Sicherheit in Cyber Physical Systems

Grundprojekt Ausarbeitung

Sascha Waltz

Sommersemester 2016

HAW Hamburg

Zusammenfassung. Das Ziel dieser Ausarbeitung ist es, einen Einblick in die Projektarbeit des Grundprojektes zu liefern. Hierfür sollen Grundlagen im Bereich Internet of Things, Cyber-Physical Systems und in diesem Zusammenhang auch IT-Security analysiert werden. Anschließend wird die Umsetzung des Projektes und die Umgebung dafür beleuchtet.

1 Einleitung

Dieser Abschnitt der Ausarbeitung dient dazu, die Motivation hinter dem Projekt und den Aufbau der Ausarbeitung darzulegen.

1.1 Motivation

Die Interaktion mit alltäglichen Dingen wird immer mehr in digitale Umgebungen verlagert. Immer mehr physische Dinge werden durch Erweiterungen, Module und Sensoren in der digitalen Welt abgebildet und zum Zugriff über das Internet, Netzwerke oder andere Schnittstellen verfügbar gemacht. Diese Digitalisierung ermöglicht immer mehr steuerbare oder zugreifbare Geräte. Diese Geräte sind teilweise auch kritische Systeme, die nicht von unautorisierten Personen genutzt werden dürfen. Für diese Systeme müssen Maßnahmen ermöglicht werden, um den unberechtigten Zugriff zu unterbinden und autorisierten Personen oder Systemen eben diesen Zugriff zu ermöglichen. Diese Authentifizierung soll dabei möglichst schnell und unkompliziert ablaufen, nach Möglichkeit ohne das Eingreifen eines Benutzers. Mit diesem Projekt soll eine Plattform hierfür geschaffen werden.

1.2 Aufbau der Ausarbeitung

Diese Ausarbeitung wird sich zunächst mit der Analyse des Internets der Dinge und Cyber-Physical Systems befassen. Dazu kommt die Interaktion und Kommunikation mit solchen Systemen. Das dritte Kapitel befasst sich mit Safety und

Security im IT-Bereich. Kapitel Vier beschreibt dann die Umsetzung des Projektes samt Zielen, dem geplanten Aufbau der Plattform, der Projektumgebung und der Evaluation des Projekts. Das abschließende Kapitel beinhaltet ein Fazit und den Ausblick auf das Hauptprojekt.

2 Analyse

Dieser Abschnitt befasst sich mit der Analyse der gegebenen Situation und dem Ist-Zustand in der heutigen Welt. Außerdem wird die Umgebung beschrieben, ich der die Projektarbeit durchgeführt wurde.

2.1 Das Internet der Dinge

Das „*Internet der Dinge (engl. Internet of Things, IoT)*“ wächst in den letzten Jahren stetig weiter und beinhaltet immer mehr in der Virtualität abgebildete Objekte. Somit wird die Informationslücke zwischen der realen und der virtuellen Welt immer weiter geschlossen. Diese „*Cyber-Physical-Systems (CPS)*“ sind alltägliche Dinge, von Kaffeetassen bis zu komplexen Fertigungsanlagen, die sich heutzutage detailliert erfassen und in Form von Daten darstellen lassen. Hierzu sind Sensoren und Schnittstellen nötig, welche Daten erfassen und weiterleiten bzw. zur Verfügung stellen können.
Das IoT stellt ein riesiges Netzwerk dar, in dem viele Geräte miteinander kommunizieren, ohne dass ein Mensch darauf Einfluss nehmen kann oder muss. Daten werden ausgetauscht, ausgewertet und genutzt um auf bestimmte Situationen oder Gegebenheiten zu reagieren. Beispielsweise können Umwelteinflüsse schneller registriert und Alarm ausgelöst werden, der Straßenverkehr wird analysiert und nach der Auswertung die Ampeln entsprechend geschaltet oder der Kühlschrank stellt fest, dass ein Lebensmittel zur Neige geht und bestellt dieses selbstständig nach. Dies sind nur einige banale Beispiele für alltägliche Abläufe im Internet der Dinge.

2.2 Cyber-Physical-Systems

Cyber-Physical-Systems ist ein sich immer weiter verbreitender und auch passenderer Begriff für physische Systeme, welche mit der informationstechnischen Welt verbunden sind und eine enge Zusammenarbeit zwischen diesen beiden Welten ermöglichen. Diese Systeme sind in der Lage, durch Sensoren physikalische Daten zu erfassen, zu verarbeiten und über digitale Netze bereitzustellen. Außerdem können sie Daten und Dienste nutzen sowie Schnittstellen zur Verfügung stellen, die zur Kommunikation und Steuerung genutzt werden können. (vgl. [8] S. 22)
Unter den Cyber-Physical-Systems finden sich auch die eingebetteten Systeme und vernetzte eingebettete Systeme, diese bilden die Grundlage für Cyber-Physical-Systems, da sie in einen technischen Kontext eingebunden sind und dank globaler Datennetze sind sie gleichzeitig verteilt und vernetzt. Abbildung 1 zeigt den Zusammenhang der eingebetteten Systeme, den Cyber-Physical-Systems und dem

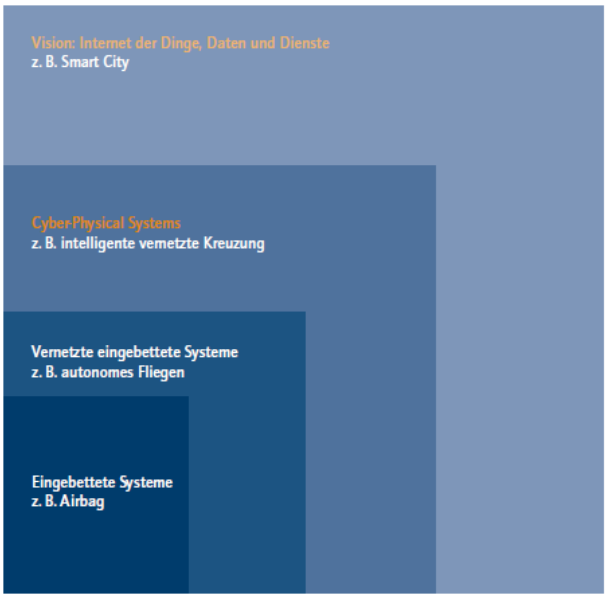


Abb. 1. Aufbau von eingebetteten System zum Internet der Dinge [8]

Internet der Dinge. Des Weiteren spielt die Entwicklung weiterer Technologien eine wesentliche Rolle für Nutzung von CPS. Zum einen wäre da das allgegenwärtige Computing (Ubiquitous Computing), bei dem in der physischen Umgebung Computer eingebettet werden und ihre Arbeit verrichten, ohne dass die Umgebung dies direkt wahrnimmt. Zum Anderen lassen die Nutzung des Internets für Wartungs- und Verwaltungsaufgaben und die Nutzung des semantischen Webs zum Aufbau von Wissens- und Kommunikationsnetzen sowie Communities eine immer einfachere Interaktion von Nutzern und Cyber-Physical-Systems zu.
So lassen sich diverse neuartige Funktionen, Dienste und Eigenschafen in eingebetteten Systemen schaffen, die eine weitaus größere Vielfalt an Möglichkeiten als die bisherigen Systeme bieten.

2.3 Möglichkeiten von Cyber-Physical-Systems

Grundsätzlich kann ein Cyber-Physical-System sämtlichen Einfluss auf die physische Umgebung ausüben, der ihm durch seine Beschaffenheit und die vernetzten, steuerbaren Geräte möglich ist. Sensoren können die Daten erfassen, die durch ihren Aufbau erfassbar sind und Aktoren reagieren entsprechend und geben Steuersignale an Maschinen oder Benutzeroberflächen weiter. Durch die Verbindung verschiedener Cyber-Physical-Systems entstehen für nahezu jeden Anwendungs- oder Problembereich Systeme und Lösungen die immer neue Möglichkeiten bieten. Ob im medizinischen Bereich, in Kraftwerken oder in autonom arbeitenden Fabriken, in jeder Umgebung ist die Arbeit von CPS möglich und meist auch

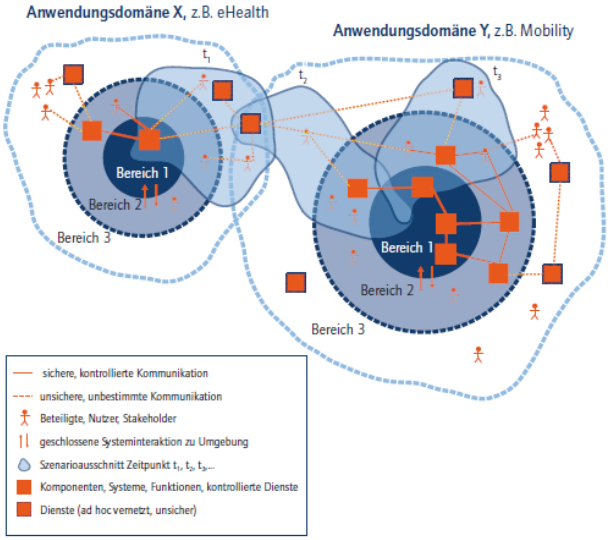


Abb. 2. Schematische Darstellung der domänenübergreifenden Integration von Cyber-Physical Systems [1]

äußerst sinnvoll. Die Verbindung von Internet, Echtzeit-Computer-Systemen und industriellen Prozessen ist hier ein typisches Merkmal und machen moderne vernetzte industrielle Infrastrukturen zu Cyber-Physical-Systems (vgl. [2]).
Die domänenübergreifenden Integration von CPS macht die Zusammenarbeit verschiedener Systeme in unterschiedlichen Anwendungsgebieten möglich und lässt den Daten- und Informationsaustausch zwischen diesen Systemen zu. Um Informationen aus unterschiedlichen Anwendungen verarbeiten zu können, muss eine semantische Kompatibilität gegeben sein, was bedeutet, dass alle Systeme Informationen in dem selben Format bereitstellen müssen, dass die gleichen Schnittstellen genutzt werden und dass Daten auf die gleiche Art interpretiert werden. (vgl. [1])
Um solche vernetzten CPS aufzubauen, müssen Nutzer und offene Systeme miteinander interagieren und es müssen alle Informationen verlässlich und verfügbar sein. Die Schwierigkeiten bei der Kommunikation zwischen mehreren CPS werden noch im folgenden Abschnitt aufgeführt.
Um diese Interoperabilität zu ermöglichen, werden Cyber-Physical-Systems idealer Weise in drei Schichten unterteilt, wie in Abbildung 3 dargestellt. Diese werden wie folgt aufgeteilt:

- **Akteure:** Nutzerprozesse oder -interaktionen über Dienste und Oberflächen, Nutzer interagieren über entsprechende Schnittstellen mit den einzelnen Systemen
- **Dienste:** Dienste verarbeiten und stellen die Daten bereit, je nach Bedarf des Nutzers oder des Systems

– **Domänenspezifische Plattform:** Die Plattform oder das eigentliche CPS liefert Daten, verarbeitet sie und kommuniziert mit anderen Systemen auf Grundlage seines Nutzungszwecks und seiner Beschaffenheit

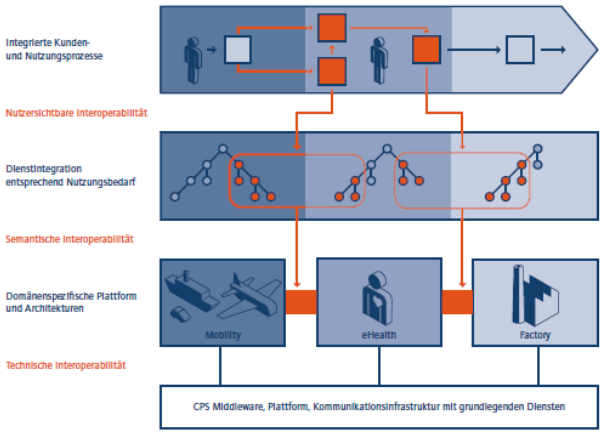


Abb. 3. Idealtypisches Schichtenmodell der Cyber-Physical Systems [1]

Der unterste Kasten stellt hierbei die notwendige Kommunikationsinfrastruktur in Form einer Middleware dar, über die Cyber-Physical-Systems miteinander auf gleicher Basis kommunizieren. Dieser Abschnitt gehört nicht mehr zu den drei angesprochenen Schichten sondern bildet ein eigenes System. Durch die vielfältigen Möglichkeiten zur Kommunikation ermöglichen Cyber-Physical-Systems eine umfassende Zusammenführung und Interpretation unterschiedlichster Aspekte (vgl. [3]). Durch den Einsatz in immer neuen Bereichen und dem Entstehen neuer Lösungen in den bereits erschlossenen Gebieten wird das Spektrum der Möglichkeiten stetig erweitert. Es werden immer neue Vernetzungsmöglichkeiten eröffnet, die bis dahin nicht zusammen gearbeitet haben.
Die Einsatzgebiete mit dem größten wirtschaftlichen Potential für Cyber-Physical-Systems werden voraussichtlich die folgenden (vgl. [3]):

– Produktion
– Medizintechnik
– Energienetze
– Eingebettete Systeme im Verkehr
– Comsumer Electronics

Auch alle weiteren Bereiche, in denen die Nutzung möglich ist, werden weiter ausgebaut und durch die immer feinere Vernetzung der einzelnen Systeme und dank der gegebenen Interoperabilität wachsen die Bereiche immer weiter zusammen und profitieren von den Daten der anderen.

Eine große Herausforderung für die Nutzung dieser Möglichkeiten ist die Bereitstellung der Daten in Echtzeit, so dass direkt darauf reagiert werden kann. Hierfür müssen die Daten entsprechend aufbereitet und Benutzern oder anderen Systemen direkt zur Verfügung gestellt werden, damit diese auf Veränderungen sofort reagieren können.
Zugleich sollen diese CPS auch noch robust, ausfallsicher und abgesichert sein. Die Verlässlichkeit der Daten spielt bei Cyber-Physical Systems eine sehr große Rolle, da fehlende, falsche oder veränderte Daten einen Ausfall des Systems bedeuten würden oder falsche Aktionen auslösen können. Zu den Details dieser Anforderungen wird in Unterabschnitt 3.2 weiter eingegangen.
Die größte Herausforderung bei der Nutzung aller Möglichkeiten von CPS ist das Vertrauen in das System. Hierbei kommen Zuverlässigkeit, Ablauf- und Ausfall-Sicherheit, Sicherheit vor unbefugtem Zugriff, Privatsphäre und Benutzerfreundlichkeit zusammen. (vgl. [11]) In einem CPS müssen alle diese Punkte zuverlässig abgedeckt sein und funktionieren.

2.4 Mobile Interaktion mit Cyber-Physical-Systems

Die Interaktion hat sich mit dem erhöhten Aufkommen von tragbaren Geräten wie Smartphones, Tablets oder inzwischen auch Wearables wie Augmented Reality Brillen stark verändert. Früher wurden Eingaben direkt per Tastatur und Maus am Gerät vorgenommen, heutzutage können wir nahezu von jedem beliebigen Ort auf Geräte zugreifen und diese Dank Internet und Netzwerken steuern. Die meisten Eingaben werden zur Zeit über Smartphones oder Tablets getätigt. Diese Geräte werden von fast jedem mit sich geführt und lassen sich schneller nutzen, was grade für kurze Eingaben oder Abfragen von Vorteil ist. Des Weiteren lassen sich hier nicht nur Tastaturen zur Eingabe nutzen, neben Sprachbefehlen sind auch noch Eingaben über die vielen verschiedenen Sensoren, beispielsweise eines Smartphones, möglich. Da diese Geräte sich sehr einfach mitführen lassen, sind auch ortsbasierte Dienste zur Interaktion denkbar.
Mit der Zeit haben sich verschiedene Interaktionskonzepte entwickelt, die eine möglichst einfache aber umfangreiche Interaktion ermöglichen sollen. Trotz allem gibt es weiterhin die Tastatur und auch eine Interaktion ähnlich der Eingabe mit einer Maus ist möglich, aber alles virtuell auf einem recht kleinen Bildschirm. Darüber hinaus hat sich eine recht adäquate Spracheingabe entwickelt, die auch sprecherabhängig umgesetzt sein kann, so dass nur bestimmte Personen Befehle über die Spracherkennung eingeben können. Eine weitere Möglichkeit ist die Eingabe bzw. Steuerung per Gesten auf dem Touch-Screen. Dank diverser Sensoren in Smartphones lassen sich auch Gesten mit dem Gerät selber durchführen und anhand der Beschleunigungssensoren nachvollziehen. Ebenso lassen sich die Kamera oder integrierte NFC (Near-Field-Communication) nutzen. Zur Standortbestimmung können sowohl GPS- als auch WLAN-Daten herangezogen werden um auf ein paar Meter genau zu bestimmen, wo sich das Gerät befindet. Die meisten mobilen Geräte besitzen inzwischen etwa 10 verschiedene Arten von Sensoren, auf die zurückgegriffen werden kann. Dazu kommen noch diverse

Möglichkeiten um die Befehle zu übermitteln, WLAN und Bluetooth sind hier die am häufigstens verwendeten Techniken. (vgl. [4, S. 196-207])

2.5 Kommunikation der Cyber-Physical-Systems

Die Kommunikation ist, wie im vorangegangenen Abschnitt erwähnt, ein essentieller Bestandteil von Cyber-Physical Systems. Der Datenaustausch, die Eingaben oder die Interaktion eines Benutzers, die Ausgabe von Steuerbefehlen oder das Abfragen von Sensoren, all das ist von Kommunikationsmöglichkeiten abhängig.
Um diese Kommunikation zu ermöglichen bedarf es der entsprechenden Schnittstellen, wie Ethernet, WLAN, Bluetooth oder ähnlichem. Der Datenaustausch erfolgt dann über das lokale Netzwerk oder, wie in den meisten Fällen, über das Internet. Im Allgemeinen unterscheidet man hier zwischen drahtgebundener und drahtloser Kommunikation.
Die Vernetzung der einzelnen Systeme stellt dabei eine enorme Herausforderung dar, da sie zur Entwicklungszeit eher statisch, im Betrieb aber dynamisch miteinander verbunden sind. Dazu kommt, dass die Virtualität der Cyber-Physical Systems voraussetzt, dass einzelne Systeme größtenteils sowohl unabhängig von Materialien, Orten und Geräten sind, als auch losgelöst von physikalischen Beschränkungen. Und dennoch erzeugen sie ein Bild der Realität in der virtuellen Welt. Die Ortsungebundenheit von Daten, Informationen und Diensten, ihre Unabhängigkeit von bestimmten Geräten oder Infrastrukturen ist dennoch für CPS enorm wichtig, um die Virtualität der Systeme zu gewährleisten (vgl. [1]).
Bei der Kommunikation offener Systeme treten einige Schwierigkeiten auf,

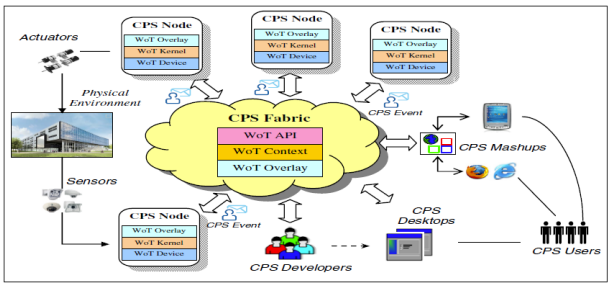


Abb. 4. Referenz-Architektur eines Cyber-Physical Systems [6]

angefangen bei der Semantik in der die Systeme miteinander kommunizieren. Die entstehenden Daten müssen zum einen sowohl von den Systemen als auch von Menschen les- und interpretierbar sein, was eine nahtlose Integration und Anpassung der Daten für Menschen als auch für physikalische Systeme erfordert (vgl. [6]). Hierzu müssen die Rohdaten, welche von den CPS erfasst werden zunächst aufbereitet (d.h. gesäubert, gefiltert, validiert, etc.) werden.

3 Safety und Security

In diesem Kapitel sollen die Unterschiede zwischen Safety und Security dargelegt und beschrieben werden, welche Aspekte es in dieser Hinsicht in CPS gibt.

3.1 Der Unterschied von Safety und Security

Sowohl Safety als auch Security werden im Deutschen mit Sicherheit übersetzt. Ursprünglich waren aber für beide Begriffe unterschiedliche Bedeutungen angedacht bzw. sind es im Englischen immer noch. Im IT-Umfeld sind die beiden Begriffe noch etwas enger abgegrenzt und auf Computer und Netzwerke zugeschnitten:

- **Safety** Mit dem Begriff "Safety" wird die Betriebssicherheit bezeichnet. Diese umfasst die funktionale Sicherheit der Maschine oder Anlage und den Schutz vor anormalem Betrieb. Es wird somit sichergestellt, dass ein reibungsloser Betrieb gewährleistet wird.
- **Security** Der Begriff "Security" bezeichnet den Schutz, der nötig ist, um die Betriebssicherheit sicher zu stellen. Hier werden alle Maßnahmen zusammengefasst, die erforderlich sind, um Beeinflussung oder Angriffe von außen auf Systeme zu verhindern. Aber auch ungewollt auftretende Fehler müssen hier abgefangen und behandelt werden.

Im großen Ganzen ist Security der Prozess, welcher nötig ist, um Safety zu gewährleisten. [9] Das Zusammenspiel dieser beiden Disziplinen ist daher extrem wichtig.
Zur Authentifizierung eines Benutzers werden in der Regel 3 Methoden genutzt:

- **Wissen** Der Benutzer muss beweisen, dass er Kenntnis von etwas hat, beispielsweise einem Passwort
- **Besitz** Der Benutzer ist im Besitz eines Gegenstandes, der ihn zu etwas berechtigt, etwa eines Schlüssels oder einer Keycard
- **Biometrie** Der Benutzer kann sich anhand körperlicher, eindeutiger Merkmale identifizieren, dem Fingerabdruck oder der Iris zum Beispiel

Es sind auch Kombinationen der einzelnen Methoden möglich um den Zugriff noch weiter abzusichern.

3.2 Sicherheit in Cyber-Physical-Systems

Die Sicherheit in Cyber-Physical Systems zu gewährleisten, stellt eine noch größere Herausforderung dar. Da hier oftmals diverse verteilte Systeme miteinander Kommunizieren, Daten austauschen oder sich gegenseitig steuern können, birgt ein nicht ordnungsgemäß funktionierendes System eine gravierende Schwachstelle für alle benachbarten Systeme.
Hier gilt es zunächst die einzelnen Systeme abzusichern und dann dafür zu sorgen, dass beim Austausch von Daten zwischen den verschiedenen Systemen keine Schwachstelle entsteht. Oftmals liegt hier der einfachste Angriffspunkt um

die Datenintegrität zu beeinflussen. Sobald die Korrektheit von Daten oder der Funktion eines Systems nicht mehr gewährleistet werden kann, ist das System beeinträchtigt und kann nicht genutzt werden, bis die Integrität wieder hergestellt ist.

Abb. 5. ThyssenKrupp Aufzugswartung per Microsoft Hololens

Grade die Interaktion mit kritischen Systemen, also solchen, die für Sicherheit von Anlagen oder Menschen verantwortlich sind, darf nur bestimmten Personen überhaupt möglich sein. Abbildung 5 zeigt ein Beispiel der Firma ThyssenKrupp, bei der ein Techniker auf eine Augmented-Reality-Schnittstelle zugreift um einen Fahrstuhl zu warten. Dieser Zugriff sollte natürlich nur einem entsprechendem Techniker gewährt werden, da sonst das System beeinträchtigt oder sogar Menschen zu Schaden kommen könnten. Also ist es unumgänglich festzustellen, dass nur die berechtigte Person Zugriff erhält als auch, dass die Daten während der Kommunikation nicht manipuliert werden. Die Absicherung der Kommunikation soll nicht Teil dieser Arbeit sein. Die Absicherung des Zugriffs an sich, geschieht, wie im vorherigen Abschnitt erläutert, über Wissen, Besitz oder Biometrie, die Abfrage und die Übermittlung der Daten sollen Teil dieses Projektes sein.

4 Umsetzung des Projektes

Dieser Abschnitt behandelt die Ziele und die Umsetzung des Projektes. Es wird dargelegt, welche Ziele erreicht werden sollten, wie das Projekt angegangen und umgesetzt wurde. welche Probleme auftauchten und welche Ergebnisse erzielt wurden.

4.1 Ziele

Die hauptsächlichen Ziele der Projekte sind es, eine Plattform zu schaffen, die genutzt werden kann, um den Zugriff auf Komponenten von Cyber-Physical-Systems zu beschränken bzw. ihn nur berechtigten Personen zu gewähren und die Authentifizierung hierbei möglichst automatisch ablaufen zu lassen, ohne dass der User selbst eingreifen muss. Es sollen mehrere Möglichkeiten zur Kommunikation in Betracht gezogen werden.

4.2 Aufbau der Plattform

Die Plattform, welche in diesen Projekten entsteht, soll es ermöglichen, eine einfache aber sichere Authentifizierungsmöglichkeit bei der Kommunikation mit Cyber-Physical-Systems zu ermöglichen. Dank der Kommunikation über eine Middleware, lassen sich die erforderlichen Maßnahmen zentral implementieren und müssen nicht für jedes Gerät angepasst oder neu entwickelt werden.
Die Kommunikation eines Users mit einem CPS-Gerät soll ablaufen wie in

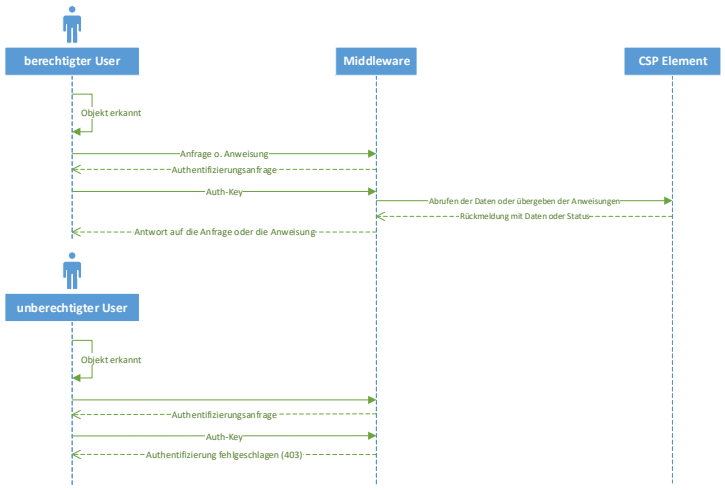


Abb. 6. Ablauf der Kommunikation zwischen User, Middleware und CPS

Abbildung 6 gezeigt:

- **Objekt erkennen** Der Benutzer identifiziert die CPS-Komponente mit dem er interagieren möchte anhand eines Tags an dem Gerät oder in dessen Umgebung. Dieser Tag enthält beispielsweise den Channel-Namen oder den Namen des Objektes, so werden keine Informationen über das Netz veröffentlicht und die Agenten der Middleware wissen dennoch, an welche Komponente die Nachrichten geschickt werden müssen. Die Erkennung der Tags wird im Hauptprojekt umgesetzt, an dieser Stelle wird davon ausgegangen, dass das Objekt schon bekannt ist.
- **Anfrage an das Gerät** Der Benutzer startet eine Interaktion mit der Komponente. Die kann eine Abfrage oder eine Eingabe sein, welche an die Middleware geschickt wird, da diese die Kommunikation verwaltet, wie in Unterabschnitt 2.5 bereits erwähnt.
- **Authentifizierungsanfrage** Die Middleware schickt dem User eine Anfrage mit der Bitte um eine Authentifizierung zurück.
- **Authentifizierung** Der Benutzer sendet (automatisch) eine Authentifizierung an die CPS-Komponente
- **Antwort auf die Anfrage** Die Middleware fragt im Falle einer positiven Authentifizierung die Daten von der CPS-Komponente ab und sendet diese zurück an den User. Ist die Authentifizierung fehlgeschlagen, werden keine Daten abgefragt und die Middleware sendet eine entsprechende Ablehnung an den Benutzer zurück.

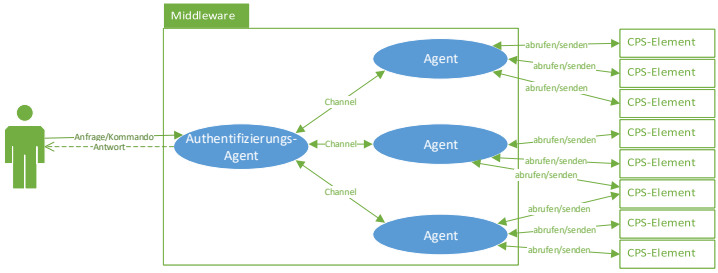


Abb. 7. Interaktion zwischen User, Middleware und CPS

Es wäre auch eine direkte Kommunikation mit CPS-Geräten denkbar, da aber in der Regel eine Middleware zum Einsatz kommt, wird auch in diesen Projekten von so einer Umgebung ausgegangen. Der Ablauf einer Interaktion ist in Abbildung 7 noch einmal schematisch dargestellt. Man erkennt hier, dass die Agenten in der Middleware die Kommunikation übernehmen, sowohl mit dem User als auch mit den angeschlossenen CPS-Geräten. Bei der erfolgreichen Authentifizierung des Benutzers leitet der Authentifizierungs-Agent die Anfrage

oder den Befehl an den entsprechenden Agenten weiter, welcher die Daten in dem Channel der CPS-Komponente abfragt oder veröffentlicht. In diesem Szenario muss die Kommunikation zwangsläufig über die Middleware stattfinden, damit die Authentifizierung zentral vorgenommen werden kann. Die Verbindungen vom User bzw. den CPS-Komponenten zu den Agenten soll verschlüsselt umgesetzt werden um die Sicherheit zu gewährleisten, die Kommunikation innerhalb der Middleware wird nicht Teil dieser Projekte, da diese schon implementiert ist (vgl. [7]).

4.3 Projekt- und Entwicklungsumgebung

Die Umsetzung dieses Projektes erfolgte in einem Forschungslabor der HAW-Hamburg, dem Creativ Space for Technical Innovations, kurz CSTI[1]. Hier werden unter Anderem Projekte mit den Schwerpunkten Smart Objects, Emotion Tracking Systeme, Virtual und Augmented Reality umgesetzt. In dieser Umge-

Abb. 8. Raumplan CSTI [5]

[1] CSTI - HAW Hamburg - http://csti.haw-hamburg.de; letzter Zugriff: 29.10.2017

bung lassen sich Projekte mit Smart Objects, also auch CPS-ähnliche-Systeme, gut umsetzen, da sowohl die Kommunikationsinfrastruktur incl. Middleware, als auch die Möglichkeit Objekte im Raum zu positionieren gegeben ist. Des Weiteren steht auch Hardware in Form von Raspberry Pi, Arduino, diversen Sensoren und Modulen zur Verfügung.
Zur Entwicklung der Agenten für die Middleware wurde die Sprache Scala[2] gewählt, da diese in den meisten anderen Agenten der Umgebung auch zum Einsatz kommt und Akka-Aktoren[3], welche für die Middleware benötigt werden, sich hier leicht implementieren lassen.
Das Akka-Framework implementiert das von C. Hewitt Mitte der 70er Jahre am MIT entwickelte Actor-Modell und ermöglicht so lose gekoppelte parallele Prozesse. Die Aktoren kommunizieren hierbei über Nachrichten, die in verschiedenen Kanälen verschickt werden. Ein Aktor reagiert hier nur auf Nachrichten, wenn sie ihn betreffen, alle anderen Nachrichten werden ignoriert.

4.4 Umsetzung

Für die Umsetzung des Projektes wurden zwei Raspberry Pi 3 ausgewählt, einer um die Authentifizierung vorzunehmen und einer um das Authentifizierungs-Token abzufragen und die angeforderten Daten bereitzustellen oder die gesendeten Befehle weiterzuleiten. Die Kommunikation erfolgte im Versuchsaufbau über Ethernet-Kabel und einen WLAN-Access-Point und einen Router zwischen zwei Netzwerken, wie in Abbildung 9 dargestellt. Auf beiden Raspberry Pi ist das auf

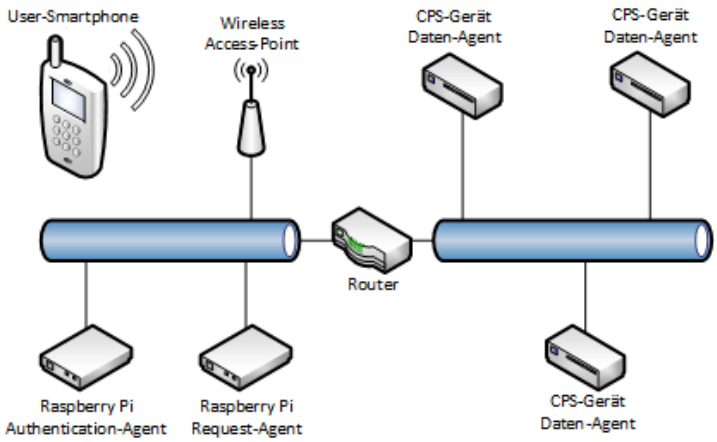


Abb. 9. Projektaufbau mit Raspberry Pi und Ethernet

[2] Scala Programmiersprache - http://www.scala-lang.org/; letzter Zugriff: 29.10.2017
[3] Akka-Framework - https://akka.io; letzter Zugriff: 29.10.2017

Debian basierende Betriebssystem Raspbian[4], welches für den Betrieb auf dem Raspberry Pi optimiert ist, auf 8GB Speicherkarten installiert.
Auf jedem Raspberry Pi läuft ein Akka-Agent, welcher seiner jeweiligen Aufgabe nachgeht und bei Anfrage eines Benutzers die Authentifizierung durchführt und dem User ein Token ausstellt und bei Vorlage des Tokens dann Daten austauscht.
Der Benutzer greift im Projektaufbau per Android-Smartphone auf das kleine CPS zu und fragt Daten beispielsweise von verschiedenen Sensoren ab. Der Aufbau der Sensoren wurde im Projekt nicht umgesetzt, dafür gibt der Anfrage-Agent seine Reaktionen auf die Nachrichten des Benutzer-Smartphones aus, um kontrollieren zu können, dass die Reaktionen korrekt sind.
Das Smartphone des Benutzers wird über WLAN in das Netzwerk gebracht um mit den Agenten zu kommunizieren. Weitere Kommunikationswege wurden im Grundprojekt nicht umgesetzt, aber Smartphone als auch der Raspberry Pi bieten Bluetooth zur Kommunikation, mit Hilfe von Modulen oder Arduinos können auch einfach Nahbereichskommunikationsmethoden angeschlossen werden, z.B. NFC, oder iBeacons. Diese Techniken können aber auf die gleiche Weise funktionieren und mit den Agenten kommunizieren.

4.5 Evaluierung

Die Evaluierung des Projektes geschieht anhand von gängigen Prozessen und Methoden, die seit Jahren etabliert sind. So zum Beispiel die Authentifizierung mit Kerberos[5] die auf einem Verfahren beruht, ähnlich dem in Unterabschnitt 4.2 beschriebenen. Die Nachrichten 1 und 2 sind hier Authentication Server Request und Reply, die Nachrichten 3 und 4 sind dann die eigentlichen Application Request und Reply, in denen die Anfragen des Clients mit und die angeforderten Daten ausgetauscht werden.
Des Weiteren wird das Akka-Framework eingesetzt, welches seit Jahren in komplexen Serveranwendungen zum Einsatz kommt und dank Nebenläufigkeit durch sein Nachrichtensystem und Robustheit im Umgang mit Fehlern eine solide Basis für das System darstellt.

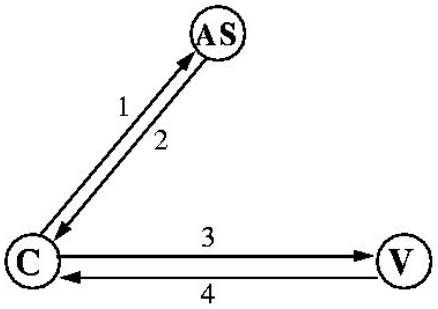
5 Fazit

Das abschließende Kapitel umfasst eine kurze Zusammenfassung dieser Ausarbeitung, sowie einen Ausblick auf das Hauptprojekt.

5.1 Zusammenfassung

In den vorangegangenen Kapiteln wurde beschrieben, welche Voraussetzungen für eine sichere Authentifizierung im Rahmen von Cyber-Physical Systems benötigt

[4] Raspbian - http://www.raspbian.org; letzter Zugriff: 07.11.2017
[5] Kerberos: An Authentication Service for Computer Networks - http://gost.isi.edu/publications/kerberos-neuman-tso.html; letzter Zugriff: 29.10.2017



1. as_req: c, v, $time_{exp}$, n
2. as_rep: $\{K_{c,v}$, v, $time_{exp}$, n, ...$\}K_c$, $\{T_{c,v}\}K_v$
3. ap_req: $\{ts,ck, K_{subsession}$, ...$\}K_{c,v}$ $\{T_{c,v}\}K_v$
4. ap_rep: $\{ts\}K_{c,v}$ (optional)

$T_{c,v} = K_{c,v}$, c, $time_{exp}$ ...

Abb. 10. Vereinfachte Darstellung des Kerberos-Protokolls (vgl. [10])

werden. Hierzu wurde beleuchtet, wie Cyber-Physical Systems arbeiten und kommunizieren, sowohl untereinander als auch mit Befehlen von außen. Es wurde auf den generellen Einsatz einer Middleware zur Kommunikation eingegangen und erläutert, wozu diese notwendig ist. Des Weiteren wurde auf Sicherheitsaspekte hingewiesen, die beachtet werden müssen und welche Unterschiede zwischen Safety und Security bestehen. Zuletzt wurde der Aufbau und die Umgebung des Projektes erläutert und anhand aktueller gängiger Konzepte die Machbarkeit dargelegt.

5.2 Ausblick

Nach der Herausarbeitung der Machbarkeit der Security-Infrastruktur für Cyber-Physical Systems soll im Hauptprojekt auf weiterführende Konzepte eingegangen und diese auch umgesetzt werden. Das immer aktueller werden Thema “Blended Reality“ bringt noch weitere, modernere Bedienkonzepte mit sich, ebenso wie neue Eingabegeräte.
So soll auch die Interaktion mit CPS über VR/AR Schnittstellen im Hauptprojekt betrachtet werden. Die Abbildung von physischen Geräten in virtuellen Welten macht auch hier die Bedienung möglich und das hier erläuterte Konzept muss auch für diese Bedienkonzepte funktionieren. Um auch AR-Brillen oder ähnlichen Wearables eine einfache Bedienung zu ermöglichen, sollte die Authentifizierung hier möglichst automatisch passieren, ohne dass der Benutzer zusätzlich interagieren muss.

Literatur

1. acatech (ed.): Cyber-Physical Systems — Merging the Physical and Virtual Worlds, pp. 15–21. Springer Berlin Heidelberg, Berlin, Heidelberg (2011), http://dx.doi.org/10.1007/978-3-642-29090-9_4
2. Akkaya, I., Liu, Y., Lee, E.A.: Modeling and Simulation of Network Aspects for Distributed Cyber-Physical Energy Systems, pp. 1–23. Springer Berlin Heidelberg, Berlin, Heidelberg (2015), http://dx.doi.org/10.1007/978-3-662-45928-7_1
3. Broy, M. (ed.): Einleitung, pp. 13–15. Springer Berlin Heidelberg, Berlin, Heidelberg (2010), http://dx.doi.org/10.1007/978-3-642-14901-6_1
4. Butz, A., Krüger, A.: Mensch-Maschine-Interaktion. De Gruyter Studium Series, Walter de Gruyter GmbH, 2. auflage edn. (2017)
5. CSTI: Csti-raumplan (2016), http://csti.haw-hamburg.de/projekt/
6. Dillon, T., Chang, E., Singh, J., Hussain, O.: Semantics of Cyber-Physical Systems, pp. 3–12. Springer Berlin Heidelberg, Berlin, Heidelberg (2012), http://dx.doi.org/10.1007/978-3-642-32891-6_3
7. Eichler, T.: Agentenbasierte Middleware zur Entwicklerunterstützung in einem Smart-Home-Labor. Master's thesis, Hamburg University of Applied Sciences (2014), http://users.informatik.haw-hamburg.de/~ubicomp/arbeiten/master/eichler.pdf
8. Geisberger, E., Broy, M.: agendaCPS: Integrierte Forschungsagenda Cyber-Physical Systems. acatech Studie, Springer Berlin Heidelberg, Berlin, Heidelberg (März 2012), http://dx.doi.org/10.1007/978-3-642-29099-2_1
9. für Sicherheit in der Informationstechnik, B.B.: Ics-security-kompendium (Nov 2013), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.pdf
10. Neuman, B.C., Ts'o, T.: Kerberos: An authentication service for computer networks. Usc/isi technical report, Institute of Electrical and Electronics Engineers (1994)
11. Sha, L., Gopalakrishnan, S., Liu, X., Wang, Q.: Cyber-physical systems: A new frontier. In: 2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (sutc 2008). pp. 1–9 (June 2008)