SYSTEMTECHNIK

Industrielle Informatik

MATURA 2016

STEFAN GEYER

Inhaltsverzeichnis

1 Cloud Computing und Internet of Things 2
1.1 Sensornetze im IoT 2
1.1.1 Anwendungsbereiche von Sensornetzen 2
1.1.2 Integrationsansätze mit IoT Gateways 3
1.1.3 Integrationsansätze mit der LoRa-Technologie 5
2 Automatisierung, Regelung und Steuerung 5
2.1 M2M (Machine to Machine) 5
2.2 Bussysteme 6
2.2.1 CAN-Bus 6
2.2.2 GPIB 6
2.3 Sensoren und Aktoren 6
2.3.1 Sensoren 6
2.3.2 Aktoren 8
3 Security, Safety, Availability 8
3.1 Reaktion im Fehlerfall eines Systems – Der Watchdog 8
3.1.1 Aufbau eines Watchdogs 8
3.2 CIA-Triangle 9
3.2.1 Confidentiality – Vertraulichkeit 9
3.2.2 Integrity – Integrität 10
3.2.3 Availability – Verfügbarkeit 10
3.3 AES on Chip 10
4 Authentication, Authorization, Accounting 11
5 Desaster Recovery 11
6 Algorithmen und Protokolle 11
6.1 Drahtlose Kommunikation zwischen Mikrocontrollern 11
6.1.1 WiFi 11
6.1.2 ZigBee 11
7 Konsistenz und Datenhaltung 12
7.1 SD-Cards 12
8 Abbildungsverzeichnis 13
9 Literaturverzeichnis 13

1 Cloud Computing und Internet of Things

Das zukünftige Internet wird als „Internet of Things“ ausgelegt werden. Das IoT kann als weltweites Netzwerk aus miteinander verbundenen Objekten, welche durch ein standardisiertes Kommunikationsprotokoll eindeutig adressiert sind, beschrieben werden. Mit einer eindeutigen Adresse ausgestattet, können Objekte wie Computer, Sensoren, RFID-Tags oder Mobiltelefone dynamisch dem Netzwerk beitreten und mit anderen Objekten kommunizieren bzw. arbeiten. [1]

1.1 Sensornetze im IoT

Wären Sensornetze im IoT ansprechbar, würde das viele neue Möglichkeiten eröffnen. Mithilfe eines Sensornetzes können viele Informationen über die Umwelt gesammelt werden. Wird ein Sensornetz mit dem Internet verbunden, müssen erst ein paar Probleme aus dem Weg geräumt werden, bevor man die Vorteile einer solchen Integration nutzen kann.

1.1.1 Anwendungsbereiche von Sensornetzen

Die Anwendungsbereiche von Sensornetzen kann in drei Hauptkategorien aufgeteilt werden: Aufzeichnung von Umgebungen, Objekten und der Interaktion von Umgebung und Objekten

- Aufzeichnung von Umgebungen

  Ein Beispiel dafür sind Aufzeichnungen der Umwelt. Sensornetze werden in Umgebungen wie Wäldern, Berglandschaften, Gletschern oder auf Bojen im Meer angebracht, um auf lange Zeit Informationen über die Umweltbedingungen dieser Region zu sammeln. Zum Beispiel können Temperatur-, Feuchtigkeits- und Helligkeitswerte dazu verwendet werden, um Naturphänomene, wie der Einfluss des Klimawechsels auf die Steinschlagraten in Dauerfrostgebieten zu erforschen.

- Aufzeichnung von konkreten Objekten

  Die Strukturüberwachung ist ein mögliches Beispiel für diese Kategorie. Durch das Messen von Vibration und Geräuschemissionen, können potentielle Bruchstellen bei Gebäuden und Brücken gefunden werden.

- Aufzeichnungen der Interaktion zwischen Umgebung und Objekten

  Diese Art ist eine Kombination der beiden vorherigen Kategorien und beinhält unter anderem das Aufzeichnen von Naturkatastrophen, wie Tsunamis oder Vulkanausbrüchen.

[1]

1.1.2 Integrationsansätze mit IoT Gateways

Es gibt drei Haupansätze ein Sensornetz mit dem Internet zu verbinden, die sich durch den Grad der Integration in die Internetstruktur der Sensornetze unterscheiden.

Der erste Ansatz, welcher derzeit von den meisten Sensornetzen, die sich mit dem Internet verbinden, umgesetzt wird und die höchste Abstraktion zwischen Netzwerken mit sich bringt, besteht daraus, dass sich das gesamte Sensornetz über ein einzelnes Gateway mit dem Internet verbindet.

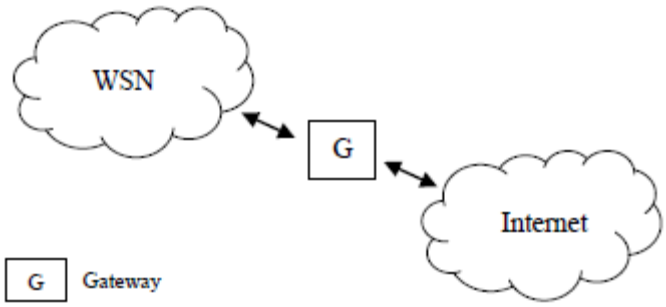

Abbildung 1: Unabhängiges Netzwerk [1]

Der zweite Ansatz bildet ein hybrides Netzwerk, welches aus mehreren unabhängigen Netzwerken besteht. Dabei können nur einige Sensorknoten sich zum Internet verbinden.

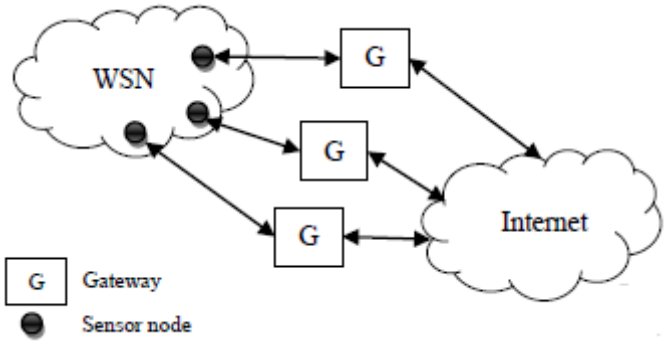

Abbildung 2: Hybrides Netzwerk [1]

Der letzte Ansatz ist von einer WLAN-Struktur inspiriert und hat die Form eines dichten Access-Point-Netzwerks, indem die Sensorknoten das Internet über einen Hop erreichen können.

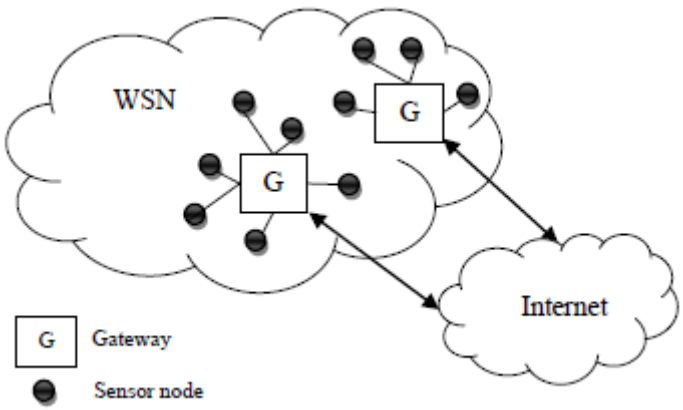

Abbildung 3: Access-Point Netzwerk [1]

Es ist offensichtlich, dass der erste Ansatz aufgrund der Tatsache, dass nur ein Gateway vorhanden ist, einen Singe-Point-Of-Failure mit sich bringt: Ein Absturz des Gateways würde die Internetverbindung des gesamten Sensornetzes unterbrechen. Durch die Verwendung von mehreren Gateways und Access-Points verhindern die Ansätze zwei und drei dieses Problem. Daher sind diese Ansätze immer zu bevorzugen, um ein robustes Netzwerk zu garantieren.

Welche der beiden übrigen Ansätze letztendlich gewählt wird, hängt vom Anwendungsszenario des Sensornetzes ab.
Der zweite Ansatz eignet sich dann, wenn die Sensorknoten in einem vermaschten Netz angeordnet sind. In einem vermaschten Netz ist jeder Netzwerkknoten mit einem oder mehreren anderen verbunden. Die Informationen werden von Knoten zu Knoten weitergereicht, bis sie das Ziel erreichen. In diesem Fall ist das Ziel jener Sensorknoten, der mit dem Gateway, und somit mit dem Internet, verbunden ist. Dieser Ansatz eignet sich für die Aufzeichnung von Umgebungen und für Aufzeichnungen der Interaktion zwischen Umgebung und Objekten.
Dadurch, dass das Internet immer über einen Hop erreichbar ist, wird der dritte Ansatz dann verwendet, wenn die Anwendung am Sensor-Endgerät eine niedrige Latenzzeit und daher eine direkte Verbindung benötigt. Dieser Ansatz eignet sich für die Aufzeichnung von Objekten. [1]

1.1.2.1 „IP to the field“-Paradigma

Es ist wichtig zu erwähnen, dass die Integrationsansätze nur statische Netzwerkkonfigurationen unterstützen. Jedes neue Gerät, welches über Internetzugriff verfügen soll, erfordert eine zeitaufwändige Neuprogrammierung des Gateways. Das bedeutet, dass die Flexibilität, welche vom zukünftigen IoT erwartet wird, nicht bereitgestellt werden kann.
Um den Erwartungen bezüglich Flexibilität nachzukommen, sollte das „IP to the Field“-Paradigma angewandt werden. Das Paradigma setzt voraus, dass die Sensorknoten intelligente Netzwerkkomponenten, und nicht mehr nur auf das Erfassen von Daten limitiert sind. Durch das Übertragen der Intelligenz auf die Sensorknoten, beschränken sich die Aufgaben des Gateways auf das Forwarding von Anfragen und Protokollübersetzungen. Auch andauernde Neuprogrammierungen wären durch den Einsatz von dynamischer Netzwerkkonfiguration nicht mehr notwendig. [1]

1.1.2.2 Sicherheitsproblematik bei Sensornetzen im IoT

Durch das „IP to the field“-Paradigma übernimmt der Sensorknoten mehr Verantwortung. Das bringt Vorteile aber auch Sicherheitsprobleme mit sich.
Ein Sensornetz ohne Internetverbindung anzugreifen ist schwer: Eine physikalische Nähe zu einem Sensorknoten ist notwendig um Daten abzugreifen. Durch eine Internetverbindung am Sensorknoten ist das nicht mehr notwendig. Angreifer können das Netz von überall angreifen. Außerdem kann Malware durch eine Internetverbindung wesentlich einfacher auf die Geräte gelangen. Um das zu verhindern, muss das Gateway einen entsprechend guten Schutz bereitstellen. Generell ist es notwendig, dass innovative Sicherheitsmechanismen entwickelt werden, um Sensornetze von Angriffen aus dem Internet zu schützen. [1]

1.1.3 Integrationsansätze mit der LoRa-Technologie

Der Begriff „LoRa“ steht für „Long Range“, was auch schon den großen Vorteil dieser Technologie hervorhebt. Die Datenrate, mit der operiert werden kann, liegt im Rahmen von Kilobits pro Sekunde. Die Technologie eignet sich daher nicht für Video-Streaming, sondern eher für das Internet of Things und M2M-Anwendungen.
LoRa kann in einem breiten Frequenzbereich von 137 MHz bis 1020 MHz verwendet werden. Dieser Bereich beinhält zahlreiche lizenzfreie Frequenzbänder wie zum Beispiel 169 MHz, 433 MHz, 868 MHz, 915 MHz.

Geräte, die z.B. aufgrund ihrer Lage oder einer freien Sicht eine bessere Verbindung zum Gateway haben, können hohe Datenraten bis zu 11 kB/s verwendet und so Batterie sparen. Geräte mit einer schwachen Verbindung können niedrigere Datenraten verwenden, welche bei freier Sicht zum Gateway bis zu einer Distanz von 30 km verfügbar sind. [2]

1.1.3.1 LoRaWAN

LoRaWAN ist das MAC-Protokoll für ein IoT-Netzwerk aus LoRa-Knoten. Konkret handelt es sich um einen LPWAN-Standard (Low Power Wide Area Network), welcher die oben beschriebenen Vorteile von LoRa nutzt, um Batterielebensdauer und Servicequalität der LoRa-Knoten zu optimieren.

Das Protokoll arbeitet vollkommen bidirektional, was den Empfängern von Nachrichten ermöglicht die Ankunft einer Nachricht zu bestätigen. Das Protokoll unterstützt End-to-End Verschlüsselung für eine sichere Kommunikation und Multicast. Des Weiteren können sich die Knoten per Funk am Gateway registrieren. Zusätzlich ist es möglich, die Positionen der Knoten mithilfe von GPS ausfindig zu machen. [2]

2 Automatisierung, Regelung und Steuerung

2.1 M2M (Machine to Machine)

„Machine to Machine“ beschreibt Technologien die, ohne die Unterstützung eines Menschen, über ein Netzwerk Informationen austauschen und Aktionen durchführen können und wird oft im Bereich der Remote-Datenaufzeichnung angewandt. M2M formt die Basis für das Internet of Things.

Die wichtigsten Komponenten eines M2M Systems sind Sensoren, eine Möglichkeit sich per Funk mit dem Internet zu verbinden, eine Art der Identifizierung wie RFID und eine Software die einer Netzwerkkomponente hilft Daten zu interpretieren und Entscheidungen zu treffen.

M2M ist noch nicht standardisiert und viele M2M Systeme werden für spezielle Aufgaben gebaut. Dadurch, dass M2M immer allgegenwärtiger wird, werden sich die Hersteller aber auf gemeinsame Standards einigen müssen. [3]

2.2 Bussysteme

2.2.1 CAN-Bus

Der CAN-Bus wurde ursprünglich für die Autoindustrie entwickelt. Das Ziel war es, durch die Einführung eines Bussystems im Kraftfahrzeug die Verkabelung der einzelnen Systeme, Sensoren und Aktoren zu vereinfachen.

Der Bus muss für sogenannte Klasse-C Applikationen geeignet sein. Das bedeutet, der Bus muss in der Lage sein, zeitkritische Informationen mit Zykluszeiten von 1 bis 10ms und Latenzzeiten von unter 1ms zu übertragen. Die Länge einer Nachricht umfasst dabei wenige Bytes, während die zu erwartende Datenrate bei dieser Anwendung im Bereich von 250 kBit/s bis 1 MBit/s liegt. Beispiele für typische Klasse-C Applikationen sind der Bereich des Motormanagements und der Stabilitätskontrolle.

Aus Sicherheitsgründen ist es notwendig, dass ein CAN-Bus eine Multimaster-Fähigkeit besitzt. Dabei ist jeder Knoten in der Lage Kommunikation einzuleiten. So kann verhindert werden, dass z.B. durch einen Defekt in einem Knoten die Funktion des Gesamtsystems gefährdet ist. [4]

2.2.2 GPIB

Der „General Purpose Interface Bus“ ist ein Datenbus, der oft in Messgeräten und Peripheriegeräten eingesetzt wird. Der Bus dient der Kommunikation zwischen Talker, Listener und Controller.
Wie der Name schon sagt, kann der Talker Nachrichten senden, und der Listener Nachrichten empfangen. Es ist möglich, dass Talker gleichzeitig auch der Listener ist. Der Talker kann zum Beispiel ein Messgerät sein, welches Daten zu einem oder mehreren Listenern (andere Messgeräte) oder zum Controller sendet.
Der Controller überwacht und verwaltet die Kommunikation und den Informationsfluss auf dem Bus indem er Befehle an alle angeschlossenen Geräte schickt. Er stellt die zentrale Schaltstelle dar, die einen Talker mit dem entsprechenden Listener verbindet. Bevor ein Talker seine Nachricht absetzen kann, wird er durch Steuerbefehle des Controllers freigegeben. Nach dem die Nachricht übertragen wurde, kann der Controller andere Talker oder Listener durchstellen.

Manchmal findet man auch GPIB-Konfigurationen vor, die ohne Controller arbeiten. In diesem Szenario ist lediglich ein Talker mit einem Listener verbunden und der Talker kann nur eine Talk- und der Listener nur eine Listen-Funktion ausführen. [5]

2.3 Sensoren und Aktoren

2.3.1 Sensoren

2.3.1.1 Kapazitive Sensoren

Kapazitive Sensoren arbeiten berührungslos und wandeln Größen, die relevant für Produktionen sind (Distanz zu einem Objekt oder ein Füllstand) in ein weiterverwendbares Signal um. Die Funktion beruht auf der Änderung des elektrischen Feldes in der Umgebung der aktiven Zone des Sensors. Der

Grundaufbau besteht aus einem RC-Oszillator als Aufnehmer, einem Demodulator und einer Ausgangstufe.
Die Annäherung von Metallen oder Nichtmetallen in die aktive Zone des kapazitiven Sensors bewirkt eine Kapazitätsänderung, die den RC-Oszillator zum Schwingen bringt. Das bewirkt, dass die dem Oszillator nachgeschaltete Triggerstufe kippt und der Schaltverstärker seinen Ausgangszustand ändert. Die Schaltfunktion am Ausgang ist je nach Gerätetyp Schließer, Öffner oder Wechsler.

Kapazitive Näherungsschalter werden oft für die Steuerung und Überwachung von Maschinenprozessen, und zur Messung des Füllstands in Behältern verwendet. [6]

2.3.1.1.1 Bündige Version

Sensoren mit einem geradlinigen elektrischen Feld. Geräte mit solchen Sensoren tasten Festkörper auf Distanz, oder eine Flüssigkeiten durch eine Trennwand aus Glas oder Kunststoff (höchstens 4 mm) ab. [6]

Abbildung 4: Bündige Version eines kapazitiven Sensors [6]

2.3.1.1.2 Nicht Bündige Version

Sensoren mit einem kugelförmigen elektrischen Feld. Diese Geräte sollen mit ihrer aktiven Fläche das aktive abzutastende Produkt (z.B. Granulat, Sand, Öl oder Wasser) berühren. [6]

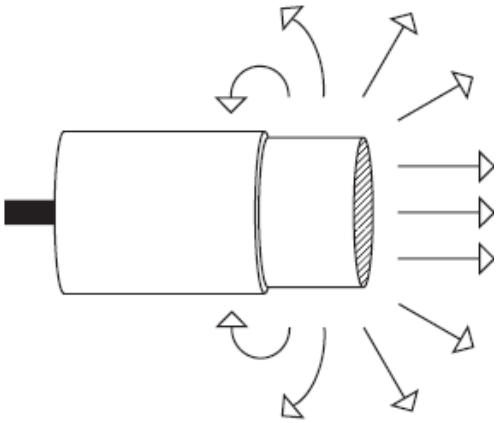

Abbildung 5: Nicht bündige Version eines kapazitiven Sensors [6]

2.3.1.2 Induktive Sensoren

Induktive Sensoren nutzen die Wechselwirkung metallischer Leiter mit ihrem elektromagnetischen Wechselfeld. Im Leiter werden Wirbelströme induziert, die dem Feld Energie entziehen und dadurch die Höhe der Schwingungsamplitude reduzieren. Diese Änderung wird vom induktiven Sensor ausgewertet. Als aktive Fläche bezeichnet man den Bereich, durch den das hochfrequente Sensorfeld in den Luftraum eintritt. [7]

„Aufgrund ihres Funktionsprinzips sind induktive Sensoren ausschließlich für die Erkennung metallischer Objekte geeignet. Dies tun sie allerdings äußerst zuverlässig und sind zudem sehr robust und widerstandsfähig (z.B. bei Umwelteinflüssen), was sie für zahlreiche industrielle Anwendungen interessant macht.“ - [7]

2.3.2 Aktoren

2.3.2.1 Digitale Aktoren

PBN

2.3.2.2 Analoge Aktoren

Problematik der Reichweite

Aktoren: Digital (PBN), Analog (Problematik der Reichweite)

3 Security, Safety, Availability

3.1 Reaktion im Fehlerfall eines Systems – Der Watchdog

Ein Funktionswächter oder Watchdog ist eine unabhängige Hardware- und Softwarelösung, die dazu dient ein System zu überwachen. Wird ein Fehlzustand, ein Ausfall oder Fehlfunktion durch den Funktionswächter entdeckt, werden Korrekturmaßnahmen eingeleitet. Oberste Priorität ist es, das System in einen normalen Betriebszustand zu bringen. Danach kann versucht werden, einen normalen Betriebszustand wiederherzustellen. Der Watchdog ist ebenso ein wichtiger Schutz gegen böswilligen Code, Designfehler oder unvorhersehbare Ereignisse. [8]

3.1.1 Aufbau eines Watchdogs

Der Funktionswächter besitzt einen digitalen Zähler, der mit einem bestimmten Tempo, abhängig von einem festen Taktgeber, von einem Anfangswert bis zu einem Zielwert zählt. Oft wird von einem variablen Startwert runter bis Null gezählt. Wenn der Zähler beim Zielwert angelangt ist, wird ein Timeout-Signal generiert. Das Timeout-Signal wiederum ist zu einem externen Schaltkreis verbunden.

Der Watchdog-Timer (WDT) wird beim Systemboot gestartet. Generiert der Timer durch das Erreichen des Zielwerts ein Timeout, wird normalerweise ein Hardware-Reset durchgeführt. Um das zu verhindern, muss das System in Regelmäßigen Abständen den Zählerstand des Watchdogs auf den Anfangswert setzen.

Watchdog-Timer sind ein wichtiger Bestandteil von Mikrocontrollern, da sie einen automatischen Mechanismus zur Verfügung stellen, der sowohl Software- als auch vorübergehende Hardwarefehler behandeln kann. Ein Funktionswächter kann viel schneller auf Fahler reagieren als ein Mensch und ist daher von unschätzbarem Wert, wenn menschliche Benutzer nicht schnell genug auf Fehlzustände reagieren können. [8]

3.2 CIA-Triangle

CIA steht für Confidentiality (Vertraulichkeit), Integrity (Integrität) und Availability (Verfügbarkeit) und bezeichnet die Eigenschaften eines Informationsverarbeiteten und -lagernden Systems.
In diesem Zusammenhang ist Vertraulichkeit ein Regelsatz, welcher den Zugriff auf Informationen beschränkt, Integrität ist die Gewissheit, dass die Informationen zuverlässig und genau sind, und Verfügbarkeit garantiert, dass autorisierte Personen immer Zugriff auf die Information haben. [9]

3.2.1 Confidentiality – Vertraulichkeit

Vertraulichkeit kann man in gewisser Art und Weise Geheimhaltung von Daten vergleichen: Die Maßnahmen die ergriffen werden, um Vertraulichkeit zu garantieren, haben das Ziel zu verhindern, dass sensible Daten an die falschen Personen gelangen, während die richtigen Personen aber darauf zugreifen können. Die Daten werden oft danach kategorisiert, wie viel und welche Art von Schaden angerichtet wäre, wenn sie in falsche Hände fallen.

Ein gutes Beispiel, das die Methoden aufzeigt, die genutzt werden um Vertraulichkeit zu garantieren, sind Accounts beim Online-Banking. Oft kommt eine Art der 2-Factor-Authentifikation zum Einsatz, bei die neben der Authentifikation mit ID und Passwort, auch noch einen separaten Identitätsnachweis voraussetzt. Das kann beispielsweise ein Code sein, der per SMS an das Telefon des Nutzers gesendet wird. Eine andere Möglichkeit wäre zum Beispiel eine Art der biometrische Identifikation, wie das Scannen der Iris. [9]

3.2.2 Integrity – Integrität

Integrität beschreibt das erhalten von Konsistenz, Genauigkeit und Zuverlässigkeit von Datensätzen über deren gesamten Lebenszyklus hinweg. Es ist wichtig, dass die Daten nicht ungewollt verändert werden, daher müssen Maßnahmen getroffen werden. Diese Maßnahmen bestehen unter anderem aus dem Festlegen von Zugriffsrechten auf Dateien und User-Access-Controls (UAC). Oft wird auch eine Art der Versionskontrolle genutzt, um ungewollte Änderungen, oder das Löschen von Dateien rückgängig machen zu können.
Selbstverständlich müssen auch Gegenmaßnahmen getroffen werden, um Datenänderungen die nicht vom Menschen verursacht wurden, wie zum Beispiel elektromagnetische Pulse oder Serverabstürze, aufzuspüren. Dabei können Checksummen, zum Überprüfen der Datenintegrität sehr hilfreich sein. Dementsprechend müssen auch Backups verfügbar sein, um von einem fehlerhaften Zustand auf einen gewünschten zurückzugehen. [9]

3.2.3 Availability – Verfügbarkeit

Verfügbarkeit kann vor allem durch das regelmäßige Warten der Systeme erzielt werden: Defekte Hardware wird so bald wie möglich repariert und das Betriebssystem wird so gewartet, dass keine Softwarekonflikte entstehen können. Zusätzlich ist es notwendig die Systemsoftware immer aktuell zu halten, um eventuelle Sicherheitslücken zu schließen. Der Einsatz von redundanten Systemen, Failover-Clustern oder RAID-Systemen kann die Konsequenzen des Ausfalls von Hardware deutlich mildern. Backup-Kopien sollten bei einer geografisch isolierten Position aufbewahrt werden, welche eventuell sogar gegen Feuer und Wasser geschützt ist.
Weiters ist eine schnelle Desaster-Recovery essentiell für den schlimmsten Fall. Daher ist es unbedingt notwendig, dass ein Desaster-Recovery-Plan existiert. Darin müssen auch die unwahrscheinlichsten Szenarien, wie Naturkatastrophen oder der Ausbruch von Feuer bedacht werden.
Firewalls und Proxy-Server helfen gegen Downtime und unerreichbare Daten durch Aktionen wie eine Denial-Of-Service-Attacke. [9]

3.3 AES on Chip

Um Verschlüsselungen mit dem AES-Algorithmus schneller durchführen zu können, kann die Ver- und Entschlüsselung direkt auf Hardwareebene ausgeführt werden. Ein Beispiel dazu ist AES-Ni (New Instructionset) von Intel. AES-Ni enthält sechs neue Anweisungen, die die Verschlüsselung möglich machen. Intel hat sämtliche Westermere-CPUs mit dem Befehlssatz ausgestattet. [10]

„Intel nennt fünf verschiedene Einsatzgebiete, in denen die AES-Befehle zum Einsatz kommen können: beim Verschlüsseln kompletter Laufwerke (mittels Tools wie BitLocker, PGP oder TrueCrypt), beim Verschlüsseln von Archiven (beispielsweise 7-Zip oder WinZip), bei zugriffsbeschränktem HD-Material (Pay-to-Play), Internet-Sicherheit und der VoIP-Kommunikation.“ – [10]

4 Authentication, Authorization, Accounting

N-1

5 Desaster Recovery

Voting Systeme

Hardware mit Votern
Es gibt Microcontroller die das am Chip erledigen

Heterogene Microcontroller kombinieren

Man verwendet verschiedene Systeme, damit, wenn eins ausfällt, das andere noch geht.

- Wenn ich in einem System immer den gleichen mc hab, und einer aufgrund Systemabhängiger Sachen ausfällt, wird ein anderer wahrscheinlich noch gehen.

Ausfallsicherheit

- Was mach ich einer der heterogenen Microcontroller ausfällt?

6 Algorithmen und Protokolle

6.1 Drahtlose Kommunikation zwischen Mikrocontrollern

6.1.1 WiFi

WiFi-Verbindungen sind bei vielen Entwicklern weit verbreitet, besonders da sie in so gut wie jedem Haushalt zu finden sind. Die für diese Technologie benötigte Infrastruktur ist weit verbreitet, die eine sehr schnelle Übertragung, in kleinen, aber auch in sehr großen Datenmengen erlauben.

WiFi operiert normalerweise auf den Frequenzbändern 2.4 GHz und 5 GHz. Der derzeitig am weitesten verbreitete WiFi-Standard ist 802.11n, mit welchem ein Datentransfer von mehreren hunderten Megabit pro Sekunde möglich ist. Das eignet sich zwar gut für das Übertragen von Files oder Streaming, aber für viele IoT-Anwendungen ist der dadurch entstehende Stromverbrauch zu hoch. Die Reichweite eines WiFi-Netzwerks beträgt außerdem auf freier Fläche etwa 50 Meter, was für viele IoT-Anwendungen einfach zu wenig ist. [11]

6.1.2 ZigBee

ZigBee bringt eine große Basis an Operationen mit sich. Die meisten ZigBee-Profile basieren auf einem Standard für Netzwerkverbindungen über Funk, der auf dem Frequenzband 2.4 GHz arbeitet und nur relativ selten einen Datenaustausch voraussetzt. ZigBee-Gateways haben in Normalfall eine Reichweite von etwa 100 Meter.

ZigBee hat einige große Vorteile gegenüber anderen Funk-Technologien. Das Kommunizieren kostet sehr wenig Energie (laut der Website kommt ein Gerät jahrelang mit einer einzigen Batterie aus),

eine starke Security wird angeboten und durch die hohe Skalierbarkeit können in einem System auch sehr viele Endpunkte verwendet werden. Aus diesen Gründen eignet sich ZigBee zum Beispiel für Sensornetze im IoT und generell für M2M-Anwendungen.

Zusammengefasst: ZigBee-Gateways operieren auf lizenzfreien Frequenzbändern wie 2.4 GHz, 900 MHz und 868 MHz und können bis zu einer Reichweite von 100 Metern angesprochen werden. Daten können mit einer Geschwindigkeit von bis zu 250 kBit/s übertragen werden. [11]

7 Konsistenz und Datenhaltung

7.1 SD-Cards

SD-Karten sind in vielen Bereichen eine beliebte Speicherkartenlösung. Momentan sind die microSD-Karten im Umlauf, die die miniSD-Karten abgelöst haben. Diese haben sich aufgrund ihrer minimalen Abmessungen sehr schnell verbreitet und gelten im Handy-Bereich bereits als Standard. Praktischerweise können microSD-Karten über passende Adapter auch als miniSD- oder SD-Karten verwendet werden.

Ein wichtiger Faktor für den Erfolg der SD-Karte ist sicherlich auch die SD-Schnittstelle, die noch immer abwärtskompatibel zur SPI-Schnittstelle ist.

Was für Problematiken bei SD-Cards auf Mikrocontrollern
Identifikation eines Datensatzes/Information
Wenn ich eine Info auf einem Bus weiterleite, muss ich das identifizieren können

8 Abbildungsverzeichnis

Abbildung 1: Unabhängiges Netzwerk [1] 3
Abbildung 2: Hybrides Netzwerk [1] 3
Abbildung 3: Access-Point Netzwerk [1] 3
Abbildung 4: Bündige Version eines kapazitiven Sensors [6] 7
Abbildung 5: Nicht bündige Version eines kapazitiven Sensors [6] 7

9 Literaturverzeichnis

[1] D. Christin, A. Reinhardt, P. S. Mogre und R. Steinmetz, „Wireless Sensor Networks and the Internet of Things: Selected Challenges," Darmstadt, Germany.

[2] V. Prajzler, „LORA, LORAWAN AND LORIOT," 01 08 2015. [Online]. Available: https://loriot.io/lora-lorawan-loriot.html. [Zugriff am 05 06 2016].

[3] M. Rouse, „machine-to-machine (M2M)," TechTarget, [Online]. Available: http://internetofthingsagenda.techtarget.com/definition/machine-to-machine-M2M. [Zugriff am 02 06 2016].

[4] T. Wedemeyer, „Grundlegende Informationen zum CAN-Bus," [Online]. Available: http://www.thomas-wedemeyer.de/uploads/File/CAN.PDF. [Zugriff am 02 06 2016].

[5] ITWissen, „GPIB (general purpose interface bus)," [Online]. Available: http://www.itwissen.info/definition/lexikon/general-purpose-interface-bus-GPIB-GPIB-System.html. [Zugriff am 02 06 2016].

[6] SensoPart, „Kapazitive Sensoren - SensoPart," [Online]. Available: www.sensopart.com/jdownloads/Gesamtkatalog/Kapazitve_Sensoren.pdf. [Zugriff am 05 06 2016].

[7] SensoPart, „Induktive Sensoren - SensoPart," [Online]. Available: http://www.sensopart.com/jdownloads/Gesamtkatalog/Induktive_Sensoren.pdf. [Zugriff am 05 06 2016].

[8] D.-H. Do, Möglichkeiten des Nachweises der funktionalen Sicherheit von technischen Systemen, Wien, 2013.

[9] M. Haughn und S. Gibilisco, „confidentiality, integrity, and availability (CIA triad)," TechTarget, [Online]. Available: http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA. [Zugriff am 02 06 2016].

[10] B. Kraft, „Beschleunigte Verschlüsselung: AES-NI," tomshardware, [Online]. Available: http://www.tomshardware.de/Intel-Clarkdale-Core-i5-661,testberichte-240477-3.html. [Zugriff am 02 06 2016].