Fachtext

**Internet of Things  
Autonomes Fahren**

ZHAW

Communication Competence

IT19a\_ZH Team 1

Autoren: Oliver Corrodi

Erman Zankov

Nikita Smailov

Tobias Ritscher

Auftraggeber: Bundesamt für Umwelt (BAFU)

Abgabetermin: 11.06.2020 23:55

# Abstract

# Inhaltsverzeichnis

[Abstract 2](#_Toc41324119)

[Inhaltsverzeichnis 3](#_Toc41324120)

[Einleitung 4](#_Toc41324121)

[1 Theoretische Grundlagen 5](#_Toc41324122)

[1.1 Stand der Technik 5](#_Toc41324123)

[1.2 Automatisierte Fahrzeugsicherheit 6](#_Toc41324124)

[1.2.1 Sensoren in einem autonomen Fahrzeug 7](#_Toc41324125)

[1.2.2 Künstliche Intelligenz in autonomen Fahrzeugen 8](#_Toc41324126)

[1.3 Cyber-Sicherheit 9](#_Toc41324127)

[1.4 Internet of Things 10](#_Toc41324128)

[1.5 Datenschutz 11](#_Toc41324129)

[2 Resultate 12](#_Toc41324130)

[3 Diskussion und Ausblicke 13](#_Toc41324131)

[Literaturverzeichnis XIV](#_Toc41324132)

[Abbildungsverzeichnis XV](#_Toc41324133)

[Abkürzungsverzeichnis XVI](#_Toc41324134)

# Einleitung

Das Ziel dieser Arbeit ist es, dem Leser Grundkenntnisse über autonomes Fahren zu vermitteln. Mit diesem Wissen wollen wir das Stigma und die Angst, die es umgibt, beseitigen. Die Themen, mit denen wir uns befassen werden, sind die aktuellen technologischen Fortschritte, Sicherheitsfragen und die Entwicklungen, die in der Zukunft stattfinden werden.   
Wir werden uns mit zahlreichen Datenquellen befassen, die sich mit den Sicherheitsfragen im Zusammenhang mit autonom fahrenden Autos befassen und mit der Frage, warum sie sicherer sind als jedes andere Verkehrsmittel.

Diese Arbeit wird zeigen, warum autonom fahrende Fahrzeuge die Zukunft sind, indem die verschiedenen Autonomiegrade und der Prozess, der in solchen Fahrzeugen während der Fahrt abläuft, geklärt werden.

Zum Schluss werden wir die Ergebnisse unserer Daten diskutieren und darstellen, weshalb es langfristig besser ist, autonom fahrende Fahrzeuge zu haben.

# Theoretische Grundlagen

## Ein Bild, das Screenshot enthält. Automatisch generierte BeschreibungStand der Technik

Abbildung 1: Der Weg der Automatisierung zum vollständig autonomen Fahrzeug

Wenn wir vom autonomen Fahren sprechen, müssen wir zwischen den sechs verschiedenen Stufen unterscheiden, die von der Society of Automotive Engineers (SAE) vorgegeben sind.

“The Society of Automotive Engineers (SAE) defines 6 levels of driving automation ranging from 0 (fully manual) to 5 (fully autonomous). These levels have been adopted by the U.S. Department of Transportation.” (Synopsis 2020)

Derzeit sind die meisten Fahrzeuge auf Stufe 0. Das bedeutet, dass das Fahren hauptsächlich vom Fahrer selbst durchgeführt wird. Die einzige Form der Automatisierung und Autonomie ist das Notbremssystem, aber da es das Auto technisch nicht antreibt, zählt es nicht als Teil des autonomen Fahrens.

Die nächste Stufe, die Stufe 1, ist die unterste Stufe des automatisierten Fahrens. Das Fahrzeug verfügt über ein einziges automatisiertes System zur Fahrerunterstützung, wie z.B. Lenkung oder Beschleunigung (Tempomat).

Stufe 2 wird als Teilautomatisierung der Fahrer klassifiziert. Dies wird als fortgeschrittene Fahrerassistenzsysteme oder ADAS bezeichnet. Das Fahrzeug kann sowohl die Lenkung als auch die Beschleunigung/Verzögerung steuern. Hier bleibt die Automatisierung hinter dem Selbstfahren zurück, da ein Mensch auf dem Fahrersitz sitzt und jederzeit die Kontrolle über das Fahrzeug übernehmen kann.

Stufe 3 oder auch Conditional Driving Automation genannt ist ziemlich wichtig, wenn man den Sprung vom technologischen Standpunkt aus betrachtet. Fahrzeuge der Stufe 3 verfügen über Umwelterkennungs-Fähigkeiten und können selbst fundierte Entscheidungen treffen, wie z.B. das Vorbeifahren an einem langsam fahrenden Fahrzeug. Aber sie müssen immer noch von Menschen überbrückt werden.

Stufe 4 ist die höchste Stufe der Antriebsautomatisierung. Der Hauptunterschied zwischen der Automatisierungsstufe 3 und der Stufe 4 besteht darin, dass Fahrzeuge der Stufe 4 eingreifen können, wenn etwas schief läuft oder ein Systemfehler auftritt. In diesem Sinne erfordern diese Fahrzeuge in den meisten Fällen keine menschliche Interaktion. Fahrzeuge der Stufe 4 können im Selbstfahrermodus betrieben werden.

Stufe 5 ist die volle Fahrautomatisierungsstufe. Solche Fahrzeuge erfordern keine menschliche Aufmerksamkeit - die "dynamische Fahraufgabe" entfällt. Fahrzeuge dieser Stufe haben nicht einmal Lenkräder oder Beschleunigungs-/Bremspedale. Sie werden frei von Geofencing sein, überall hinfahren und alles tun können, was ein erfahrener menschlicher Fahrer tun kann.

Die Technologie und die Ressourcen, die erforderlich sind, um ein Fahrzeug von Stufe 0 auf Stufe 5 zu wenden, sind bereits vorhanden. Die derzeit größten Probleme beim autonomen Fahren sind die Software, die zur Nutzung der Hardware erforderlich ist, und die derzeitige Infrastruktur der Städte. Das größte Problem für die autonomen Fahrzeuge ist nicht die Technologie, sondern die Unfallhäufigkeit und die Unfall Haftpflicht. Wer haftet für Unfälle, die von einem selbstfahrenden Auto verursacht werden, und wie oft passieren Unfälle in der offenen Welt?

## Automatisierte Fahrzeugsicherheit

90% aller Unfälle auf der Strasse sind auf menschliches Versagen zurückzuführen und selbst die besten Autofahrer fahren nur zehnmal besser als der Durchschnitt (vgl. Kahyyam 2020, 39). Diese Risiken in unserem alltäglichen Leben können durch Autonome Fahrzeuge signifikant minimiert werden. Wichtig dafür ist ein optimales Gleichgewicht zwischen Hardware und Software. Um die Umgebung in Echtzeit zu analysieren und gefährliche Situationen in kürzester Zeit zu erkennen, braucht es sowohl eine Vielzahl an Sensoren, als auch einen leistungsstarken Computer, der mit dieser Datenmenge umgehen kann.

Ein Bild, das Uhr enthält.

Automatisch generierte Beschreibung

Abbildung 2: Die durch den Einsatz von Multisensoren verursachte komplexe Situationswahrnehmung des autonomen Fahrzeugs

Wie sie in Abbildung 2 sehen, wird die Umgebung konstant mit sechs verschiedenen Sensorarten gemessen und digitalisiert. Diese Sensoren generieren einen grossen Informationsfluss, welcher extrem wichtig ist, um bei jeder Momentaufnahme die Situation so genau wie möglich analysieren zu könne. Da es möglichst viele Momentaufnahmen braucht, herrscht ein schwieriges Gleichgewicht zwischen der Anzahl Sensoren und dem Zeitintervall zwischen den einzelnen Momentaufnahmen. Desto mehr Sensoren man einbaut, desto mehr Informationen hat man über die Umgebung. Allerdings führt dies auch zu einer grösseren Datenmenge, welche länger braucht, um bearbeitet zu werden und somit die Reaktionszeit des Autos um entscheidende Sekunden verlängert. Daher sind die Informationslücken (Blind Spots) genauso wichtig wie die Sensoren und bis zu einem gewissen Mass eine Erhöhung der Sicherheit.

### Sensoren in einem autonomen Fahrzeug

**Ultraschall (kurze Distanz):** Dieser Sensor benutzt Schallwellen mit hohen Frequenzen (50kHz), welche vom Auto gesendet werden und an Objekten abprallen. Das Auto misst die Zeit bis die Wellen zurückkommen, um den Abstand zu berechnen.

**Kameras:** Kameras werden benötigt, um visuelle Objekte zu analysieren. Sie erkennen Hindernisse in Echtzeit, ermöglichen eine Erkennung der Fahrspur und verfolgen Fahrbahninformationen (z. B. Strassenschilder). Um die Bilder zu analysieren werden komplexe Algorithmen benutzt, welche mit der Hilfe der anderen Sensoren relevante Informationen aus den Bilddaten filtern.

**Radar (Kurze und weite Distanz):** Der Radarsensor sendet Radiowellen, welche wie beim Ultraschall durch die Zeit bis zur Rückkehr die Berechnung der Distanz ermöglichen. Der Radar wird benutzt, um den Abstand zu anderen Fahrzeugen und Fussgängern zu ermitteln.

**LiDAR:** Dieser Sensor misst die Distanz zu Objekten durch Abgabe von pulsierendem Laser Licht und die Zeit bis zur Reflexion. Das Resultat ist eine sehr genaue 3D Erkennung der Umgebung. LiDAR wird vor allem auf mittlere bis weite Distanz eingesetzt, um die Gesamte Umgebung zu analysieren.

**DSRC:** DSRC (Dedicated Short Range Communication) ermöglicht die Kommunikation sowohl mit anderen Autos als auch mit weitern Geräten über 4G, Wi-Fi, Bluetooth, etc.

**Standort Sensoren:** Jedes Autonome Fahrzeug braucht auch noch weitere Sensoren, um den genauen Standort und den momentanen Zustand des Fahrzeuges zu messen.

GPS wird verwendet, um die Koordinaten des Fahrzeuges zu bekommen.

Ein Beschleunigungsmesser misst die aktuelle Veränderung der Geschwindigkeit.

Das Gyroskope gibt die Neigung und die Rotation des Fahrzeuges an und eine Rad-  
Kegelmessung berechnet die Position der Räder.

### Künstliche Intelligenz in autonomen Fahrzeugen

Um All diese Daten zu verarbeiten, braucht es eine leistungsstarke Software. Diese Aufgabe wird mit einem Künstliche Intelligenz (KI) Model übernommen. Dieses Modell hat 3 Teile:

1. **Daten sammeln**

Wie bereits erwähnt hat ein autonomes Fahrzeug eine Vielzahl an Sensoren. Diese riesige Datenflut umfasst alle Informationen, welche ein menschlicher Fahrer wahrnehmen würde. Diese Daten werden gesendet und als «aktuelle Situation» verarbeitet. Nach diesem Schritt weiss die Software genau, was in diesem Moment um das Fahrzeug passiert.

1. **Pfad planen, Entscheidung treffen**

Diese Momentaufnahme wird in einer Datenbank gespeichert und mit bisherigen Erfahrungen abgeglichen. Diese Abgleichung erlaubt der KI aus der Vergangenheit zu lernen und bessere Entscheidungen zu treffen. Die daraus gewonnenen Erkenntnisse werden dann gebraucht, um die sicherste, angenehmste und ökonomisch beste Option für das weitere Vorgehen zu bestimmen. Schlussendlich enden all diese Berechnungen in einer optimalen Route von A nach B, welche auch Hindernisse umgehen muss und dabei die physikalischen Beschränkungen des Fahrzeuges (maximaler Wendekreis, Bremsweg, etc.) und das Einhalten einer angenehmen Fahrweise beachtet.

1. **Handeln**

Basierend auf den getroffenen Entscheidungen der KI, ist das Fahrzeug nun im Stande Hindernisse auf der Strasse zu erkennen, durch den Verkehr zu navigieren, Fussgänger auszuweichen und Rechtsvortritte zu beachten. Eine sichere und angenehme Fahrt zum Ziel ist somit gewährleistet. Die KI muss dazu aber das Fahrzeug vollständig bedienen können. Deshalb hat die Software Zugriff auf alle Teile des Fahrzeuges inklusive Lenkrad, Gaspedal und Handbremse.

Diese drei Phasen befinden sich in einer Dauerschlaufe welche erst beim ausschalten des Motors beendet wird. Desto öfter die Schlaufe durchlaufen wird, desto intelligenter ist das AI Modell und desto präziser sind die Entscheidungen. Dies trifft vor allem auf komplexere Situationen zu, da das Modell aus der Vergangenheit lernt.

## Cyber-Sicherheit

Es ist keine Untertreibung zu behaupten, dass die Cybersicherheit von Fahrzeugen ein entscheidender Faktor ist, um den Anteil an selbstfahrenden Autos auf der Strasse zu erhöhen. In einer von der AAA durchgeführten Umfrage zeigte sich, dass 75% aller Autofahrer vor allem aufgrund von Sicherheitsbedenken Angst davor haben, in einem selbstfahrenden Auto zu fahren (vgl. Causevic 2017).

“In a 2016 speech, GM CEO Mary Barra acknowledged that “a cyber incident is a problem for every automaker in the world…it is a matter of public safety.”   
(Causevic 2017).

Noch vor einem Jahrzehnt verbaute die Automobilindustrie Prozessoren mit zu geringer Leistung, da die Daten mit Kabeln direkt übertragen wurden und keine grosse Rechenleistung nötig war. Heutige Fahrzeuge werden jedoch mit wesentlich leistungsfähigeren System-on-Chip (SoC)-Designs ausgeliefert, die weitaus mehr leisten können. Autonome Autos müssen noch einen Schritt weiter gehen, da sie genügend Rechenleistung benötigen, um wichtige Entscheidungen auf der Grundlage sensorischer Eingaben zu treffen.

”But added complexity comes at the cost of increased vulnerability. Two years ago, security researchers Charlie Miller and Chris Valasek demonstrated how a Jeep Cherokee can be hacked remotely via its internet connection. The duo was able to paralyze the car on a highway, remotely.” (Causevic 2017).

Wie bei allen Anwendungen des maschinellen Lernens besteht der erste Schritt zum Einsatz künstlicher Intelligenz zur Bekämpfung von Sicherheitsrisiken in autonomen Fahrzeugen in der Sammlung und Speicherung der richtigen Daten. Wenn das interne Netzwerk eines Autos mit einer Plattform überwacht wird, die Protokolle speichern und analysieren kann, kann das Fahrzeug selbst böswillige Aktivitäten erkennen und Angriffe verhindern - oder zumindest die Fahrer warnen und ihre Auswirkungen mildern.

“An example of a “learn and prevent” device that works in a vehicular context is the anti-hacking solution developed by Miller and Valasek. This device is an intrusion-detection system for vehicles with certain automated features.” (Causevic 2017)

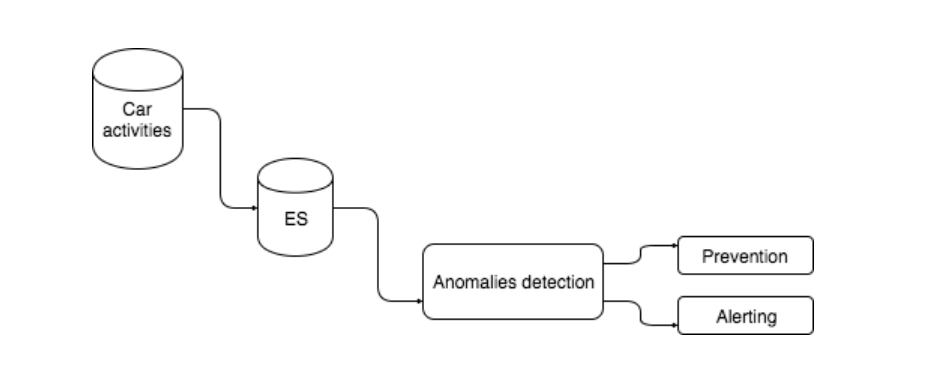


Abbildung 3: Aufbau eines "lernen und verhindern" Gerätes

## Internet of Things

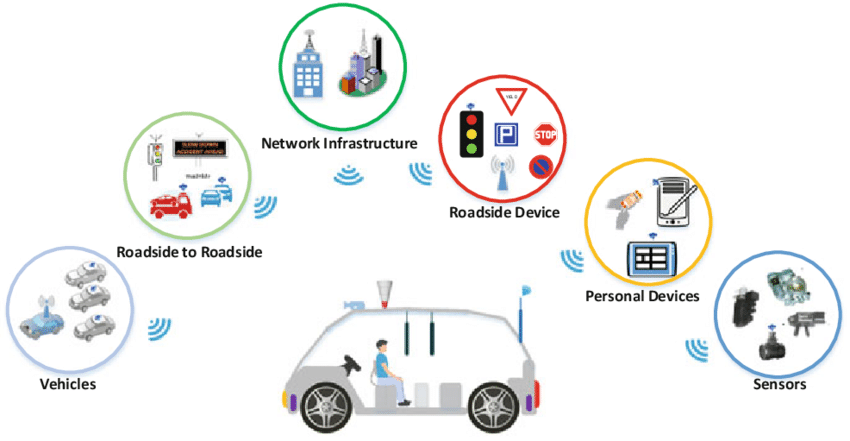


Abbildung 4: Grafische Darstellung der Kommunikation durch IoT

Als Internet of Things (IoT) wird die Kommunikation zwischen verschiedenen Geräten bezeichnet. Diese Kommunikation ist ein Grundelement zum Erfolg von autonomen Fahrzeugen. IoT erlaubt zum Beispiel einer Ampel den wartenden Autos mitzuteilen, wann sie fahren dürfen. Dies ist viel weniger Fehleranfällig und viel effizienter als das Analysieren von Bildern von einer Kamera. Auch würde es einem Ambulanzfahrzeug ermöglichen, ihren Standort den Autos in der Umgebung mitzuteilen und so könnten die Autos im richtigen Moment ausweichen. Kurz gesagt, IoT ermöglicht eine Bienenähnliche Schwarmintelligenz, welche die Sicherheit auf der Strasse enorm erhöhen könnte.

Eine IoT Plattform besteht typischerweise aus einem Cloudspeicher und einer Internet Infrastruktur. Im Cloudspeicher werden alle Daten in einer enorm grossen Datenbank gespeichert und in der Internet Infrastruktur wird die Kommunikation zwischen den Geräten sichergestellt.

Internet zwischen Geräten bedeutet aber nicht, dass nur Fahrzeuge auf diese Plattform Zugriff haben. Alles kann ein Gerät werden. Das verlinken von Velos, Parkplätzen, Zügen, Fussgänger, Wetterstationen und vielen weiteren Objekten ist denkbar. Ein optimales System ist ein vollständig digitalisiertes Modell der Umgebung durch Sensoren in allen Objekten. Durch eine solche Schwarmintelligenz wird die Wahrscheinlichkeit eines unvorhergesehenen Ereignisses auf ein Minimum gebracht.

## Datenschutz

Die Schwarmintelligenz durch IoT hat viel Potential. Das Auto bremst für einen Fussgänger, bevor dieser für das menschliche Auge überhaupt sichtbar ist. Ampeln werden nicht mehr gebraucht, da bei einer Kreuzung alle betreffenden Fahrzeuge abstimmen können, um den Vortritt zu bestimmen.

Doch was man bei all diesen Verbesserungen nicht vergessen darf, sind die Grundrechte jeder einzelnen Person. Deshalb ist es enorm wichtig, diese Datensammlung so anonym wie möglich zu machen. Diese Datenbank darf nicht zu einem Standortverlauf der Menschheit werden, sondern soll Positionen von anonymisierten Geräten enthalten und diese nur so lange speichern, wie sie benötigt werden.

Das Einhalten des Datenschutzes muss auch hier oberste Priorität haben.

# Resultate

Der stetige Zuwachs an autonomen Fahrzeugen mit immer höheren Automationsstufen in den letzten Jahren schafft einen neuen Trend zur Einführung verschiedener intelligenter Techniken und Technologien, um die Leistung und Qualität der automatischen Entscheidungsfindung zu verbessern. Die Integration von KI und IoT für autonome Fahrzeuge bietet hochleistungsfähige Systeme, die eingesetzt werden können, um dynamischere und sicherere Steuerungssysteme zu ermöglichen.

Während die wichtigsten Software- und Hardwarekomponenten von autonomen Fahrzeugen aus Sicherheits- und Reliabilitätsgründen immer noch direkt im Auto verbaut werden, können viele Daten und Hilfsmittel mit Hilfe von IoT ausgelagert werden um einige technische Herausforderungen wie Stromverbrauch, Rechenleistung und Sicherheit zu bewältigen.

# Diskussion und Ausblicke

Das Thema Künstliche Intelligenz und autonomes Fahren wird wohl noch lange mit viel Vorbehalt betrachtet werden. Filme wie «Terminator» und «I, Robot» haben uns aufgezeigt was alles schieflaufen kann, und die Angst vor diesen Technologien geschürt.

Unser Fachtext basiert auf gut recherchierten Fakten und soll eine objektive Ansicht auf das Thema werfen. Aber auch wenn autonome Fahrzeuge viel Potential zu mehr Sicherheit und besserer Effizienz beinhalten, gibt es noch viele Risiken, welche es zu beachten gilt.

Der Strassenzustand kann für die Sensoren eine grosse Schwierigkeit darstellen. Strassen ohne Markierungen, unklar beschilderte Strassen, Verkehrspolizisten an Kreuzungen, Baustellen auf der Strasse, etc. sind nur einzelne Beispiele. Als Autofahrer trifft man täglich auf unklare oder unsichere Situationen. All das muss bei der Entwicklung beachtet werden. Das Risiko bei Fehlern ist gross.

Das grösste Problem überhaupt sind aber wir Menschen. Niemand kann berechnen, was ein anderer Autofahrer macht. Vortrittsmissachtung oder Auffahrunfälle in stockendem Verkehr sind für autonome Fahrzeuge genauso ein grosses Risiko wie für alle anderen Verkehrsteilnehmer. So lange es Menschen auf der Strasse gibt, bleibt der Verkehr unvorhersehbar.

Autonome Fahrzeuge können die Strassen sicherer machen und wir können uns auf eine Zeit freuen, in der man, durch Schwarmintelligenz und KI, die Strasse überqueren kann und dabei den Verkehr teilt, wie Moses damals das Meer. Jedoch müssen wir gut Acht geben, dass, in all diesem Trend zu mehr Vernetzung und mehr Sicherheit unsere Anonymität und Freiheit nicht vergessen geht.

# Literaturverzeichnis

**Gupta,** Anil (2017): Five challenges in designing a fully autonomous system for driverless cars. (21.08.2017)   
URL: https://iiot-world.com/artificial-intelligence/five-challenges-in-designing-a-fully-autonomous-system-for-driverless-cars/ [Stand: 21.05.2020]

**Kahyyam,** Hamid et al. (2020): Artiﬁcial Intelligence and Internet of Things for Autonomous Vehicles. In: Dai, Liming / Jazar, Reza N. (Hrsg.): Nonlinear Approaches in Engineering Applications. New-York: Springer-Verlag. 39-68.  
URL: https://www.researchgate.net/publication/335021813\_Artificial\_Intelligence\_and\_Internet\_of\_Things\_for\_Autonomous\_Vehicles [Stand: 21.05.2020]

**Ercan,** Serdar (2019): IoT and Smart Autonomous Cars. #EasyMobiliser. (27.03.2019)  
URL: https://blog.hslu.ch/majorobm/2019/03/27/iot-smart-autonomous-cars-easymobiliser/ [Stand: 21.05.2020]

**Synopsis** (2020): The 6 Levels of Vehicle Autonomy Explained. URL: https://www.synopsys.com/automotive/autonomous-driving-levels.html   
[Stand: 21.05.2020]

**Oka,** Dennis Kengo (2019): Securing the Modern Vehicle. A Study of Automotive Industry Cybersecurity Practices. URL: https://www.sae.org/binaries/content/assets/cm/content/topics/cybersecurity/securing\_the\_modern\_vehicle.pdf   
[Stand: 21.05.2020]

**Causevic,** Dino (2017): How Machine Learning Can Enhance Cybersecurity for Autonomous Cars. URL: https://www.toptal.com/insights/innovation/how-machine-learning-can-enhance-cybersecurity-for-autonomous-cars [Stand: 24.05.2020]

# Abbildungsverzeichnis

Abbildung 1: Der Weg der Automatisierung zum vollständig autonomen Fahrzeug 5

Abbildung 2: Die durch den Einsatz von Multisensoren verursachte komplexe Situationswahrnehmung des autonomen Fahrzeugs 7

Abbildung 3: Aufbau eines "lernen und verhindern" Gerätes 10

Abbildung 4: Grafische Darstellung der Kommunikation durch IoT 11

# Abkürzungsverzeichnis

IoT = Internet of Things

KI = Künstliche Intelligenz

SoC = System-on-Chip