

Kurzbericht

1 Allgemeine Angaben

FKZ: 16KIS1684

Projekt: UltraSec

Thema: Sicherheitsarchitektur für eine UWB-basierte IoT-Anwendungsplattform

Antragsteller(in):

Bundesdruckerei GmbH
Kommandantenstrasse 18
10969 Berlin

Laufzeit: 01.09.2022 bis 28.02.2025
(kostenneutral verlängert bis 30.08.2025)

Verfasser: Dipl.-Ing. (FH) Olaf Dressel

Inhaltsverzeichnis

1	Allgemeine Angaben	1
2	Zusammenfassung und Ergebnis	2
3	Ausführlicher Schlussbericht	3
3.1	Ausgangssituation und Erwartung	3
3.2	Ableitung des Projektziels (Zieldarstellung und Vorgehensweise).....	4
3.3	Ergebnisdarlegung und Erläuterung.....	7
3.3.1	Initiierung und Nutzung der UWB Funktionen.....	7
3.3.2	Sicherheitsansätze der FIRA	8
3.3.3	Motivation für das UWB Mesh System	8
3.3.4	Design des UWB Mesh Systems	9
4	Verwertungsplan	10
5	Veröffentlichte Projektergebnisse:	10

2 Zusammenfassung und Ergebnis

Durch das Projektvorhaben UltraSec wurden die sicherheitstechnischen Voraussetzungen für einen hochsicheren Technologieansatz zur Vernetzung von lokalen Kommunikationspartnern (P2P/P2M/M2M) auf der Basis von UWB evaluiert, konzipiert, modelliert und prototypisch umgesetzt, der in der Zukunft den komfortablen Aufbau und Betrieb einer hochsicheren, einfach anzuwendenden und skalierenden, dynamisch anpassbaren digitalen Infrastruktur in der Qualität eines funkgebundenen Verwaltungsnetzwerkes ermöglicht. Die Projektpartner PHYSEC GmbH, Bundesdruckerei GmbH, NC Systems GmbH, das KKH Bochum, das Fraunhofer HHI, sowie die FU Berlin haben dieses gemeinsam durchgeführt und haben organisatorische, technische und praktische Aspekte am Beispiel einer Vernetzung von Krankenhaus IoT mit UWB untersucht. Die Bundesdruckerei hat hier den Fokus auf die Sicherheit des Verfahrens und entsprechende Lösungsansätze für den Praxispartner gesetzt.

UWB kann und soll die Sicherheit von Security Token mit der Kommunikationsfähigkeit anderer Verfahren kombinieren und ist somit eine Kerntechnologie in der (hoch)sicheren, resilienten Kommunikation von Personen mit den sie in Zukunft umgebenden technischen Systemen und deren zahlreicher automatischer Komponenten (secure IoT und Smart City) untereinander. Die Teilnehmer dieser lokalen Netze können z.B. Personen, Maschinen/Roboter, Infrastruktur oder Güter sein und die Kommunikationsdaten und die physischen Abstände zwischen ihnen sollen hohen Sicherheitsanforderungen und Verfügbarkeiten genügen.

Die technischen Voraussetzungen der Technologie insbesondere im Anwendungsfall Krankenhaus wurden sehr positiv bewertet, da UWB als Kommunikationsverfahren einen äußerst geringen, breitbandigen Signalpegel hat und nahezu bedenkenlos neben anderen Funktechnologien verwendet werden kann. Auch wurden Studien hinsichtlich der physiologischen Auswirkungen auf Personen gesichtet, die auch hier jegliche Beeinflussung ausschließen. Dies spricht für eine gute Ausgangssituation zur Verwendung im Bereich der humanoiden Medizin und medizinischen Geräten und Einrichtungen.

Die Technologie hat sich in den 3 Jahren des Projektes sehr schnell, insbesondere durch die sehr intensiven Standardisierungsverfahren der FIRA, weiterentwickelt. An dieser Stelle wurden die Anwendungen gegenüber der Sicherheit priorisiert, was der Zielstellung dieses Projektes in Teilen nicht entsprach. Im Rahmen des Projektes wurden zahlreiche Forschungsarbeiten recherchiert und gesichtet, um detaillierte Hinweise auf möglicherweise bereits detektierte oder korrigierte Schwachstellen zu finden.

Die aufgrund der Technologie der Laufzeitmessung, des sehr breitbandigen Signals mögliche, sicher beweisbare Abstandsmessung zwischen den Teilnehmern kann durch technische Einflussnahmen nur in engen Grenzen beeinträchtigt werden. Die Robustheit des Systems wurde durch die Projektpartner evaluiert und es können durch die organisatorische Umsetzung einer qualitativen Überwachung des Signaltransfers mögliche Angriffe sofort detektiert werden. Es gibt nur sehr wenig erfolgreiche Angriffe auf die Qualität der Abstandsmessung, welche wiederum durch geeignete Maßnahmen detektiert und unterbunden werden können. Da es im Markt eine noch recht neue Technologie ist, sind weitere Angriffsvektoren nicht endgültig auszuschließen.

Die Initiierung der Abstandsmessung durch andere, weniger sichere Verfahren (Bluetooth) und die in der Folge der weiteren Prozessierung durch eben diese ist sicher ein Grund, dass die sehr gute Kommunikationsfähigkeit von UWB trotz der möglichen hohen Datenrate (30Mbits/s) und der sehr geringen Latenz (<<10ms) nicht intensiver genutzt wird.

Im Projekt wurde strikt vom Gedanken eines „pure UWB“ ausgegangen, so dass nicht nur die Abstandsmessung, sondern auch der gesamte Datenverkehr verschlüsselt, primär über UWB verarbeitet werden kann (selbstvernetzende und selbstüberwachende Systeme). Dadurch wird sichergestellt, dass - mindestens initial - nur physisch interagierende Komponenten Teilnehmer des Systems werden dürfen. Deren in der Fortführung kontinuierliche physische Interaktion ergibt eine überprüfbare Anordnung und ein definiertes Kommunikationsverhalten mit klaren Indizien für gegebenenfalls stattfindende Angriffe und optionale Maßnahmen.

Die insgesamt sehr positiv ausgefallene Einschätzung der UWB-Technologie liefert eine nahezu perfekte Ausgangslage, um UWB als Mesh-System in der Qualität eines funkbasierten Verwaltungsnetzwerkes weiterzuentwickeln. Die Sicherheitskriterien des BSI „Besitz, Wissen, Inhärenz“ sowie Verfügbarkeit u.a. kann durch Bereitstellung eines physisch beweisbaren Ortes hervorragend für ein durchgängiges Zero Trust-Konzept von KRITIS Anbietern verwendet werden. Geht man davon aus, kritische Komponenten mit UWB räumlich zu verbinden, so können darüber physisch beweisbare und kaum angreifbare Daten erzeugt werden, um Zero-Trust Voraussetzungen zu schaffen.

Die Anwendungen für ein auf dieser Basis konzipiertes Mesh-Netzwerk sind zum Beispiel elektronische Identitäten zur Nutzung als physische Freigabe von Türen oder IT-Geräten, Verteilung von Zugangsdaten über die örtliche Präsenz, Geräteüberwachung, Neustart und Firmwareupdates, ohne möglicherweise korrumpierte Datenwege zu nutzen. Im Rahmen des Projektes wurde einiges exemplarisch umgesetzt.

Fazit :

Durch die im Projekt gewonnen Erkenntnisse und Erfahrungen konnte nun klar nachgewiesen werden, dass durch UWB eine sehr hohe Sicherheit und Verfügbarkeit von IoT und ID-Systemen auch mit einem funkbasierten Verfahren erzielt werden kann. Trotz dieser erzielbaren sehr hohen Sicherheit kommt es aber nicht zwingend zu Funktionseinschränkungen, sondern es können zudem zahlreiche Mehrwerte für Prozesse und Benutzer erreicht werden. Die Umsetzung eines solchen hochverfügbaren und sicheren Systems bedingt zwingend die Einbindung mehrerer Anwendungen auf der Grundlage einer gemeinsamen Nutzungsdefinition, reduziert sowohl die Kosten und unterstützt technisch eine technisch gesicherte, gemeinsame Datenlage.

3 Ausführlicher Schlussbericht

3.1 Ausgangssituation und Erwartung

Bei Projektbeginn 2022 gab es bereits einige wenige Hersteller für UWB geeignete Hardware gab (u.a. die Unternehmen NXP, Quorvo). Auch gab es bereits die ersten Phasen der umfangreichen Kommerzialisierung der Technologie durch zum Beispiel Organisationen wie die FIRA und die UWB Association. Zu diesen wurden bereits vor Projektbeginn Kontakte hergestellt, eine Mitgliedschaft aufgrund der nicht unmittelbar anstehenden Kommerzialisierung jedoch nicht angestrebt. Im Zeitraum des Projektes hat sich der Anbietermarkt deutlich verstärkt und die UWB-Anwendungen haben stark zugenommen.

Die zu Projektbeginn favorisierte Verwendung von UWB war die sehr genaue Abstandsmessung auf Grundlage der Berechnung der Signallaufzeit und in Abhängigkeit der Anzahl der beteiligten Kommunikationspartner auch die Berechenbarkeit des Abstands (ca.

0...15m, bis zu 0.1 m genau) bis hin zu einer genauen örtlichen Triangulation und Verortung innerhalb eines abgedeckten Bereiches. Einige Besonderheiten ergaben sich insbesondere aus der Art des verwendeten Signals, nämlich eines energetisch sehr schwachen, dafür aber sehr breitbandigen getakteten Signals (500 MHz), welches neben einer sehr geringen Signallaufzeit (<50us) doch hohe Datenraten von bis zu 30 Mbit/s erlaubt. Die favorisierten Applikationen sind im Automobilbereich (physische Zugangskontrolle, Fahrzeugsteuerung, explizit über das CCC Konsortium) und im Logistikbereich angesiedelt. Im Bereich Consumer gab es zu diesem Zeitpunkt die ersten Geräte, welche diese Technologie integriert haben, jedoch noch kein einheitliches Gesamtkonzept („near by“ von Fa. Google war der erste Ansatz)

Aus all diesen zusammengetragenen Informationen ergab sich vage die Möglichkeit, mit UWB erstmalig eine Technologie in der „Hand zu haben“, welche trotz stark erhöhter Sicherheit, dem Benutzer/der Anwendung keine Einschränkungen auferlegt, sondern ebenfalls eine Reihe von Vorteilen bietet. Aus der klassischen Sicht „Besitz, Wissen, Inhärenz“ könnte nun der „Ort“ eine zusätzliche Rolle spielen. Die Dokumentationspflicht im Krankenhaus kann bei Eignung des Verfahrens zahlreiche automatisierte Datenereignisse erzeugen.

Wie definiert man also das Einsatzgebiet, die Anwendbarkeit und die Sicherheit für diesen konkreten Fall, was geht per se, was muss organisatorisch geregelt werden, was kann gegebenenfalls standardisiert werden-?

3.2 Ableitung des Projektziels (Zieldarstellung und Vorgehensweise)

Das Ziel des Projektes war es - am konkreten Anwendungsszenario Krankenhaus - zu untersuchen, welche Möglichkeiten die UWB-Technologie im Bezug auf eine Verbesserung der praktischen (physischen) IT-Sicherheit bieten kann und wie sich die technische Ausgangslage darstellt, welche Vor- und/oder Nachteile im Bezug auf bekannte bzw. eingesetzte Technologien bestehen und wie eine Umsetzung der Technologie ggf. bestehende Nachteile beseitigen und weitere Vorteile generieren könnte. Die am Projekt beteiligten Expertisen haben dann in ihren jeweiligen Schwerpunktthemen gezielte Herausforderungen untersucht.

Die Bundesdruckerei GmbH als Hersteller von ID-Lösungen hat nun in ihrem Arbeitspaket insbesondere auf die Thematik fokussiert, welchen Grad an Sicherheit man in UWB bisher erreicht hat oder was notwendig wäre, um einen Einsatz im Kontext „Hochsichere Systeme“ anstreben zu können. Gerade die Interaktion von Mensch Maschine/Systemen unter der Voraussetzung einer nachgewiesenen Identität (ID) ist betrachtenswert. Das dies für KRITIS Infrastrukturen und Prozesse relevant werden kann, war eine der Grundannahmen. Die Basis der Einordnung für Systemsicherheit und Anwendbarkeit wird von den z.T. vergleichbaren Technologien wie NFC, Bluetooth und WiFi gebildet.

Für das konkrete Ziel (im Kontext des betrachteten Falls Krankenhaus) wurden mit dem Projektpartner (KKB) zahlreiche Gespräche und Diskussionen geführt, in welchem die möglichen, aber auch die gewünschten Anwendungsfälle im Krankenhaus diskutiert wurden. Am Anfang wurden vorrangig die erzielbaren Mehrwerte bei bekannten Prozessen, durch z.B. die automatisierte Verortung von Prozessschritten, aber auch hier bereits durch mögliche Sicherheitsgewinne, adressiert. Da die zuverlässige Prozessdokumentation eine große Rolle spielt, wurde dies als weiteres Verwendungsziel verortet. „Zuverlässig“ referenziert hier klar PRO Sicherheit – der manipulations- und störungsfreie Langzeitbetrieb.

THESEN

UWB benötigt eine Systemlandschaft / Infrastruktur.
 UWB liefert eine absolute Ortsinformation innerhalb dieser.
 UWB ist sicher.

UWB Kommunikation und deren Sicherheit ist technisch / mathematisch beweisbar !

- 2 und mehr Geräte kommunizieren per Funk, die physikalische Interaktion ist technisch/mathematisch beweisbar.
- Die Kommunikation ist nicht oder nur schwer detektierbar.
- Die Kommunikation ist nicht oder nur schwer störfähig.
- Die Kommunikation ist nicht oder nur schwer abhörbar.
- Die Kommunikation ist nicht oder nur schwer zu manipulieren.
- Die Kommunikation lässt keine eindeutige / eindeutige Zuordnung des Senders zu.

Gegenüberstellung ausgewählter Übertragungstechnologien	LTE	5G	WiFi	BT / LE	LoRa	ZigBee (vgl.)	NFC	UWB
Störungsresistenz	●	●	●	●	●	●	●	●
Ortungsgenauigkeit	●	●	●	●	●	●	●	●
Strahlungsaarm	●	●	●	●	●	●	●	●
Hohe Datenrate	●	●	●	●	●	●	●	●
Hohe Echtzeitfähigkeit	●	●	●	●	●	●	●	●
Geringer Hardwareaufwand	●	●	●	●	●	●	●	●
Geringer Energiebedarf	●	●	●	●	●	●	●	●
Geringer Sicherheitsaufwand	●	●	●	●	●	●	●	●

Wie ist der Stand der Technik. Welche Verschlüsselung für UWB ist „die beste“ Wie beeinflusst UWB und wie kann es beeinflusst werden ? Wie ergänzt UWB Infrastrukturen oder ersetzt diese zum Teil ?

ultraSEC

Abbildung 1 - Ausgangsthesen des Projekts

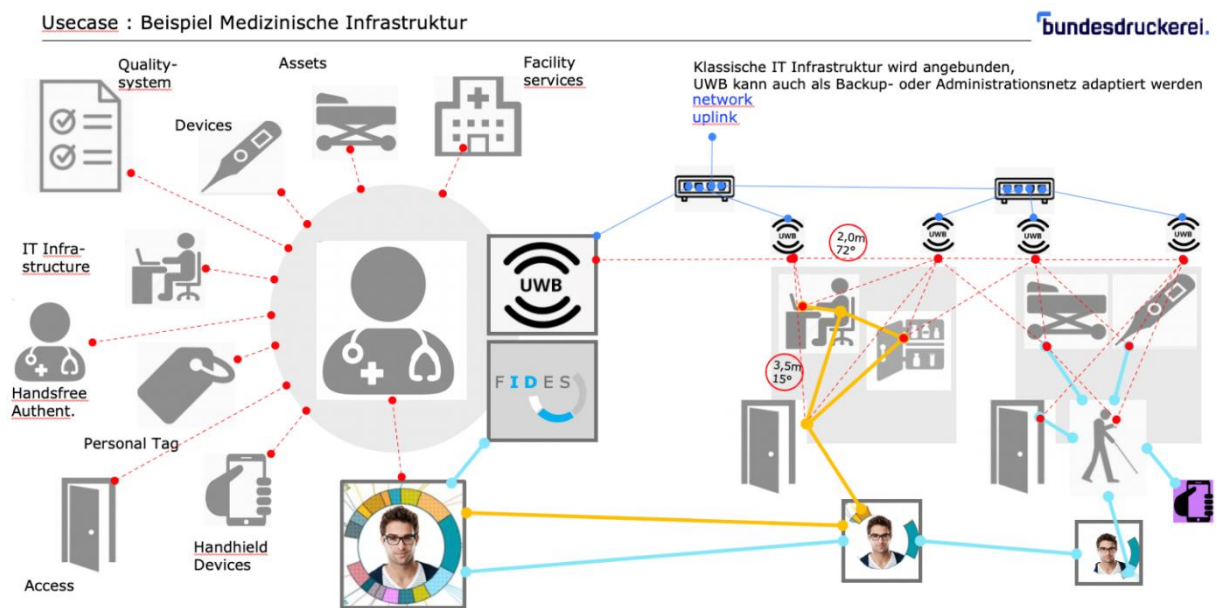


Abbildung 2 - Mögliche Anwendungen (Person+Rolle)

Es seien an dieser Stelle einige aussagekräftige Anwendungsbeispiele genannt:

„Wischmopp“ – eine exakte Ortung der Aktivitäten eines Reinigungsvorgangs, in z.B. einem Patientenzimmer, zeitlicher und qualitativer Nachweis des Prozesses, Abrechnungsparameter und Verbrauchsmittelabschätzung, -nachbestellung etc. Auch Datenschutz spielt hier eine Rolle, da ja Arbeitsleistungen von Mitarbeitern erfasst und ausgewertet werden können.

„Patientenbett“ – Bereitstellung der Informationen für berechtigtes Personal in angepasster Darstellungstiefe am Display vor Ort (Datenschutz), Abrechnung Personalzeiten per Fall, Nutzungsanalyse, zusätzliche Sensorik, Verortung des Betts und dessen Status im Klinikgelände, Wartung/Reinigung/Verfügbarkeit u.v.a.m.

„Diebstahl“ – eine unerwartet starke, negative Kennzahl in öffentlich zugänglichen Gebäuden – das betrifft nicht nur Verbrauchsmaterial (der Zugang zu den Vorratsräumen ist oft nicht gesichert) – es sind auch oft technisch notwendige, hochpreisige Gegenstände.

Es wurden zahlreiche weitere Fälle dokumentiert, diskutiert und hinsichtlich des Mehrwertes und des notwendigen Sicherheitsniveaus diskutiert. Dies führt nun unmittelbar auch zu einer Darstellung des Lebenszyklus eines Gerätes, welches sich innerhalb der Infrastruktur „bewegt“ und das daraus resultierende Netzwerk, welches diese Fälle abdecken muß.

Beispiel 2/3 : IM Patientenzimmer

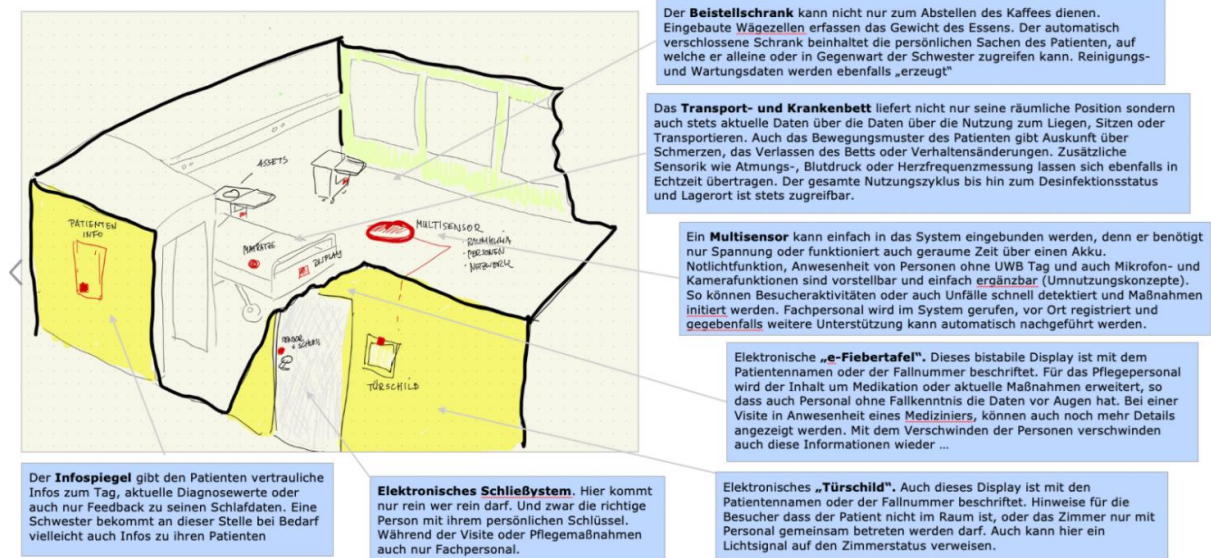


Abbildung 3 - IoT Geräte im Patientenzimmer

Beispiel 3/3 : VOR dem Patientenzimmer

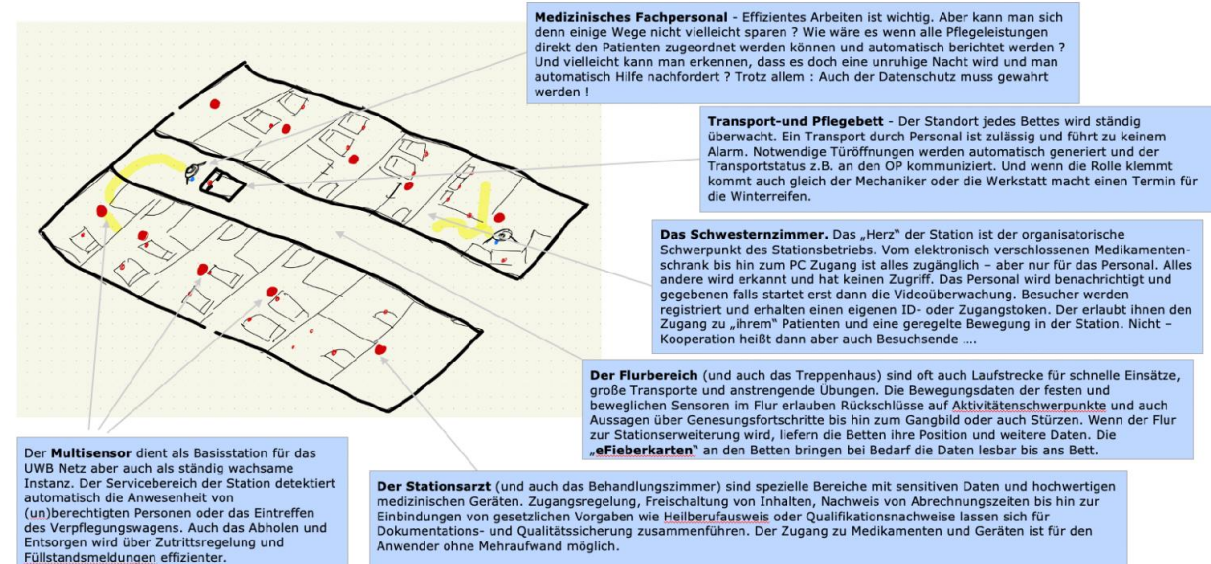


Abbildung 4 - IoT Geräte im Klinikbereich

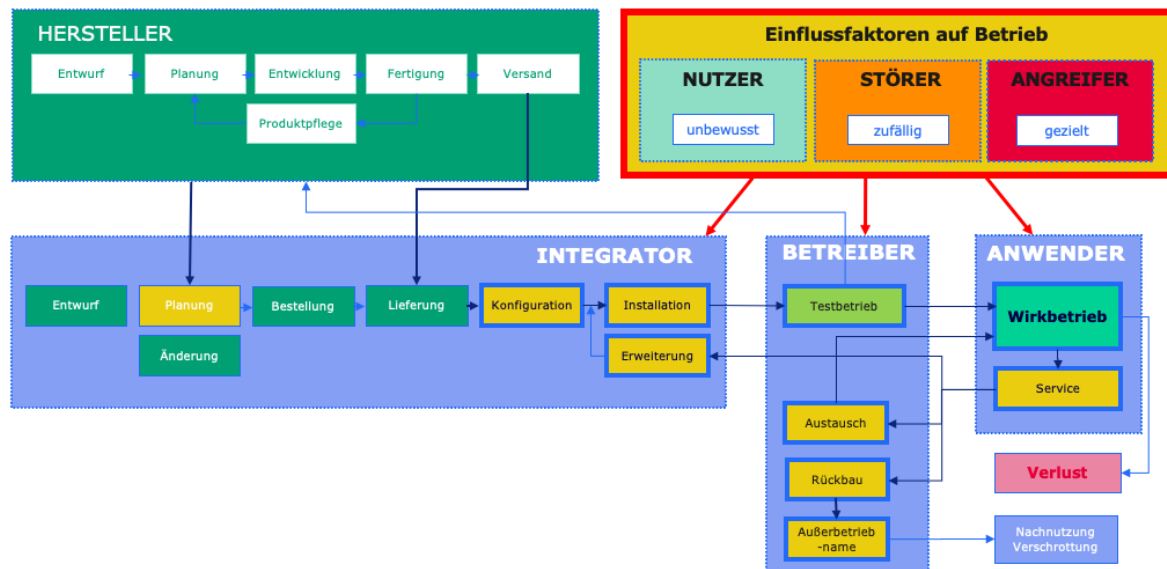


Abbildung 5- Lebenszyklus UWB Gerät

Es hat sich sehr schnell gezeigt, dass es mehrere Anwendungsdomänen gibt, wobei bei geeignetem Design durchaus eine Architektur entworfen werden kann, die ausgehend von der höchsten Anforderungspriorität sehr sicher, verfügbar und rein über Konfiguration anschließend mehrere Anwendungsbereiche abdeckt (Plattformgedanke). Damit werden in der Folge auch bessere, einheitlichere und validierbare Daten erzeugt, die über automatisierte Prozesse verlässlicher prozessiert werden können. Als Nebeneffekt benötigt man dann auch nur noch EIN IoT System, anstelle je eines per Anwendungsfall - zusätzlich aller Anschaffungs-, Pflege und Auditkosten.

3.3 Ergebnisdarlegung und Erläuterung

Im Bezug auf den Entwurf eines geeigneten Systems war zunächst eine Definition des Basissystems notwendig. Die Kommunikation zwischen nur 2 Komponenten ist grundsätzlich auch möglich, aber wird nicht primär betrachtet (z.B. Türschloss + Anker – Person mit Token/Handy). Bei 2 Teilnehmern ist nur eine reine Abstandsmessung möglich (Umkreismessung), bei 3 Teilnehmern ist bereits die Festlegung auf 2 Positionen möglich (gespiegelte Referenz) und ab 4 Teilnehmern kann eine Triangulation vorgenommen werden.

Die häufigsten UWB-Systeme findet man aktuell in der Logistik (RTLS) und diese arbeiten oft mit LAN/WLAN und UWB, meist nur mit sehr geringen Datenmengen und mit hohen, energiesparenden Latenzen. Dies wurde relativ früh im Projekt erkannt und die Verwendung von klassischer RTLS im Krankenhausumfeld ist sicher möglich und auch sinnvoll, aber stark für den Anwendungsfall Logistik beschränkt. Das langsam wachsende Sicherheitsbewusstsein ist bedingt vorhanden, oft wird keine Verschlüsselung aktiviert, bei älteren Systemen ist häufig nur AES-128 möglich, aktuell sollte mindestens AES-256, so inzwischen auch wie von der FIRA definiert, mindestens vorgesehen werden.

3.3.1 Initiierung und Nutzung der UWB Funktionen

Die, auch aus Gründen der Marktdurchdringung von der FIRA favorisierte Herangehensweise, eine Initiierung der Messung nach einem Bluetooth-Connect zu starten, ist insbesondere

energetisch begründet, erscheint aus sicherheitstechnischer Sicht zunächst aber ungünstig. An dieser Stelle kommt zum Tragen, dass UWB a la FIRA natürlich primär einen anderen Fokus hat, nämlich die Verbreitung der Technologie und damit insbesondere unter Nutzung / Kompatibilität zu bekannter und verbreiteter Technologie wie eben Bluetooth.

Der größte Energiebedarf tritt nicht beim Senden einer Information auf (es handelt sich um ultrakurze Impulse mit sehr geringer Energie) sondern durch stetigen Empfang und der darauffolgenden Signalanalyse. Die beiden definierten Modulationsverfahren HRP (high rate puls - dies ist das von der FIRA favorisierte Verfahren) und LRP (low rate puls) unterscheiden sich in der Signalform, im niedrigeren Energiebedarf von LRP und geringerer Datenrate. Eine Kombination beider Verfahren scheint den Verzicht auf Bluetooth in speziellen Anwendungen möglich zu machen. Die Empfehlung lautet an dieser Stelle, mit einer sicheren Kommunikationsmethode einen möglichst hohen Vertrauenslevel initial bereit zu stellen – NFC scheint hier für das Pairing sehr gut geeignet. Basierend auf dem Konzept „ZERO TRUST“ werden dann ausschließlich nur bereits validierte Teilnehmer mit aktivierter Verschlüsselung im System akzeptiert.

In der FIRA wird die Kommunikation auch über NFC ebenfalls angesprochen, jedoch nachrangig zu Bluetooth. Beide dienen lediglich dazu, UWB zur Abstandsmessung zu initiieren. Eine Initiierung direkt über UWB (ohne eine der beiden anderen Technologien im täglichen Gebrauch zu nutzen) ist derzeit nicht favorisiert, dies könnte sich aber im Hinblick auf die verbesserten Eigenschaften z.B. durch UWB LRP möglicherweise ändern.

3.3.2 Sicherheitsansätze der FIRA

An dieser Stelle kommt bei UWB der Unterschied zum Tragen, dass es nicht wie Bluetooth auf einzelnen, festgelegten und zuverlässig detektier- und störbaren Frequenzen arbeitet. Auch ist der unter Umständen angreifbare Protokoll Stack hier wesentlich kleiner und es ist bei sicherheitsgemäßer Umsetzung von Beginn an nur eine Kommunikation der Kommunikationspartner mit zuvor bekannten Schlüsselmaterial möglich (a la VPN).

Die FIRA hat zur Sicherung gegen mögliche Angriffe, insbesondere mit Blick auch auf das initiierte Bluetooth, Verfahren wie PAAST (Pre-Authorized Access Service Token), Rate Limiting und STS auf dem physischen Layer implementiert. Diese Verfahren sollen sicherstellen, dass UWB erst dann eingesetzt wird, wenn definierte Voraussetzungen und keine Angriffe (Bluetooth !!!) vorliegen.

3.3.3 Motivation für das UWB Mesh System

Wenn man die Zielstellung eines hochsicheren IoT Systems verfolgt, dann geschieht das mit dem Ziel, dass nachfolgende bzw. direkt eingebundene Prozesse beweisbar auf Verfügbarkeit, Validität und Vertrauen der Infrastruktur und zu denen von ihr generierten Daten setzen können. Das betrifft auch die Verlässlichkeit bei, durch die Infrastruktur zu übertragenden Informationen, wie beispielsweise Sicherheitssteuerungen, Updates oder Schlüsselmaterial.

Alle anderen Konzepte, welche nicht konsequent nach Zero-Trust-Regeln designt werden, sind im Nachgang zu einer bestehenden Systemarchitektur nicht oder nur mit sehr hohem Aufwand umzusetzen.

Diese Betrachtungen flossen u.a. in die Erstellung der Secrecymaps, die Fragestellung nach Privacy bei UWB (Tracking bestimmter Geräte aufgrund physischer Eigenschaften) oder die

Umsetzung in Hardware durch eben ein vollständig im UWB Protokoll inkludierten Vernetzungslayer ein. (Anm. siehe dazu Berichte der Projektpartner)

Aktuell wird UWB primär für das sehr genaue Ranging zwischen einer oder mehreren Instanzen verwendet. Die Berechnung der Position kann nun auf Seiten der Infrastruktur oder auf Seiten des Empfängers erfolgen. Die Infrastruktur wird i.d.R. durch sogenannte Anker gestellt, also örtlich mindestens zueinander räumlich referenzierbare UWB fähige Geräte.

3.3.4 Design des UWB Mesh Systems

Ein UWB- System besteht i.d.R. bei UWB aus „Ankern“, die eine bekannte und prüfbare örtliche absolute oder relative Position einnehmen und die Referenz bilden. Sie kommunizieren untereinander per LAN oder auch WLAN, vorzugsweise aber mit einer separaten, abgesicherten Kommunikationsschicht innerhalb von UWB, was neben einer geringeren Angriffsfläche auf andere Technologien auch zu einer kontinuierlichen dynamischen Validierung der Infrastruktur genutzt werden kann. Erweiternd ist damit auch ein Mesh System möglich, welches den Ausfall oder Anomalien in Bezug auf bauliche oder Signalveränderungen einer oder mehrerer Komponenten in Echtzeit feststellen und in vielen Punkten auch gezielt kompensieren kann.

Bei Bedarf eines absolut georeferenzierten UND beweisbaren Systems, kann eine physisch fest positionierte Grundanordnung von Ankern exakt vermessen und zertifiziert werden. Sobald sich diese Werte in unbestimmter Weise verändern, können entsprechende Strategien zum Einsatz kommen, wie der Entzug von Recht, der Verfall von Zertifikaten usw. Hier handelt sich dann tatsächlich um die beweisbare Verknüpfung „Besitz, Wissen, Inhärenz“, Vertraulichkeit, Verfügbarkeit und den physischen Ort.

Natürlich sind auch einfachere Ansätze denkbar, wie eine relative Positionierung wo es vor allem um die Positionierung in oder um einen Bereich geht, dass sich dieser Bereich in seiner Größe nicht verändert und die Funktion sichergestellt ist. Anwendbar zum Beispiel auf Transporteinheiten (Schiff, Bus etc.) oder mobilen Installationen (Lagerplätze, Zeltanlagen etc.).

Die Anker des Systems überprüfen die Position ihrer Nachbarn, die Validität der Signale und auch gegebenenfalls auftretende Ausfälle. Durch das System benachbarter Anker können auch priorisierte Informationskanäle reserviert werden, damit sind Konzepte wie verteilter Code und Multifaktor Authentifizierung von Hardware und verschiedenes andere möglich.

Wenn man ein Mesh unter diesen Voraussetzungen betreibt, dann lassen sich zahlreiche Prozesse inklusive möglicher sicherheitstechnischer Beweise (Signatur, Zeitstempel und nun natürlich auch Ort) mit höchsten Ansprüchen an ihre Rechtmäßigkeit automatisieren.

Verschiedene Nachweisfragen in dem im Projekt betrachteten Krankenhaus (und mit reinem UWB sogar direkt im Operationssaal möglich) seien hier genannt – andere Funktionen zum Thema Datenschutz wurde bereits weiter oben angeführt. Es ist selbsterklärend, dass viele der Funktionen auch in anderen öffentlichen Gebäuden oder im SmartCity Kontext passend sind.

Insbesondere mit Bezug auf eine zuverlässige Personenzuordnung eines UWB Gerätes zu einer Person über einen tragbaren ID-Token mit Bewegungsanalyse, UWB-fähige Mobilgeräte mit eigene Authentisierungsverfahren oder auch dediziert aufgestellte biometrische Authentisierungsstationen, auch in Kombination mit anderen Geräten / Wearables.

Hier einige weitere Prozessanwendungen :

- Protokollierung von Behandlungszeiten und Personen beim Patienten
- Nachweis von Experten und der räumlichen Aktivität während einer OP
- Automatisierte Öffnung und Buchung von Räumen, Schränken oder Behältnissen mit Medikamenten und Material
- Verfolgung und Kontrolle über den Nutzungszyklus von Pflegebetten
- Kompletverschluss physischer Zugangsbereiche nur exklusiv und ohne merkbare Einschränkungen für authentifizierte Personen
- Freischaltung von Gerätefunktionen je nach Rolle/Befähigung
- Ortung, Verfolgung und/oder Deaktivierung von markiertem Material / Geräten

Mit der Nutzung eines durchgängig sicherheitstechnisch validierten Meshsystems ist es also vorstellbar, Ereignisdaten mit sehr hohen Nachweisanforderungen direkt am Entstehungsort zu erzeugen. Am konkreten Beispiel kann das dazu genutzt werden, dass die kontinuierliche Anwesenheit eines Anästhesisten im OP an einem bestimmten Ort als beweisbarer Datensatz automatisiert generiert werden kann.

Abschließend ist festzustellen, dass das im Projekt betrachtete UWB-Kommunikationsverfahren sehr viele überzeugende Eigenschaften aufweist, die einen Einsatz für sicherheitskritische Anwendungen im lokalen Kontext bei Wahrung möglichst geringer Sicherheitseinschränkungen hervorragend eignet. Eine entsprechende Definition / Standard für diesen Einsatz steht noch aus.

Weitere Herausforderungen für ein komplettes System, welche auch die mobile Authentifizierung der Personen oder die Detektion und Verortung (z.B. UWB-Radar) nicht authentifzierter Personen berücksichtigt, sind noch zu lösen.

4 Verwertungsplan

Die erzielten Ergebnisse entsprechen den Erwartungen.

Mit dem Projekt ist kein verwertbarer Zustand entstanden.

5 Veröffentlichte Projektergebnisse:

- Zahlreiche Präsentationen, in Teilen auch zusammen mit Projektpartnern
 - NXP (uwb Chiphersteller - insbesondere auch mit Bezug auf FIRA)
 - Infineon (uwb Chiphersteller - insbesondere auch mit Bezug auf FIRA)
 - uwb RTLS Hersteller : Kinexon AG München, Sewio, AIRTLS b.v.
 - Messtechnik : Rhode & Schwarz, Aronia, Tektronix
 - Charité zu Berlin, Bereich IT; Uniklinikum Freiburg, Klinikum HH-Harburg
 - Sonstiges : BSI
 - Firmen : Genua GmbH, Omnikey, Elatec,