursensor aus der Gerätedatenbank liefern. Der Planungsalgorithmus des Security Controllers trifft aus der Menge aller möglichen Geräte eine zufällige Auswahl. Dieses Vorgehen wiederholt sich solange, bis alle Anwendungsgraphen auf reale Geräte abgebildet wurden. Alle Geräte, die zu einem Anwendungsgraphen gehören, werden im nächsten Schritt zu einer Trust Zone hinzugefügt.

Abbildung 13: Mapping von Anwendungen auf Geräte und Bildung von Trust Zones

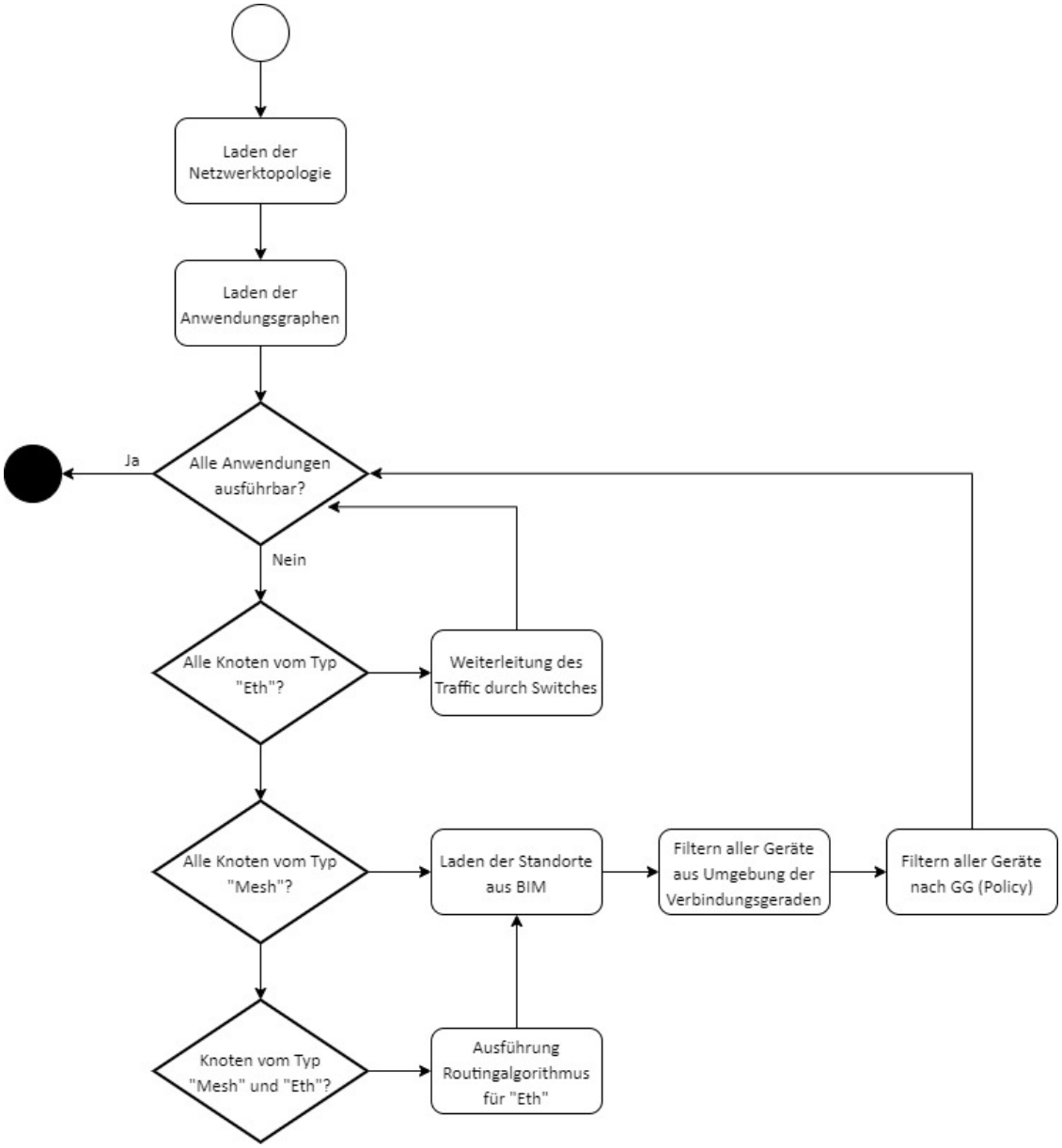


Quelle: IMD, Universität Rostock

Policy-basierte Bildung von Trust Zones

Im nachfolgenden Schritt (siehe Abbildung 14) wird abgeschätzt, ob alle Anwendungen ohne zusätzliche Netzwerkinfrastruktur ausführbar sind. Dies betrifft alle Anwendungsgraphen, deren Kanten (mindestens eine) auf WLAN-Mesh nach IEEE 802.11s basieren. Durch Kenntnis über den Installationsort der Geräte aus dem BIM in Verbindung mit dem Wissen über Wand- und Deckenparameter und somit der Signaldämpfung lässt sich ermitteln, ob zwei Geräte über einen sogenannten Single-Hop-Link (Direktverbindung) miteinander kommunizieren können. Sollte dies nicht möglich sein, lassen sich Geräte, die sich auf der geometrischen Verbindungslinie befinden, als zusätzliche Infrastrukturknoten zur Trust Zone hinzufügen. Im Fall, dass mehrere Infrastrukturgeräte als Kandidaten möglich sind, werden die Geräte herausgefiltert, welche dieselbe Firmware wie die Geräte des Anwendungsgraphen ausführen bzw. derselben Anwendungsdomäne entstammen. Bei der Wahl der Infrastrukturknoten wählt der Security Controller eine minimale Menge, um die Trust Zone und somit die Angriffsfläche so klein wie möglich zu halten.

Abbildung 14: Akquirierung von Infrastrukturknoten

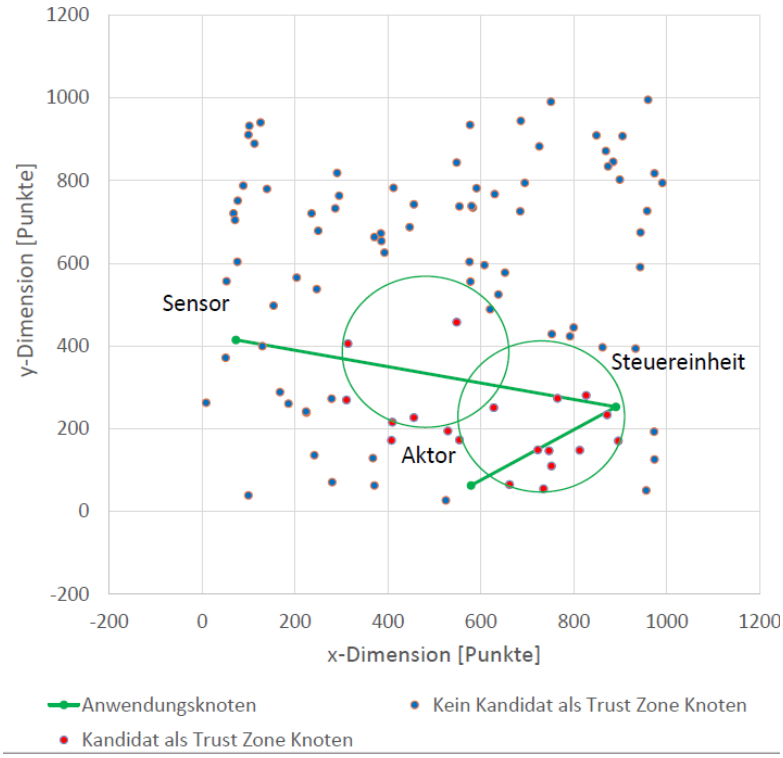


Quelle: IMD, Universität Rostock

Der entwickelte Algorithmus zur Berechnung von Trust Zones muss sicherstellen, dass alle Anwendungen ausgeführt werden können. Das heißt, dass eine zuverlässige netzwerktechnische Konnektivität zwischen den Geräten eines Anwendungsgraphen existieren muss. Der Algorithmus berücksichtigt vermaschte WLAN-Netzwerke, bei denen jedes Gerät als Netzwerkinfrastruktur (mit der Fähigkeit, Nachrichten weiterzuleiten) betrachtet wird. Netzwerke, die auf dedizierter Netzwerkhardware beruhen bzw. aus einem Verbund aus Netzwerkgeräten und vermaschten Netzwerkbereichen bestehen, können konfiguriert werden. Exemplarisch wurden reine vermaschte Netzwerke betrachtet. Basierend auf dem physischen Installationsort (bekannt aus der Ground-Truth-Datenbank des SC) trifft der Algorithmus für jedes Gerät eine Entscheidung, ob das Gerät ein Kandidat für eine Trust Zone ist oder nicht. Zur einfacheren Darstellung werden die Endgeräte in einem zweidimensionalen kartesischen Koordinatensystem dargestellt. Die Daten lassen sich aus dem BIM gewinnen. In [27] wurde ein erster Ansatz vorgestellt, der den Installationsort zwischen Geräten auswertet, um zusätzliche Knoten vorzuselektieren. Es wurde die vereinfachte Annahme getroffen, dass Geräte in einer GA gleichverteilt platziert sind. Jeder Raum verfügt u.a. über Beleuchtung, Bewegungsmelder, Raumklimasensorik und Aktoren zur Fenster- und Türsteuerung. Dabei ist es vorgesehen, dass

mehr Endgeräte als nötig Teil der Trust Zone werden, da jedes einzelne Gerät als zusätzliche Netzwerkinfrastruktur fungieren kann. Fallen Geräte zur Weiterleitung von Frames aus, ermittelt das Routing von IEEE 802.11s automatisch eine neue Route. Somit ist eine Ausfallsicherheit gegeben. In Abbildung 15 ist ein einfacher Anwendungsgraph dargestellt, bestehend aus einer Steuereinheit, die Sensordaten von einem Sensor abruft und einen Aktor steuert. In der Umgebung der direkten Verbindung zwischen zwei Geräten des Anwendungsgraphen (ungeachtet von Hindernissen und Materialeigenschaften, die sich aber aus dem BIM gewinnen lassen) werden alle Endgeräte ausgewählt. Sie sind als Trust-Zone-Kandidaten zu betrachten, da jedes Gerät, das Teil der Trust Zone werden soll, den Security Policies genügen muss. Da der Selektionsalgorithmus aus [27] lediglich Geräte aus der Umgebung der Streckenhalbierenden betrachtet und weitere sinnvolle Knoten außer Acht gelassen werden, wurde eine Verbesserung eingeführt: Der modifizierte Algorithmus betrachtet alle Endgeräte, die sich in einem Korridor der Breite *w* befinden.

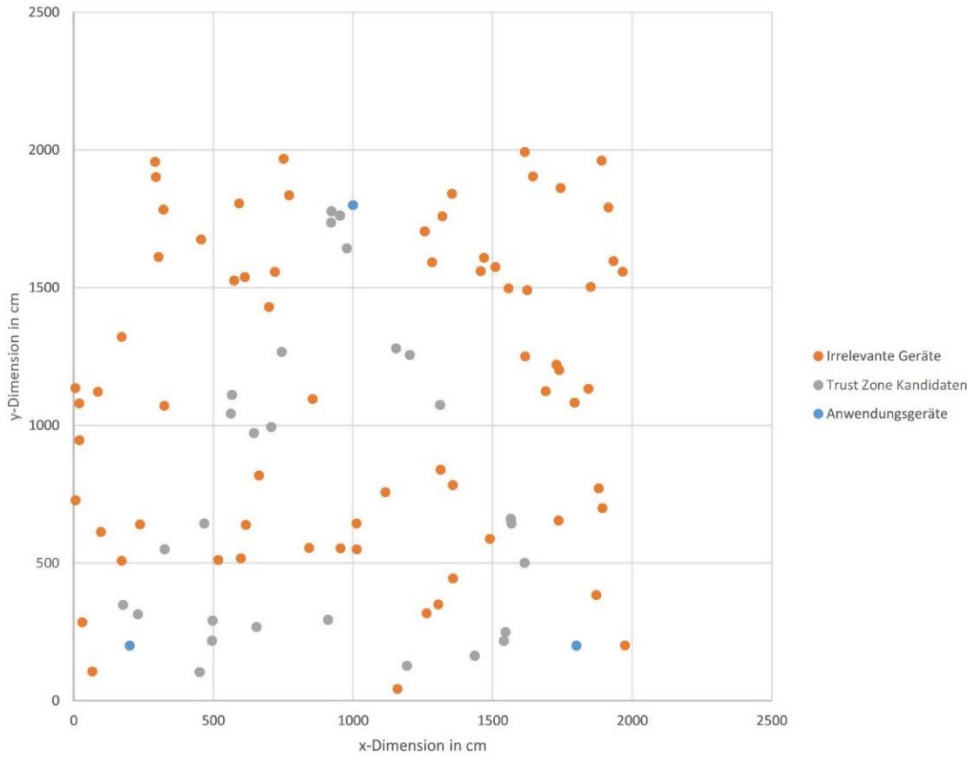
Abbildung 15: Geräte, die sich in der Umgebung der Verbindungslinien zwischen Sensor, Aktor und Steuereinheit befinden, werden als mögliche weitere Trust Zone Knoten ausgewählt



Quelle: IMD, Universität Rostock

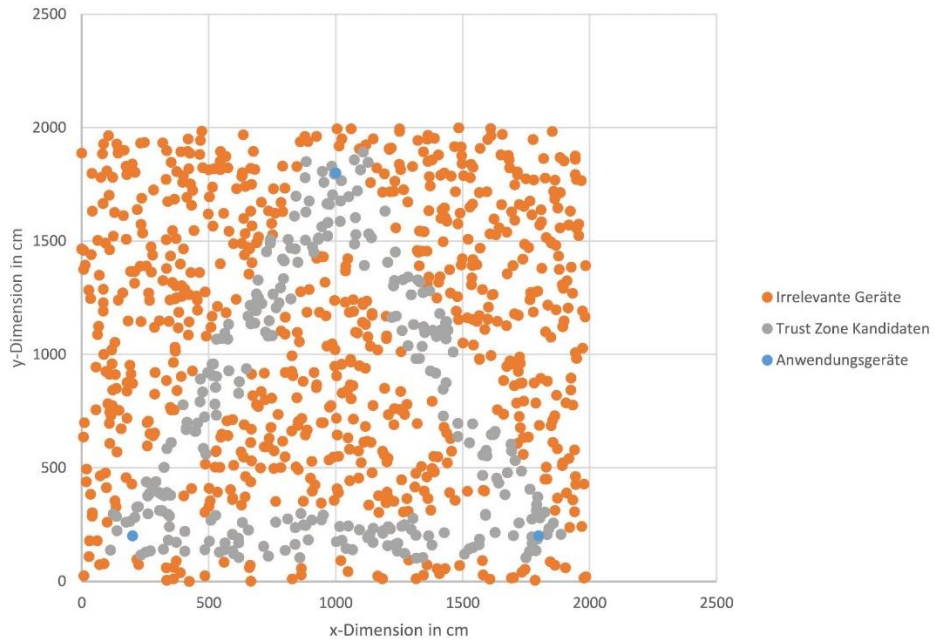
In Abbildung 16 sind in einem kartesischen Koordinatensystem durch eine eigene Simulation 100 Endgeräte zufällig gleichverteilt platziert worden. Drei Geräte, die sich möglichst weit voneinander entfernt befinden, bilden den Anwendungsgraphen. Exemplarisch wurde die Korridorbreite *w*=1m gesetzt. Die Auswahl an Trust-Zone-Kandidaten ist grau dargestellt. Um die geometrische Vorauswahl besser darstellen zu können, wurde das System auf 1000 Endgeräte erweitert. Das Ergebnis ist in Abbildung 17 dargestellt.

Abbildung 16: GA bestehend aus 100 Geräten: Optimierter Algorithmus zur Auswahl von Trust Zone Kandidaten



Quelle: IMD, Universität Rostock

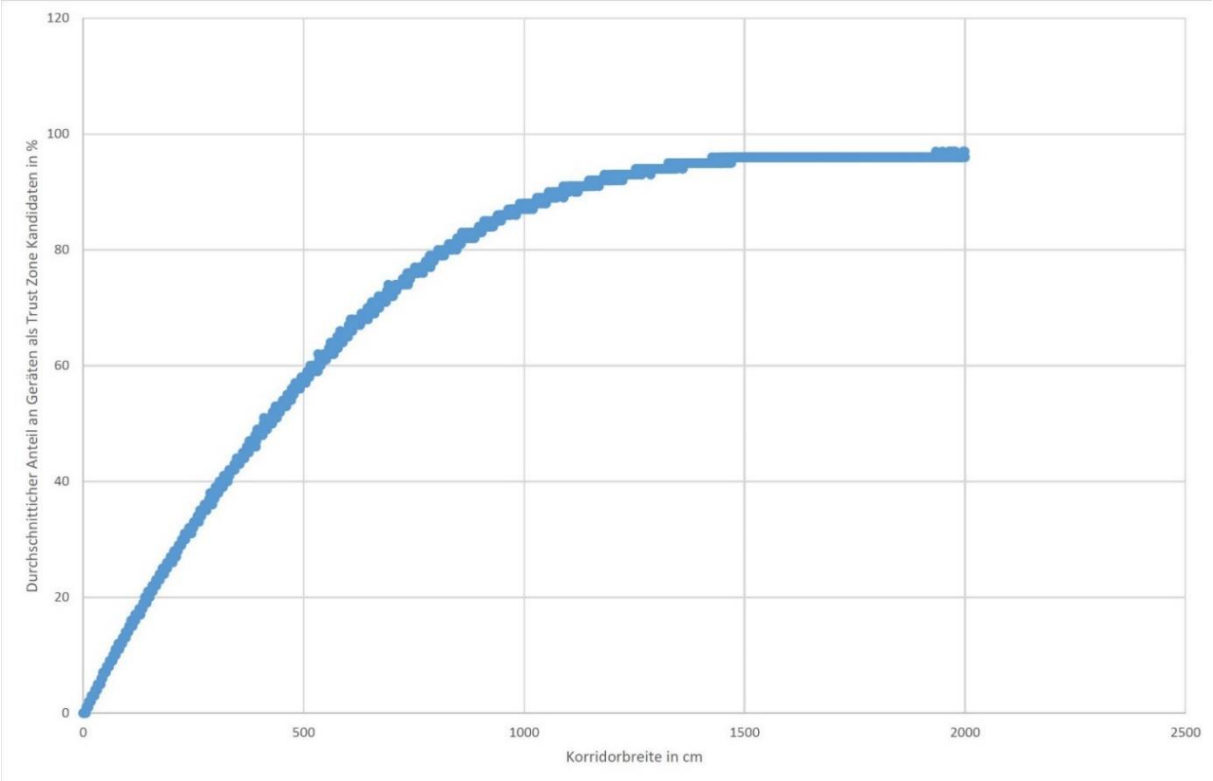
Abbildung 17: GA bestehend aus 1000 Geräten: Optimierter Algorithmus zur Auswahl von Trust Zone Kandidaten



Quelle: IMD, Universität Rostock

Des Weiteren wurde der Einfluss der Breite *w* auf den prozentualen Anteil an Endgeräten, die als Trust-Zone-Kandidaten markiert werden, bestimmt. Das Ergebnis findet sich in Abbildung 18. Jeder Messwert ist der Durchschnitt aus 1000 Durchläufen, bei denen jeweils eine neue zufällige Knotenverteilung (inkl. 3 Anwendungsgeräten) berechnet wurde. Es ist erkennbar, dass bereits bei einer geringen Breite von 5m ca. 60% aller Endgeräte berücksichtigt werden. Je nach Grad der Überbestimmtheit der Trust Zone kann der Wert angepasst werden. Dies muss jedoch anhand realer Geräteinstallationen geschehen, da die Testdaten bisher lediglich eine Gleichverteilung abbilden.

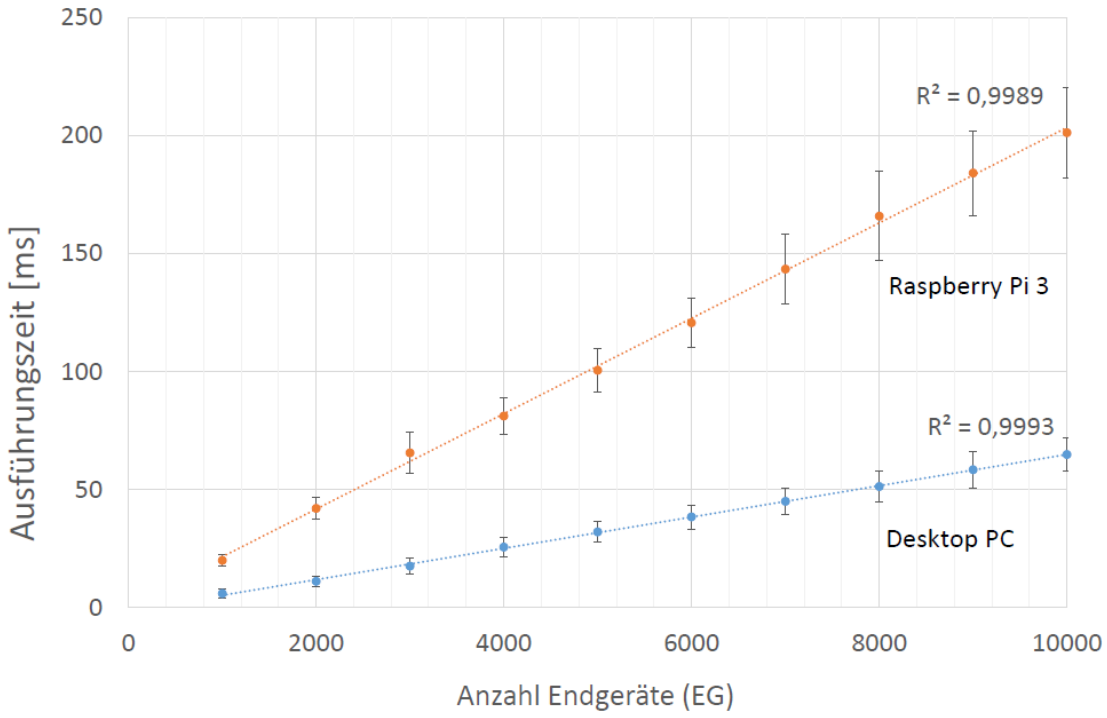
Abbildung 18: Anteil an Geräten als Trust Zone Kandidaten in Anhängigkeit von der Korridorbreite



Quelle: IMD, Universität Rostock

Weiterhin wurde die Ausführungszeit des Algorithmus bestimmt. Da jedes Endgerät unabhängig von anderen Endgeräten gemäß seinen Eigenschaften einer Gruppe zugeordnet wird, ergibt sich eine lineare Laufzeitkomplexität ($R^2 < 0{,}99$). Die Experimentalergebnisse aus Abbildung 19 belegen den linearen Zusammenhang zwischen Knotenanzahl und Ausführungszeit. Der Algorithmus wurde je auf einem Raspberry Pi 3, welcher der Leistungsklasse des SC entspricht, und auf einem Desktop PC ausgeführt. Dabei wurde der Algorithmus je Messwert 1000-mal auf verschiedenen Geräteverteilungen ausgeführt und die Ausführungszeit bestimmt. Der Raspberry Pi 3 benötigt ca. 200ms, um für einen Anwendungsgraphen aus 10.000 Geräten alle relevanten Trust-Zone-Kandidaten zu bestimmen. In einem realen Anwendungsfall sind deutlich weniger als 10.000 Geräte vorhanden, sodass dieser Wert einen Extremfall darstellt. Um *n* Anwendungen durch den Algorithmus abzubilden, beträgt die Ausführungszeit weniger als *n* * 200ms. Der tatsächliche Wert liegt jedoch unter der Geraden *n* * 200ms, da Geräte, die eine Anwendung bilden, bereits Teil einer Trust Zone sein können. Je mehr Anwendungen abgebildet wurden, desto höher ist die Wahrscheinlichkeit dafür.

Abbildung 19: Ausführungszeit des Partitionierungsalgorithmus



Quelle: IMD, Universität Rostock

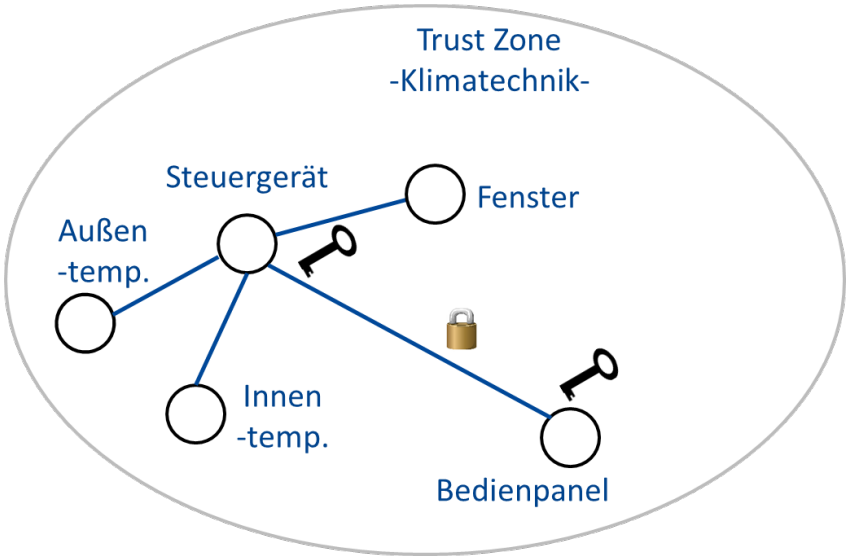
Im abschließenden Schritt wird die heuristisch ermittelte Lösung (Trust-Zone-Zuordnung von Geräten) hinsichtlich einer Security Policy geprüft. Mögliche Policies sind:

- Alle Geräte müssen einer Anwendungsdomäne zugehörig sein
- Kein Gerät darf sich in einem öffentlich zugänglichen Bereich befinden
- Alle Geräte müssen die aktuellste Firmware-Version ausführen
- Lediglich Geräte derselben Kritikalitätsstufe dürfen miteinander kommunizieren

Gerätekonfiguration durch Nutzer zur Laufzeit

Der im Abschnitt *„Erstellung und Verifikation der Anwendungsebene“* beschriebene Konfigurationsservice wertet Sensordaten aus, indem er sie mit Schwellenwerten vergleicht. Es ist konzeptionell möglich, diese Schwellenwerte während der Kommissionierungsphase eines Gebäudes oder während der Laufzeit der GA zu ändern. Letzter Fall wird realisiert, indem der Anwendungsgraph bestehend aus Sensoren, Steuergerät und Aktoren durch einen weiteren Knoten, ein Eingabegerät, erweitert wird (siehe Szenario in Abbildung 20). Der SC weist dem Steuergerät und dem Bedienpanel exklusives Schlüsselmaterial zu, damit eine abgesicherte Verbindung zur Laufzeit hergestellt werden kann. Lediglich das Bedienpanel ist in der Lage, authentifizierte Steuerdaten an den Konfigurationsservice zu senden. Das Steuergerät, das den Konfigurationsservice ausführt, ist wiederum in der Lage, durch das vertrauenswürdige Schlüsselmaterial (vom SC zugeteilt) die Authentizität und Integrität der Nachrichten sicherzustellen. Konzeptionell sind verschiedene Sicherheitsprotokolle, die einen Pre-shared Key zulassen, einsetzbar. Dazu zählen beispielsweise DTLS, TLS und OSCORE.

Abbildung 20: Geräte-/Regel-Konfiguration durch eine/n Nutzer/in



Quelle: IMD, Universität Rostock

Dezentrale Speicherung von Log-Daten

Während der Laufzeit des GA-Systems können verschiedene Events auftreten, die es zu protokollieren gilt. Für die sicherheitstechnische Analyse von Angriffen müssen Geräte daher Log-Daten anlegen. Abgerufene Sensorwerte, Serveranfragen, Login-Versuche und Fehlermeldungen stellen eine wichtige Datenquelle für die Computerforensik dar. Die angefallenen Daten sollten redundant im Netzwerk auf verschiedenen Geräten gespeichert werden, um eine Ausfallsicherheit zu gewährleisten. Des Weiteren ist es wichtig, dass andere Geräte Log-Daten nicht verändern werden können (Integritätsschutz). Da jedes Gerät, das Log-Daten produziert und speichert, über ein Schlüsselpaar verfügt, ist es möglich, eine digitale Signatur der Daten zu erstellen. Die signierten und versendeten Daten werden von anderen Netzwerkteilnehmern redundant gespeichert. Selbst wenn das Gerät, das die Daten signiert hat, kompromittiert wird, können die gespeicherten Daten zugeordnet werden. Die Abstreitbarkeit ist somit ausgeschlossen. Nachfolgend werden einige Ansätze zur redundanten Speicherung von Daten (signierten Log-Daten) vorgestellt und auf ihre Tauglichkeit für den Einsatz in einem Gebäudeautomationssystem bewertet.

Der wohl bekannteste Vertreter der Blockchain-Technologie ist die Bitcoin-Kryptowährung. Sie soll es ermöglichen, dass Teilnehmer über ein dezentral und redundant organisiertes Kassenbuch Transaktionen abwickeln. Die geschieht vor dem Hintergrund, dass sich die Teilnehmer untereinander nicht vertrauen und einzelne, bösartige Teilnehmer Kontostände zu ihren Gunsten manipulieren. Da die Kernidee der Bitcoin-Blockchain darin besteht, dass nicht eine Instanz (z. B. eine Bank) das Kassenbuch führt, sondern die Gesamtheit aller Knoten, wird das sogenannte „Proof-of-work"-Verfahren angewendet. Dabei muss ein Gerät, das einen neuen Datenblock für die Gemeinschaft erstellt, eine aufwändige Rechenaufgabe lösen, deren korrekte Lösung durch eine einfache Prüfung durch jeden der anderen Netzwerkteilnehmer geprüft werden kann. Der neue Block wird daraufhin an alle anderen Teilnehmer verteilt und redundant gespeichert. Dieses Verfahren ist jedoch aufgrund des hohen Ressourcenbedarfs nicht für den Einsatz auf eingebetteten Systemen geeignet. Außerdem könnte ein einzelner Knoten, der unter der Kontrolle eines Angreifers steht, mit Leichtigkeit durch Auslagern der Proof-of-work-Aufgabe an externe Server mehr als 51% der Rechenkapazität des gesamten Gebäudeautomationsnetzes erlangen und somit volle Kontrolle über das Logging erzielen. Dieses Problem trifft auch auf Verfahren zu, bei denen Geräte über großen Speicher verfügen müssen, um neue Einträge zu produzieren. Im Gegensatz dazu stehen „Proof-of-Stake"-Verfahren. Diese verteilten Konsensverfahren basieren auf einem dezentral organisierten Wahlverfahren, bei dem alle Knoten einen bestimmten Knoten temporär zum Anführer (Leader) wählen. Dieser einzelne Knoten ist in der Lage, den nächsten Eintrag in die Blockchain zu schreiben. Dabei besteht für jeden Knoten dieselbe Wahrscheinlichkeit, zum führenden Knoten ernannt zu werden. Ein Vertreter dieser Ansätze ist beispielsweise Raft [28].

Neben Blockchain-Ansätzen, um signierte Log-Daten redundant zu speichern, existieren P2P-Ansätze. Vollständig dezentral organisierte Verfahren wie das Kademlia-Protokoll [29] verwenden ein logisches Overlay-Netzwerk, das von den realen Geräten abstrahiert. Kademlia ermöglicht es, Daten redundant zu speichern. Dadurch wird eine höhere Ausfallsicherheit erzielt. Da Kademlia ein selbstorganisierendes Protokoll ist, das Daten auf Basis ihrer Hashwerte auf verschiedenen Geräten speichert, ist es sehr gut ohne zentrale Management-Instanz anwendbar. Damit ein Endgerät dem P2P-Netzwerk beitreten kann, benötigt es lediglich einen sogenannten Bootstrap-Knoten als Einstieg, um mit dem gesamten Netzwerk kommunizieren zu können. Die Kontaktinformationen (IP-Adresse und Hashwert) des Bootstrap-Knotens können vom Security Controller an Endgeräte übermittelt werden. Hervorzuheben ist, dass ein Bootstrap-Knoten keine besonderen Eigenschaften aufweisen muss, sodass sich jedes Endgerät, das Teil des P2P-Netzwerks ist, für diese Aufgabe eignet. Dieser P2P-basierte Ansatz stellt lediglich eine Variante dar, signierte Log-Daten dezentral und redundant zu speichern. Neben diesen Verfahren existieren auch Konzepte und Protokolle aus dem Bereich dezentraler Datenbanken.

Abgeleitete Sicherheitsvorteile

Nachfolgend werden die durch das in Schwerpunkt 2 entwickelte Konzept erzielten Sicherheitsvorteile zusammenfassend erläutert:

Sicherer Updatemechanismus

Der Security Controller besitzt das Wissen über die aktuell installierte Firmware-Version aller Geräte im Gebäude. Bei Bekanntwerden eines Zero-Day-Exploits zur Ausnutzung von Schwachstellen eines Gerätes durch einen Angreifer kann der Hersteller den Security Controller über eine Schnittstelle informieren. Der Security Controller kann daraufhin das Netzwerk so konfigurieren, dass das betroffene Gerät in Quarantäne gesetzt wird bis ein Sicherheitsupdate verfügbar ist. Die Verteilung des Updates erfolgt über eine gesicherte Verbindung, die über den Security Controller initiiert wird.

Autorisierungsmanagement

Der Security Controller verwaltet eine Autorisierungsdatenbank zur Erteilung von Zugriffsrechten zur Laufzeit. Dabei basiert die vorgestellte Realisierung auf dem formal verifizierten Autorisierungsprotokoll OAuth2.0.

Sicherheitsrichtlinien

Mithilfe des Autorisierungsmanagements lassen sich allgemeingültige Zugriffsrechte umsetzen. Dabei wird die Kommunikation zwischen bestimmten Gerätegruppen explizit erlaubt bzw. untersagt (Whitelist/Blacklist). So kann beispielsweise die Kommunikation zwischen Geräten unterbunden werden, die logisch nichts miteinander zu tun haben. Ein Gerät, wie z. B. eine smarte Glühlampe mit kompromittierter Firmware, kann daher nicht von einem Angreifer missbraucht werden, um valide Nachrichten innerhalb des Netzwerks an eine Türschließanlage zu senden.

Konfigurationsüberprüfung

Da eine moderne Gebäudeautomation einer serviceorientierten Architektur gleichkommt, bei der Geräte ihre Funktionalitäten in Form von Diensten zur Verfügung stellen, können Geräte zur Laufzeit gekoppelt werden. Eine Kopplung lässt sich durch eine Konfiguration erzielen, bei der die Kommunikationspartner miteinander logisch in Verbindung gesetzt werden. Sensorik und Aktorik wird mithilfe von Wenn-Dann-Sonst-Verkettungen miteinander verknüpft. Allerdings können solche Konfigurationen untereinander logische Fehler enthalten, die folglich zu einem Fehlverhalten des Gesamtsystems führen. Der Security Controller kann mithilfe mathematischer Methoden Logikfehler ermitteln und beheben. Dazu werden die Konfigurationen mithilfe von Binary Decision Trees (BDDs) modelliert und auf das Nicht-Vorhandensein von Konflikten formal verifiziert.

Intrusion Detection

Über den Broker kann der Security Controller zyklisch Statusinformationen von Geräten und der Netzwerkinfrastruktur abfragen. Mithilfe von Mustererkennungsverfahren lassen sich Anomalien erkennen und Gegenmaßnahmen einleiten. Wird beispielsweise ein Gerät im lokalen Gebäudeautomationsnetz missbraucht, um Angriffe gegen andere Netzwerkgeräte zu fahren (Port Scan, Denial-of-Service, Denial-of-Sleep etc.), kann dieses Gerät in Quarantäne gesetzt werden.

Sicheres Entfernen von Geräten

Nach vielen Sicherheitsanalysen und –anforderungskatalogen muss ein sicheres Entfernen von Geräten aus einem Netzwerk gewährleistet sein. Geräte enthalten sensible Daten wie Schlüsselmaterial, Autorisierungstokens oder Logdateien, die sich im Flashspeicher befinden und an Dritte gelangen können. Insbesondere sensibles Schlüsselmaterial muss bei Entsorgung des Geräts als kompromittiert angesehen werden. Da der Security Controller zu jeder Zeit eine digitale Kopie des Netzwerkstatus samt örtlicher Installation der Geräte pflegt, können bei Entfernen eines Geräts andere Netzwerkteilnehmer neu konfiguriert werden. Altes Schlüsselmaterial kann nicht mehr verwendet werden, um sich Netzwerkzugriff oder Zugriffsrechte auf Dienste zu verschaffen.

Gemäß Arbeitsplan konnte basierend auf aktuellen Sicherheitsstandards eine eigene Sicherheitsarchitektur entwickelt werden. Die Vorteile der Architektur basieren im Wesentlichen auf der Nutzung von Open-BIM und eines einheitlichen Kommunikationsbrokers (siehe Schwerpunkt 1).

Ergebnisverwertung

Die Kernergebnisse der beiden Schwerpunkte SP1 und SP2 mündeten in praktischen Implementierungen der Architekturkonzepte. Sie befinden sich in den folgenden öffentlichen Software-Repositories:

- SP1: Middleware-Architektur *Semantic Interoperability Layer:* https://gitlab.amd.e-technik.uni-rostock.de/Building-Automation/demo-semantic-interoperability-layer
- SP2: Algorithmus zur Partitionierung (Clustering) von GA-Netzwerken in isolierte Trust Zones: https://gitlab.amd.e-technik.uni-rostock.de/Building-Automation/demo-trust-zone-formation

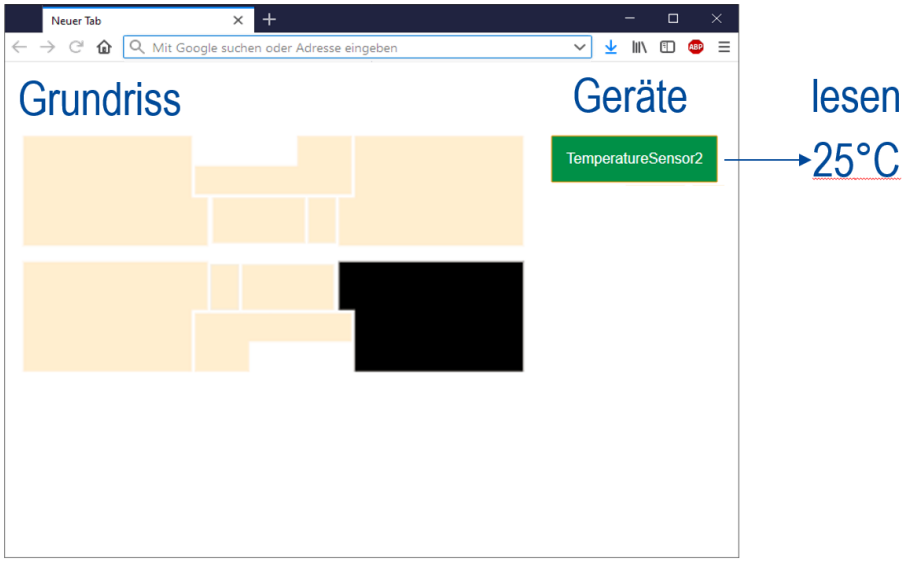
Das **erste Repository** enthält die Realisierung der GA-Middleware aus SP1 als prototypische Software-Lösung, welche plattformunabhängig oberhalb von Java- und Python-Laufzeitumgebungen ausgeführt werden kann. Zielgruppe des Demonstrators sind GA-Nutzer sowie Anwendungsentwickler, die die Verwendung einer solchen Interoperabilitätsschicht zur Erhöhung der Portabilität ihrer GA-Anwendungen anvisieren und eine Integration der entsprechenden Software-Schnittstellen erproben möchten.

Die Middleware besteht aus der zentralen Komponente des Brokers (inklusive Ontologie-Datenbasis) und mehreren Technologie-Gateways, welche zwischen einer grafischen Web-Anwendung (Webseite im HTTP-Browser) und zwei heterogenen GA-Endpunkten übersetzen. Im Demonstrator werden exemplarisch zwei Temperatursensoren genutzt, wobei einer mittels BACnet-IP und der andere mittels CoAP (Constrained Application Protocol) angesprochen wird. Beide Sensoren laufen als separate logische Server-Anwendungen auf einem Raspberry Pi als physisches Beispielgerät, während Broker und Technologie-Gateways sowie die Web-Anwendung auf einem herkömmlichen PC ausgeführt werden. Im Beispielaufbau sind PC und Raspberry Pi in einem lokalen Netzwerk (LAN) im gleichen IP-Subnetz miteinander verbunden. Die Realisierung des Brokers nutzt einen Python-basierten HTTP-Server sowie einen RDF/SPARQL-Server auf Basis des Frameworks Apache Jena Fuseki [6]. Die Realisierungen des BACnet Servers und Gateways (Proxy-Client) nutzen die Python-Bibliothek BACpypes. Der CoAP Server basiert auf unserem eigenen Java-Framework jCoAP, während das Gateway (Proxy-Client) mittels der Python-Bibliothek CoAPthon3 realisiert wurde.

Der Broker erhält eingangs seine Wissensbasis durch das Importieren von Ontologie-Beschreibungen der GA-Installation (vorliegend im RDF-Dateiformat), welche die Gerätefunktionen und deren räumliche Verortung enthalten. Im Beispiel-Demonstrator basiert das Datenmodell auf Sprachelementen der Ontologie DogOnt sowie einer Verknüpfung der beschriebenen Komponenten mit einem BIM-Modell, vorliegend als IfcOWL-Beschreigung. Die Web-Anwendung oberhalb der Middleware nutzt ein exemplarisches 2D-Gebäudelayout, das zuvor aus diesem BIM-Modell generiert wurde (siehe Abbildung 21). Mittels SPARQL-Anfragen, ausgelöst durch grafische Elemente der Web-Oberfläche, erhält die Web-Anwendung das benötigte Wissen über Art und Raumzugehörigkeit der Geräte im Gebäudeplan. Gezielte Anfragen der aktuellen Sensorwerte werden als HTTP-Anfragen an die BACnet/CoAP-Gateways (Proxy-Clients) gesendet, welche die Datenabfrage im jeweiligen, spezifischen GA-Protokoll durchführen und somit vor der Anwendungsebene verbergen.

6 https://jena.apache.org/documentation/fuseki2/

Abbildung 21: Web-Oberfläche der Beispielanwendung im Middleware-Demonstrator



Quelle: IMD, Universität Rostock

Das **zweite Repository** enthält eine prototypische Implementierung zur Demonstration des in SP2 entwickelten Partitionierungsalgorithmus zur Bildung von vertraulichen Teilnetzen in GA-Installationen (Trust Zones). Der Software-Prototyp ist als Java-Realisierung plattformübergreifend lauffähig. Der Partitionierungs-Algorithmus stellt eine Kernkomponente der modellbasierten, sicheren Kommissionierung der GA durch den in SP2 beschriebenen Security Controller (SC) dar, wie sie im Abschnitt „Kommissionierung von Endgeräten“ im Detail vorgestellt wurde. In der Beispiel-Implementierung wird zur Vereinfachung ein Gebäude-Stockwerk als 2D-Ebene angenommen, in dem eine konfigurierbare Anzahl an Endgeräten zufällig platziert wird. Eine Teilmenge dieser Endgeräte wird als logisch miteinander verknüpft angesehen und vorgegeben, wobei dieses Vorwissen stellvertretend für eingangs bekannte, anwendungsabhängige Geräteverknüpfungen ist, welche z. B. aus Anwendungsgraphen extrahiert werden können (siehe Abschnitt „Erstellung und Verifikation der Anwendungsebene“). Im Demonstrator-Beispiel erfolgt ausgehend von dieser logisch verknüpften Teilmenge an Geräten eine Auswahl weiterer Trust-Zone-Knoten anhand des Standorts und somit deren „geeigneter Platzierung“ zwischen den vorgegebenen Anwendungsknoten. Der Installationsort der Geräte ist dem Security Controller bekannt (in der Praxis z. B. aus dem verknüpften BIM- und Ontologie-Wissen der Middleware aus SP1) und die physische Nähe zwischen Geräten begünstigt deren Zuordnung in dieselbe Trust Zone. Dabei handelt es sich in realen Szenarien beispielsweise um einen gleichen Zutrittsbereich, der durch Raumgrenzen klar getrennt werden kann. Als weiterer Parameter kann in der Beispielimplementierung eine „Korridorbreite“ zwischen Gerätepaaren variiert werden, innerhalb der die Auswahl weiterer Verbindungsknoten zur Gerätegruppe erfolgen soll (siehe Konzept in Abschnitt „Policy-basierte Bildung von Trust Zones“). Als Ergebnisse der Ausführung des Algorithmus im simulierten Netzwerk-Szenario wird einerseits dessen Laufzeit zur Vervollständigung der Trust Zone durch zusätzliche Verbindungsknoten in Abhängigkeit von der Gesamtanzahl an Geräten ermittelt, andererseits wird der prozentuale Anteil hinzugezogener Geräte in Abhängigkeit von der Korridorbreite bestimmt.

Die Prototyp-Implementierung dient als Ausgangspunkt für die Integration und Erprobung von weiterführenden Sicherheits-Policies, welche in der Praxis durch Sicherheitsexperten vorgegeben werden können. Beispielsweise ist eine Konfiguration von Geräteklassen und Sicherheits-Level über Attribute denkbar, auf deren Basis eine automatisierte Vorauswahl von Trust-Zone-Kandidaten erfolgen kann. Zielgruppe des Demonstrators sind Experten mit realen GA-Daten aus der Praxis (Gebäudepläne, Geräteverteilungen, Zutrittsbereiche), die künftig neben dem reinen Geräte-Standort im Rahmen von Policies integriert werden könnten.

Das Konzept von Schwerpunkt 2, sämtliche Geräte durch einen zentralen Security Controller zu konfigurieren, wurde zudem in Form einer wissenschaftlichen Publikation mit dem Titel „Software-Defined Security Architecture for Smart Buildings using the Building Information Model“ auf der Konferenz IEEE GCIoT 2019 präsentiert und mit Fachpublikum diskutiert [13]. Der Algorithmus zur Partitionierung des Netzwerkes auf Basis des BIM in Verbindung mit Gerätemetadaten wurde im Paper „Trust Zone Formation for Building Automation Networks using Building Information Modeling“ präsentiert. Die Publikation findet sich in den Proceedings der Konferenz IEEE GCAIoT 2020 [27].

Fazit

Das Forschungsprojekt konnte zeigen, dass sich Anwendungen für Gebäudeautomations (GA)-Systeme allgemeingültig formulieren und auf eine reale Installation abbilden lassen. Dazu werden GA-Datenmodelle inklusive dem Gebäudemodell (Building Information Model - BIM) geschickt miteinander verknüpft, um maschinell lesbare Geräte-, Daten- und Funktions-Beschreibungen zu schaffen, die von gebäudespezifischen Datenpunkten abstrahieren.

Ergebnis von Schwerpunkt 1 des Projekts ist eine Middleware-Architektur, die GA-Anwendungen (z. B. Klimasteuerung) eine technologie- und herstellerunabhängige Schnittstelle auf das GA-System zur Verfügung stellt und somit den Implementierungsaufwand für Anwendungen senkt sowie deren Portabilität stark erhöht. Die Konzepte wurden in Form von Software-Lösungen implementiert und in praktischen Testaufbauten evaluiert. Reale BACnet- und CoAP-Geräte, die an ein exemplarisches Gebäudemodell annotiert worden sind, lassen sich von einer Weboberfläche aus ansteuern. Die Interfaces zwischen den entwickelten Komponenten basieren auf dem offenen HTTP-Standard, sodass eine modulare Erweiterung und Anpassung möglich ist.

Des Weiteren haben die Arbeiten im Schwerpunkt 2 gezeigt, wie globales Wissen über die Gebäudeautomationsanlage – bereitgestellt durch die in Schwerpunkt 1 entwickelte Middleware – genutzt werden kann, um einen verbesserten Schutz gegen Computersabotage zu erzielen. Hierbei fungiert ein sogenannter Security Controller (SC) als eigenständige Anwendung oberhalb der Middleware und realisiert eine sichere Kommissionierung und Konfiguration des GA-Systems. Wichtige Informationen über die Gebäudestruktur (BIM) und GA-Installation in Kombination mit universellen Sicherheitsrichtlinien (Policies) und Anwendungswissen (logische Verknüpfung von Geräten) dienen als Grundlage für einen Partitionierungsalgorithmus, der jedes Gerät in einen geschützten Netzwerkbereich gruppiert. Innerhalb eines solchen Bereichs (Trust Zone) können die eigentlichen Anwendungen (Klimasteuerung etc.) ausgeführt und Daten redundant gesichert gespeichert werden. Neben den sicherheitskritischen Entscheidungen des Partitionierungsalgorithmus werden formal beschriebene Anwendungsgraphen auf ihre Korrektheit (Widerspruchsfreiheit) verifiziert und an jedes Endgerät über einen abgesicherten Kanal (Vertraulichkeit, Integrität und Authentizität) übertragen. In Form einer praktischen Realisierung wurde der geringe Implementierungsaufwand für zusätzliche Gerätefunktionalitäten gezeigt. Der Partitionierungsalgorithmus kann aufgrund seiner linearen Laufzeitkomplexität auch größere Netzwerke bewältigen.

Das Sicherheitskonzept aus Schwerpunkt 2 profitiert unmittelbar von der Middleware-Architektur aus Schwerpunkt 1, da die Implementierung der Sicherheitsmechanismen des Security Controllers (SC) auf Anwendungsebene technologieunabhängig gestaltet werden können. Der SC und dessen Aufgaben sind stellvertretend auch für andere GA-Anwendungen, die folglich auf höherer Abstraktionsebene arbeiten und somit portabel gehalten werden können. Zwar sind die Funktionen des SC nicht zwangsweise angewiesen auf die Abstraktion durch eine einheitliche Ontologie und deren Bündelung durch eine Middleware- und Gateway-Architektur. Der Implementierungsaufwand für den SC würde sich jedoch ohne diese Entkopplung stark erhöhen und seine Portabilität erheblich verringern, da verschiedene heterogene GA-Technologien direkt vom SC unterstützt werden müssten, z. B. für Discovery-Funktionen und zur Konfiguration der Geräte. Ebenso wäre eine Verknüpfung der individuellen Gebäudeinformationen (BIM) und GA-Modelle direkt auf der Anwendungsebene des SC erforderlich, sodass dieser für unterschiedliche Einsatzszenarien und Gebäudetypen angepasst werden müsste. Die Delegation der Informationsbereitstellung und zugehöriger Protokoll-Übersetzungsfunktionen an die GA-Middleware führt zur Abstraktion und klaren Aufgabenteilung, sodass universellere GA-Anwendungen entwickelt werden können.

Mitwirkende

Autorinnen und Autoren

Wall, Arne (Institut für Angewandte Mikroelektronik und Datentechnik, Universität Rostock)

Butzin, Björn (Institut für Angewandte Mikroelektronik und Datentechnik, Universität Rostock)

Rethfeldt, Michael (Institut für Angewandte Mikroelektronik und Datentechnik, Universität Rostock)

Timmermann, Dirk (Institut für Angewandte Mikroelektronik und Datentechnik, Universität Rostock)

Verzeichnisse

[1] M. Bermudez-Edo, T. Elsaleh und P. Barnaghi, „IoT-Lite Ontology," 4 Juni 2017. [Online]. Available: http://iot.ee.surrey.ac.uk/fiware/ontologies/iot-lite.

[2] ETSI, „Smart Appliances REFerence (SAREF) ontology," 10 Februar 2015. [Online]. Available: https://sites.google.com/site/smartappliancesproject/ontologies/reference-ontology.

[3] ETSI, „TS 103 410-3: Smart Appliances Extension to SAREF Part 3: Building Domain," Sophia Antipolis Cedex, 2017.

[4] A. Haller, K. Janowicz, S. Cox, D. L. Phuoc, K. Taylor, M. Lefrançois, R. Atkinson, R. García-Castro, J. Lieberman und C. Stadler, „Semantic Sensor Network Ontology," 19 Oktober 2017. [Online]. Available: https://www.w3.org/TR/vocab-ssn/.

[5] A. Zimmermann, E. Siira, T. Ghariani, M. Girod-Genet, G. Santos, F. Silva, L. Temal, B. Teixeira, H. Järvinen und J. Kalaoja, „SEAS Ontology," 29 August 2017. [Online]. Available: https://ci.mines-stetienne.fr/seas/index.html.

[6] Brick Consortium, „Brick v1.0.3," [Online]. Available: https://brickschema.org/ontology.

[7] Automation Systems Group - TU Wien, „ThinkHome Ontology," 2013/2014. [Online]. Available: https://www.auto.tuwien.ac.at/downloads/thinkhome/ontology/.

[8] P. Pauwels und W. Terkaj, „EXPRESS to OWL for construction industry: towards a recommendable and usable ifcOWL ontology.," in Automation in Construction 63: 100-133, 2016.

[9] D. Bonino und L. D. Russis, „DogOnt," 2008. [Online]. Available: http://iot-ontologies.github.io/dogont/.

[10] V. Charpenay, S. Käbisch, D. Anicic und H. Kosch, „An Ontology Design Pattern for IoT Device Tagging Systems," in 5th International Conference on the Internet of Things (IoT), Seoul, 2015.

[11] D. Schachinger, „colibri," 2016. [Online]. Available: https://github.com/dschachinger/colibri.

[12] T. Stavropoulos, D. Vrakas, D. Vlachava und N. Bassiliades, „BOnSAI: A smart building ontology for ambient intelligence," in ACM International Conference Proceeding Series, 2012.

[13] A. Wall, B. Butzin, F. Golatowski, M. Rethfeldt und D. Timmermann, „Software-Defined Security Architecture for Smart Buildings using the Building Information Model," in IEEE Global Conference on Internet of Things, Dubai, 2019.

[14] A. Wall, Modellbasierte, sichere Service- und Netzwerkkonfiguration in der Gebäudeautomation, Rostock: Dissertation, Einreichung voraussichtlich 2022.

[15] A. Wall, H. Raddatz, M. Rethfeldt, P. Danielis und D. Timmermann, „ANTs: Application-Driven Network Trust Zones on MAC-Layer in Smart Buildings," in 15th Annual IEEE Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2018.

[16] A. Wall, H. Raddatz, M. Rethfeldt, P. Danielis und D. Timmermann, „Performance Evaluation of MAC-Layer Trust Zones over Virtual Network Interfaces," in 4th Conference On Mobile And Secure Services (MobiSecServ), Miami Beach, Florida, USA, 2018.

[17] S. Unger und D. Timmermann, „Bridging the Gap for Authentication in Smart Environments," in 19th IEEE Symposium on Computers and Communications (IEEE ISCC), Funchal, Portugal, 2014.

[18] M. Hellman und W. Diffie, „New directions in cryptography," IEEE Transactions on Information Theory, Bd. 22, Nr. 6, pp. 644-654, 1976.

[19] IEEE, IEEE 802.1AE-2006: IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security, 2006.

[20] J. Case, M. Fedor, M. Schoffstall und J. Davin, RFC 1157: A Simple Network Management Protocol (SNMP), 1990.

[21] M. Rethfeldt, A. Wall, P. Danielis, B. Konieczek und D. Timmermann, „AKadeMesh: Software-Defined Overlay Adaptation for the Management of IEEE 802.11s Networks," in 13th IEEE Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2016.

[22] S. Bari, F. Anwar und M. H. Masud, „Performance study of hybrid Wireless Mesh Protocol (HWMP) for IEEE 802.11s WLAN mesh networks," in International Conference on Computer and Communication Engineering (ICCCE), 2012.

[23] R. G. Garroppo, S. Giordano und L. Tavanti, „A joint experimental and simulation study of the IEEE 802.11s HWMP protocol and airtime link metric," in Int. J. Commun. Syst., 2012.

[24] A. Wall, V. Altmann, J. Müller, H. Raddatz und D. Timmermann, „Decentralized Configuration of Embedded Web Services for Smart Home Applications," in 11th Annual IEEE International Systems Conference (SYSCON), Montreal, Quebec, Kanada, 2017.

[25] OMA, „Open Mobile Alliance (OMA) SpecWorks," [Online]. Available: https://omaspecworks.org/. [Zugriff am 11 11 2021].

[26] H. Raddatz, M. Rethfeldt, M. Kasparick, A. Wall und D. Timmermann, „Absicherung der Gerätekommunikation im Smart Home unter Verwendung des Schutzprofils für Smart Meter Gateways," Fraunhofer IRB Verlag, Abschlussbericht Forschungsinitiative Zukunft Bau, Band F 3081, 2018.

[27] A. Wall, B. Butzin und D. Timmermann, „Trust Zone Formation for Building Automation Networks Using Building Information Modeling," in IEEE Global Conference on Artificial Intelligence and Internet of Things (GCAIoT), Dubai, United Arab Emirates, 2020.

[28] D. Ongaro und J. Ousterhout, „In search of an understandable consensus algorithm," in USENIX Annual Technical Conference, USA, 2014.

[29] J. Skodzik, V. Altmann, P. Danielis, A. Wall und D. Timmermann, „A Kad Prototype for Time Synchronization in Real-Time Automation Scenarios," in World Telecommunications Congress, Berlin, Deutschland, 2014.

Abbildungsverzeichnis

Abbildung 1: Übersicht bestehender Ontologien und deren Abhängigkeiten 12
Abbildung 2: Middleware-Architektur für GA-Netzwerke 14
Abbildung 3: Sicherheitsarchitektur aus Schwerpunkt 2 15
Abbildung 4: Ausweitung eines Angriffs auf weitere verwundbare Geräte 17
Abbildung 5: Angriff auf einzelne Trust Zone beschränkt 18
Abbildung 6: Ablauf der Kommissionierung eines Gerätes durch eine/n Nutzer/in (z. B. Techniker/in) 20
Abbildung 7: Ende-zu-Ende Sicherheit im Konfigurationsnetz zwischen Security Controller und Endgeräten 21
Abbildung 8: Zustandsautomat eines Endgeräts 22
Abbildung 9: Vom Security Controller ausgeführtes Programm zur Kommissionierung verschiedener Gerätetypen 23
Abbildung 10: Abfrage der Routingtabelle eines Endgerätes durch den Security Controller 25
Abbildung 11: Zweistufige Sensor-Aktor-Beziehung 27
Abbildung 12: Dreistufige Sensor-Aktor-Beziehung 28
Abbildung 13: Mapping von Anwendungen auf Geräte und Bildung von Trust Zones 29
Abbildung 14: Akquirierung von Infrastrukturknoten 30
Abbildung 15: Geräte, die sich in der Umgebung der Verbindungslinien zwischen Sensor, Aktor und Steuereinheit befinden, werden als mögliche weitere Trust Zone Knoten ausgewählt 31
Abbildung 16: GA bestehend aus 100 Geräten: Optimierter Algorithmus zur Auswahl von Trust Zone Kandidaten 32
Abbildung 17: GA bestehend aus 1000 Geräten: Optimierter Algorithmus zur Auswahl von Trust Zone Kandidaten 32
Abbildung 18: Anteil an Geräten als Trust Zone Kandidaten in Anhängigkeit von der Korridorbreite 33
Abbildung 19: Ausführungszeit des Partitionierungsalgorithmus 34
Abbildung 20: Geräte-/Regel-Konfiguration durch eine/n Nutzer/in 35
Abbildung 21: Web-Oberfläche der Beispielanwendung im Middleware-Demonstrator 39

Tabellenverzeichnis

Tabelle 1: Übersicht der Phasen des Konzeptes zur Kommissionierung und Konfiguration von GA-Netzwerk und -Geräten 18

Tabelle 2: RESTful API des Konfigurationsservices 26