

Facharbeit

Nutzung offener WLAN-Netze im Feuerwehreinsatz

Verfasser: **Max Schmid, M. Sc.**
Brandreferendar
Basell Polyolefine GmbH
Brühler Str. 60
50389 Wesseling

Abgabeort/-datum: Münster, den 21.12.2018

Zusammenfassung

Die fortschreitende Digitalisierung und die damit einhergehenden wachsenden Datenmengen erfordern auch die Weiterentwicklung der Übertragungstechnologien sowie den ständigen Ausbau der Kommunikationsnetze. Eine Folge davon ist zum Beispiel die steigende Verbreitung offener WLAN-Netze („Hotspots“), über die Mitarbeitern, Kunden und Touristen in Kommunen und Betrieben ein freier Internetzugang zur Verfügung gestellt wird.

Im Bereich der Feuerwehr wird zur Datenübertragung hauptsächlich auf „eigene“ Netze, wie den BOS-Funk, zurückgegriffen. Da aber auch im Feuerwehreinsatz immer mehr Daten zur Verfügung stehen, die z. B. die Einsatzkoordination und -dokumentation oder die Sicherheit vorgehender Einsatzkräfte verbessern und erleichtern können, ergibt sich auch hier der Bedarf, alternative Datenübertragungswege zu prüfen. Die Frage, die die vorliegende Facharbeit behandelt, ist, ob sich offene WLAN-Netze zur Datenübertragung im Feuerwehreinsatz eignen.

Die Vorgehensweise bei der Bearbeitung konzentriert sich darauf, mögliche Anwendungsbereiche von offenen WLAN-Netzen im Feuerwehreinsatz zu beschreiben, Anforderungen an diese aus Sicht der Feuerwehr zu benennen und abschließend eine Bewertung vorzunehmen, indem Anforderungen und Leistungsmerkmale der Netze gegenübergestellt werden. Dafür wird insbesondere die Einschätzung von Experten herangezogen.

Im Ergebnis ergibt sich ein deutliches Bild. Offene WLAN-Netze können in den meisten Fällen die Anforderungen aus Feuerwehrsicht nicht, oder nur bedingt erfüllen. Gründe dafür ergeben sich insbesondere aus der Vielzahl unterschiedlicher Netze, Anbieter und Konfigurationen und den damit verbundenen unkontrollierbaren Rahmenbedingungen. Dies resultiert u.a. in einer mangelnden Ausfallsicherheit, einer schwachen Leistung durch die parallele Nutzung vieler Benutzer oder bestehenden Hürden bei der Einbuchung, z.B. durch vorgeschaltete Anmeldeseiten. Nur in Einzelfällen, wenn z.B. im Rahmen einer Vorplanung die genannten Hürden beseitigt werden können, kann eine Nutzung offener WLAN-Netze durch die Feuerwehr sinnvoll sein. Auch im Hinblick auf alternative Technologien, wie z.B. den Mobilfunk, wird daher aus heutiger Sicht davon abgeraten, die Nutzung offener WLAN-Netze im Feuerwehreinsatz flächendeckend zu verfolgen.

Inhaltsverzeichnis

ZUSAMMENFASSUNG	I
INHALTSVERZEICHNIS	II
ABBILDUNGSVERZEICHNIS.....	IV
TABELLENVERZEICHNIS.....	IV
ABKÜRZUNGSVERZEICHNIS	V
1 EINLEITUNG.....	1
1.1 Fragestellung und Eingrenzung.....	1
1.2 Zielsetzung	2
2 METHODIK.....	2
2.1 Vorgehensweise.....	2
2.2 Informationsbeschaffung	3
3 GRUNDLAGEN.....	3
3.1 Offene WLAN-Netze.....	4
3.2 Ausbauzustand offener WLAN-Netze in Deutschland	5
4 ANWENDUNGSMÖGLICHKEITEN VON WLAN IM FEUERWEHREINSATZ	5
4.1 Anwendungsbereich Einsatzkoordination und -dokumentation	6
4.2 Anwendungsbereich Überwachung von Einsatzkräften	7
4.3 Zusammenfassung der Anwendungsbereiche	8
5 STAND DER TECHNIK.....	8
5.1 Mobile Führungsunterstützungssysteme.....	9
5.2 Digitale Atemschutzüberwachung	9
5.3 Übermittlung von Vitaldaten	9
5.4 Übertragung von Bild- und Videomaterial.....	9
5.5 Ortung von Einsatzkräften.....	10
5.6 Sonderfall WLAN-Ortung.....	10
5.7 Trend zu eigenen Ad-Hoc- und Mobilfunknetzen	10
5.8 Zusammenfassung Stand der Technik.....	11
6 ANFORDERUNGEN AUS SICHT DER FEUERWEHR	11
6.1 Allgemeine Anforderungen	11
6.2 FwDV 800	12

7	GEGENÜBERSTELLUNG VON ANFORDERUNGEN UND LEISTUNGSMERKMALEN	13
7.1	Verfügbarkeit offener WLAN-Netze	13
7.1.1	WLAN-Abdeckung.....	13
7.1.2	Nutzbarkeit offener WLAN-Netze für die Feuerwehr	14
7.2	Leistungsfähigkeit offener WLAN-Netze.....	15
7.3	Datensicherheit offener WLAN-Netze	16
8	BEWERTUNG DER NUTZBARKEIT OFFENER WLAN-NETZE	16
8.1	Nutzung zur Einsatzkoordination und -dokumentation	17
8.2	Nutzung zur Überwachung der Einsatzkräfte	17
8.3	Diskussion	18
9	FAZIT	19
9.1	Alternativen	19
9.2	Ausblick.....	20
	QUELLENVERZEICHNIS.....	VI
	ANHANG.....	XI
	Anhang A: Aufgabenstellung für die vorliegende Arbeit	XII
	Anhang B: Abbildungen	XIII
	Anhang C: Übersicht über die Experteninterviews und sonstigen Anfragen	XIV
	Eidesstattliche Erklärung.....	XV

Abbildungsverzeichnis

ABBILDUNG 1: VORGEHENSWEISE BEI DER BEARBEITUNG DER VORLIEGENDEN FACHARBEIT (QUELLE: EIGENE DARSTELLUNG)	3
ABBILDUNG 2: SCHEMATISCHER AUFBAU EINES WLAN-HOTSPOTS (QUELLE: EIGENE DARSTELLUNG NACH HMWEVL 2017)	4
ABBILDUNG 3 – ANHANG: AUFGABENSTELLUNG FÜR DIE VORLIEGENDE ARBEIT	XII
ABBILDUNG 4 – ANHANG: FREIE HOTSPOTS PRO 10.000 EINWOHNER IM 4. QUARTAL 2014 IM VERGLEICH (QUELLE: LANDEFELD 2014).....	XIII
ABBILDUNG 5 – ANHANG: BEISPIEL FÜR DIE VON DER FIRMA DRÄGER GENUTZTEN TECHNOLOGIEN ZUR DATENÜBERTRAGUNG (QUELLE: DRÄGER O. J.B).....	XIII

Tabellenverzeichnis

TABELLE 1: ANWENDUNGSBEREICHE, FÜR DIE DIE NUTZUNG OFFENER WLAN-NETZE GEPRÜFT WERDEN SOLL	8
TABELLE 2: GRUNDSÄTZLICHE ANFORDERUNGEN, DIE BEI DER NUTZUNG OFFENER WLAN-NETZE GEPRÜFT WERDEN MÜSSEN	13
TABELLE 3 – ANHANG: IM RAHMEN DER ARBEIT BEFRAGTE EXPERTEN MIT ZUORDNUNG ZUM BERUFLICHEN HINTERGRUND SOWIE DEM SCHWERPUNKT DER JEWEILIGEN EXPERTISE	XIV

Abkürzungsverzeichnis

AFKzV	Ausschuss Feuerwehrangelegenheiten, Katastrophenschutz und zivile Verteidigung des Arbeitskreises V der Innenministerkonferenz
BDBOS	Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben
BMWi	Bundesministerium für Wirtschaft und Energie
BOS	Behörden und Organisationen mit Sicherheitsaufgaben
BSI	Bundesamt für Sicherheit in der Informationstechnik
DGAUM	Deutsche Gesellschaft für Arbeitsmedizin und Umweltmedizin
DMO	Direct Mode
DSL	Digital Subscriber Line
FAZ	Frankfurter Allgemeine Zeitung
FIT	Fraunhofer-Institut für Angewandte Informationstechnik
FwDV	Feuerwehr Dienstvorschrift
GPS	Global Positioning System
HMWEVL	Hessisches Ministerium für Wirtschaft, Energie, Verkehr und Landesentwicklung
IdF NRW	Institut der Feuerwehr Nordrhein-Westfalen
IEEE	Institute of Electrical and Electronics Engineers
IM NRW	Innenministerium des Landes Nordrhein-Westfalen
IT	Informationstechnik
IuK	Informations- und Kommunikationstechnik
MWIDE NRW	Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen
o. J.	ohne Jahr
OV	Ortsverband
RFID	Radio-Frequency Identification
SIM	Subscriber Identity Module
TETRA	Terrestrial Trunked Radio
THW	Technisches Hilfswerk
TMO	Trunked Mode
USV	Unterbrechungsfreie Stromversorgung
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
5G	Mobilfunkstandard der 5. Generation

1 Einleitung

Die Digitalisierung ist eines der beherrschenden Themen unserer Zeit. Sowohl im privaten als auch im beruflichen Umfeld gehen damit eine Vielzahl neuer, innovativer Möglichkeiten einher, die unsere Industrie und Gesellschaft tiefgreifend verändern.

Mit den wachsenden Datenmengen und der fortschreitenden Vernetzung steigen auch die Anforderungen an die Datenübertragungswege. Schnelle, leistungsfähige Übertragungsstandards sind die Basis einer erfolgreichen Digitalisierung.

Eine gängige und bekannte Möglichkeit der drahtlosen Datenübertragung sind WLAN-Netze (Wireless Local Area Network). Eine besondere Form davon sind die offenen, also für jedermann zugänglichen WLAN-Netze. Behörden und Betriebe stellen ihren Mitarbeitern, Gästen und Kunden auf diesem Weg einen mobilen Zugang zum Internet zur Verfügung. Kommunen erkennen im Ausbau von Hotspots im öffentlichen Raum Chancen, ihre Attraktivität für Bewohner und Touristen zu erhöhen. (Eisele et al. 2017)

Auch bei der Feuerwehr besteht wachsender Bedarf an drahtloser Datenkommunikation. Digitale Einsatzpläne, mobile Führungsunterstützungssysteme und der mobile Zugriff auf aktuelle Datenbanken anstelle von oft veralteten Plänen und Nachschlagewerken in Papierform sind nur einige Anwendungen, die sich heute schon mehr und mehr durchsetzen. Im Hinblick auf die Möglichkeiten, die die Digitalisierung bietet, erscheinen jedoch noch viele weitere Anwendungsbereiche sinnvoll. Eine digitale Übertragung von Vitaldaten oder Aufenthaltsorten vorgehender Einsatzkräfte könnte z. B. deren Sicherheit deutlich erhöhen. Vorliegende Echtzeit-Daten eines betroffenen Gebäudes könnten der Feuerwehr helfen, schnell Einsatzschwerpunkte zu erkennen und taktisch richtige Entscheidungen zu treffen.

Die Chancen, die durch die Nutzung kabelloser Datenübertragung am Einsatzort entstehen, sind vielfältig. Gleichzeitig gibt es eine stark wachsende Verbreitung von offenen WLAN-Netzen. Hieraus resultiert die Frage, ob und wie die Feuerwehr auf bestehende, offene WLAN-Netze zugreifen und sich diese zu Nutze machen kann. Dieser Fragestellung soll in der vorliegenden Arbeit nachgegangen werden.

1.1 Fragestellung und Eingrenzung

In dieser Facharbeit sollen die Möglichkeiten der Nutzung von offenen WLAN-Netzen im Feuerwehreinsatz untersucht und bewertet werden. Die Aufgabenstellung lautet wie folgt:

Nutzung offener WLAN-Netze im Feuerwehreinsatz

„Sowohl im betrieblichen Umfeld als auch in den Kommunen finden offene WLAN-Netze eine rasche Verbreitung. Wie können Feuerwehren diese neuen Datenübertragungswege für die Überwachung der Einsatzkräfte (Atemschutz, Vitaldaten, Technische Daten, ...), der Einsatzkoordination und -dokumentation nutzen?“¹

Die Fragestellung bezieht sich somit nicht generell auf WLAN-Netze als mögliche Übertragungswege, sondern speziell auf „offene WLAN-Netze“. Eine Definition und Eingrenzung des Begriffs „offenes WLAN-Netz“ erfolgt in Kapitel 3.1. Gemäß der o.g.

¹ Siehe auch Kopie der Aufgabenstellung des IdF NRW im Anhang A

Erläuterung zur Fragestellung soll die „Überwachung von Einsatzkräften“ sowie die „Einsatzkoordination und -dokumentation“ im Feuerwehreinsatz im Zentrum der Betrachtung stehen. Rettungsdienstliche Belange werden in der vorliegenden Arbeit nicht bewertet.

In der Erläuterung zur Aufgabenstellung werden offene WLAN-Netze als „Datenübertragungswege“ bezeichnet. Daraus folgt für diese Arbeit, dass der Fokus der Betrachtung darauf liegt, die Möglichkeit der *Datenübertragung* über offene WLAN-Netze – und zwar für die o.g. Anwendungsbereiche – zu bewerten.

Aufgrund der rasanten Entwicklung der Digitalisierung sind Vorhersagen für die Zukunft nur eingeschränkt möglich. Daher konzentriert sich diese Arbeit auf heute umsetzbare Anwendungsfälle.

1.2 Zielsetzung

Ziel der vorliegenden Arbeit ist es, eine Aussage dazu zu treffen, wie offene WLAN-Netze im Feuerwehreinsatz zur Übertragung von Daten genutzt werden können.

Im Ergebnis soll eine pragmatische und für den Bereich der Feuerwehr anwendungsbezogene Aussage dazu getroffen werden, ob eine Nutzung offener WLAN-Netze im Feuerwehreinsatz möglich und sinnvoll ist und welche Faktoren für oder gegen deren Verwendung sprechen.

2 Methodik

In diesem Kapitel wird dargestellt, wie bei der Beantwortung der Fragestellung methodisch vorgegangen wurde.

2.1 Vorgehensweise

Um bewerten zu können, wie offene WLAN-Netze im Feuerwehreinsatz genutzt werden können, muss das Thema aus unterschiedlichen Blickrichtungen betrachtet werden. Aus Anwendersicht muss definiert werden, welche Vorteile die Nutzung von offenen WLAN-Netzen gegenüber dem Status Quo bieten könnte und welche Anforderungen daran gestellt werden müssen. Auf der anderen Seite muss bewertet werden, ob offene WLAN-Netze diese Anforderungen erfüllen und damit überhaupt geeignet sind. Um die Fragestellung zu beantworten, wird daher eine Gliederung in mehrere Bearbeitungsschritte gewählt:

Nach einer kurzen Beschreibung der Grundlagen zum Thema (Kapitel 3) erfolgt eine Auseinandersetzung mit den in der Fragestellung genannten möglichen Anwendungsbereichen „Einsatzkoordination und -dokumentation“ sowie „Überwachung der Einsatzkräfte“ (Kapitel 4). Anschließend wird für beide Bereiche der Stand der Technik beschrieben (Kapitel 5).

In einem nächsten Schritt werden Anforderungen genannt, die aus Sicht der Feuerwehr an offene WLAN-Netze gestellt werden müssen, um diese nutzen zu können. Dazu wird maßgeblich die neu veröffentlichte Feuerwehr-Dienstvorschrift 800 (FwDV 800) herangezogen (Kapitel 6).

Schließlich werden die Anforderungen auf der einen und die tatsächlichen Leistungsmerkmale offener WLAN-Netze auf der anderen Seite gegenübergestellt und verglichen (Kapitel 7).

Aus der Gegenüberstellung wird im letzten Schritt abgeleitet, ob und für welche Anwendungen die Nutzung offener WLAN-Netze im Feuerwehreinsatz möglich und sinnvoll ist (Kapitel 8).

Die folgende Abbildung veranschaulicht die beschriebenen Bearbeitungsschritte und formuliert für jeden Schritt eine Leitfrage.

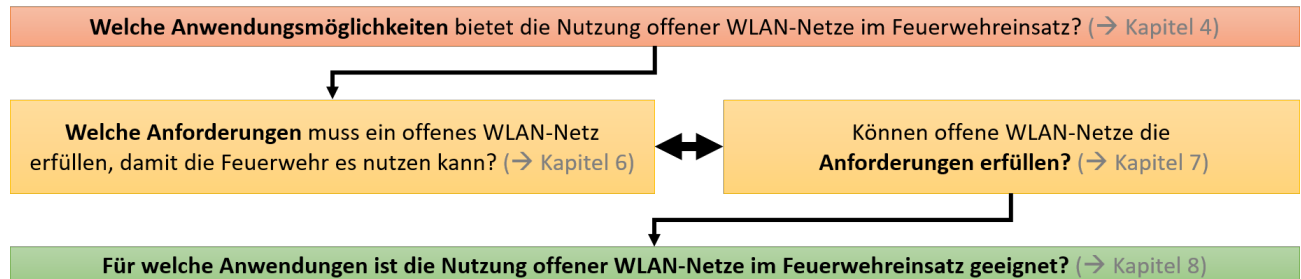


Abbildung 1: Vorgehensweise bei der Bearbeitung der vorliegenden Facharbeit (Quelle: Eigene Darstellung)

2.2 Informationsbeschaffung

Die Informationsbeschaffung für die vorliegende Arbeit teilt sich in eine Literaturrecherche und in eine Expertenbefragung auf. Auf Literaturrecherche basieren insbesondere die Beschreibung der Grundlagen, die Ausführung der Anwendungsbereiche und die Aufzeichnung des Stands der Technik. Für die Gegenüberstellung von Anforderungen und Leistungsmerkmalen offener WLAN-Netze wurde die Einschätzung von Experten herangezogen. Diese Methode ist deshalb dafür die geeignetste, weil die Schnittstelle zwischen Feuerwehr und offenen WLAN-Netzen eine sehr spezielle Anwendung darstellt, bei der eine praxisnahe Einschätzung von Personen mit Sachverstand unterschiedlicher Blickrichtungen notwendig ist. Es wurden Experten aus den Bereichen Feuerwehr (Anwendersicht), IT-Sicherheit und -Infrastruktur sowie Netzanbieter von WLAN-Infrastruktur befragt. Eine Übersicht über alle durchgeführten Interviews befindet sich neben den Angaben im Text und im Quellenverzeichnis zusätzlich im Anhang C.

3 Grundlagen

Der Begriff „WLAN“ (Wireless Local Area Network) bezeichnet lokale Netzwerke zur kabellosen Datenübertragung, die auf dem Datenübertragungsstandard IEEE 802.11 beruhen. Der Standard wurde in den 1990er Jahren vom Institute of Electrical and Electronics Engineers (IEEE) entwickelt. Heute werden für die Übertragung der Daten die Frequenzbänder 2,4 und 5 GHz genutzt, neuerdings z. T. auch das 60 GHz-Band. Die Merkmale von WLAN-Netzen sind hohe Datenübertragungsraten bei relativ kurzen Reichweiten. (HMWEVL 2017)

Seit Einführung der WLAN-Technologie wurden viele Weiterentwicklungen vorgenommen, sodass die Datenübertragungsgeschwindigkeiten heute deutlich über denen Mitte der 1990er Jahre liegen. Der heute gängige Standard IEEE 802.11n erreicht in der Praxis

Datenübertragungsraten von 70-150 MBit/s.² Der noch nicht weit verbreitete Nachfolgestandard IEEE 802.11ac erreicht unter normalen Bedingungen schon bis zu 400 MBit/s. (Sauter 2018) Andere Quellen sprechen zusammenfassend von heute typischen Nutzungsraten von bis zu 200 MBit/s. (HMWEVL 2017) Die Reichweite eines WLAN-Netzes kann bis zu ca. 300 m betragen. Sie hängt jedoch stark von Hindernissen oder davon ab, ob sich das WLAN-Netz im Freien oder in Gebäuden befindet. Ebenso spielt die genutzte Frequenz eine Rolle. (ebd.)

Im Vergleich dazu erreicht der Mobilfunkstandard LTE heute unter sehr guten Bedingungen eine Übertragungsrate von über 100 MBit/s bei einer deutlich höheren Reichweite von mehreren Kilometern. (Sauter 2018) Dabei ist jeweils zu berücksichtigen, dass die genannten Datenübertragungsgeschwindigkeiten in der Praxis oft deutlich geringer ausfallen. So kann die Datenübertragungsrate ins und aus dem Internet bei WLAN-Netzen immer nur so schnell sein, wie das Telekommunikationsnetz, über das der Hotspot angebunden ist (wie z. B. DSL).

WLAN-Netze können in unterschiedlichen Modi aufgebaut sein: Dem sogenannten *Ad-Hoc-Modus*, bei dem WLAN-fähige Geräte direkt miteinander kommunizieren, und dem *Infrastrukturmodus*, bei dem die Kommunikation vom Nutzer drahtlos zu einem Zugangspunkt (Access Point) und dann über einen Router ins Internet hergestellt wird.³ Der vorrangige Zweck von WLAN-Zugangspunkten ist, Kunden und anderen Nutzern einen einfachen, direkten Internetzugang zur Verfügung zu stellen. Daher sind die meisten offenen WLAN-Netze im Infrastrukturmodus aufgebaut. (BSI o.J.; Eisele et al. 2017) Die folgende Abbildung verdeutlicht schematisch den Aufbau eines WLAN-Hotspots im Infrastrukturmodus.

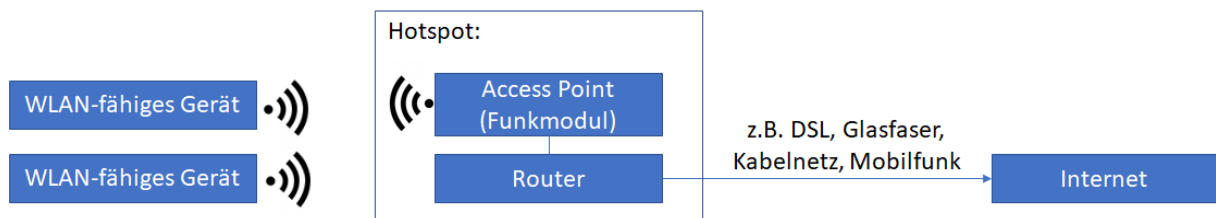


Abbildung 2: Schematischer Aufbau eines WLAN-Hotspots (Quelle: Eigene Darstellung nach HMWEVL 2017)

3.1 Offene WLAN-Netze

Offene WLAN-Netze sind eine spezielle Ausprägungsform von WLAN-Netzen. Sie werden definiert als Netze, deren Nutzung grundsätzlich keinen Benutzer ausschließt. Zum Teil sind diese WLAN-Netze komplett frei zugänglich, allerdings oft erst nach dem Akzeptieren der Nutzungsbedingungen. Bei anderen offenen WLAN-Netzen ist der Zugang mit bestimmten weiteren Bedingungen verknüpft, wie z. B. einem Restaurantbesuch oder der Entrichtung einer Gebühr. Demgegenüber stehen die geschlossenen WLAN-Netze, die z. B. durch

² Mbit/s ist eine Einheit für die Datenübertragungsrate. Beispiel: Bei einer Geschwindigkeit von 8 MBit/s können 1 MByte an Daten pro Sekunde befördert werden.

³ Die „Arbeitsweisen“ im Ad-Hoc- und Infrastrukturmodus sind vergleichbar mit den Betriebsmodi DMO und TMO im BOS-Digitalfunk

Passwortschutz nur einem bestimmten Nutzerkreis zugänglich und damit für die Öffentlichkeit nicht nutzbar sind. (HMWEVL 2017)

Die vorliegende Arbeit bezieht sich ausschließlich auf offene WLAN-Netze gemäß der o. g. Definition.

3.2 Ausbauzustand offener WLAN-Netze in Deutschland

Die Verbreitung offener WLAN-Netze ist in Deutschland im Vergleich zu anderen Ländern relativ gering. (MWIDE NRW 2018) Eine Studie des Verbandes der deutschen Internetwirtschaft ermittelte im Jahr 2014 lediglich einen Anteil von 1,87 Hotspots pro 10.000 Einwohner. Zum Vergleich gab es in Großbritannien zum selben Zeitpunkt eine Abdeckung von 28,67 Hotspots pro 10.000 Einwohner.⁴ (Landefeld 2014) In manchen Medien wird sogar vom „Internet-Mittelalter“ (Hesse 2018; Dörner 2016) oder von der „WLAN-Wüste Deutschland“ (Hesse 2018) gesprochen. Es gibt zudem Prognosen, die einen eher schleppenden Ausbau der WLAN-Infrastruktur vorhersagen. (Hegemann 2018)

Allerdings ist auch ein gegenläufiger Trend zu erkennen: Seit der Abschaffung der sogenannten Störerhaftung im Jahr 2017 ist ein wesentliches Hemmnis, WLAN-Netze „zu öffnen“, nicht mehr existent. WLAN-Betreiber haften jetzt bei Rechtsverletzungen durch Dritte nicht mehr auf Schadensersatz, Unterlassung oder Abmahnkosten. (HMWEVL 2017) Experten sehen die Störerhaftung als wesentlichen Grund dafür an, dass der Ausbau offener WLAN-Netze in Deutschland lange Zeit nur schleppend vorankam und auch heute noch der Großteil der Netze nicht offen sind. (Truthän 12.11.2018; Wiedemann 18.10.2018)

Inzwischen bieten immer mehr Kommunen öffentliche WLAN-Netze für Einwohner und Touristen an und planen auch, diese deutlich auszubauen. (z.B. NetCologne 2017) Vorteile sehen die Kommunen u.a. in der Förderung von Wirtschaft und Tourismus sowie bei der Quartiersentwicklung. (HMWEVL 2017; Eisele et al. 2017) Das Bundesamt für Wirtschaft und Energie bezeichnet freies Internet als einen „unverzichtbaren Baustein der digitalen Gesellschaft“. (BMWi o.J.) Durch gezielte Förderung, z.B. mit dem Förderprogramm „WiFi4EU“, soll der flächendeckende WLAN-Netzausbau weiter vorangetrieben und beschleunigt werden. (MWIDE NRW 2018)

Die Einrichtung offener WLAN-Netze hat übereinstimmend zum Ziel, möglichst vielen Leuten an möglichst vielen Stellen einen Internetzugang zur Verfügung zu stellen.

4 Anwendungsmöglichkeiten von WLAN im Feuerwehreinsatz

Leitfrage: Welche Anwendungsmöglichkeiten bietet die Nutzung offener WLAN-Netze im Feuerwehreinsatz?

Wie im vorangegangenen Kapitel erläutert, wächst die Anzahl offener WLAN-Netze in Deutschland. Da sowohl der öffentliche Raum als auch Betriebe potenzielle Einsatzgebiete der Feuerwehr darstellen, wächst auch die Wahrscheinlichkeit, dass an einer Einsatzstelle ein solches Datenübertragungsnetz verfügbar ist. In diesem Kapitel sollen Möglichkeiten

⁴ Siehe auch Diagramm im Anhang B

aufgezeigt werden, die durch das Vorhandensein offener WLAN-Netze am Einsatzort für die Feuerwehr entstehen könnten. Dazu ist es erforderlich, im ersten Schritt auf den grundsätzlichen Bedarf solcher neuen Datenübertragungswege einzugehen. Dies erfolgt im Rahmen einer Auseinandersetzung mit den in der Aufgabenstellung genannten Bereichen „Einsatzkoordination und -dokumentation“ sowie „Überwachung der Einsatzkräfte“. Dabei soll für beide Bereiche herausgearbeitet werden, wie eine Nutzung offener WLAN-Netze jeweils denkbar wäre.

Eine Bewertung der Praxistauglichkeit offener WLAN-Netze in Bezug auf die an dieser Stelle aufgeführten Anwendungen erfolgt in Kapitel 8.

4.1 Anwendungsbereich Einsatzkoordination und -dokumentation

Die Durchführung von Feuerwehreinsätzen bringt einen hohen Koordinationsbedarf mit sich. Gleichzeitig spielt die Dokumentation einsatzrelevanter Daten sowohl während des Einsatzes als auch in dessen Nachbearbeitung eine große Rolle. Aus diesen Gründen stellen Mittel zur Informationsgewinnung, -verarbeitung und -übertragung eine tragende Rolle zur Sicherung des Einsatzerfolgs dar. In der Feuerwehr-Dienstvorschrift 100 werden Kommunikationsmittel sogar als wichtigste Führungsmittel bezeichnet. (FwDV 100)

Die Anforderungen an diese Kommunikationsmittel ändern sich mit der Digitalisierung deutlich. Es stehen immer mehr Daten zur Verfügung, die von der Feuerwehr am Einsatzort oder rückwärtig verarbeitet werden müssen. Ein einfaches Beispiel ist die Übertragung von (Echtzeit-) Bildern oder Videos vom Einsatzort, die zur Einschätzung der Lage sowie zur weiteren Planung und Dokumentation eines Einsatzes sehr hilfreich sein können. Weitere Beispiele sind das gesteigerte Informationsbedürfnis der Bevölkerung und die wachsende Bedeutung von Social Media, die eine ständige Beobachtung entsprechender Kanäle sowie das schnelle Platzieren eigener Inhalte erfordern. Zur Verarbeitung solcher wachsenden Datenmengen sind möglichst breitbandige Datenübertragungswege erforderlich.

Nach wie vor ist im Feuerwehreinsatz neben der mündlichen Kommunikation die Sprach-Kommunikation über den „eigenen“ BOS-Funk der Standard. Diese Übertragungswege eignen sich jedoch nicht, um große Datenmengen, wie die oben genannten, entsprechend zu verarbeiten.⁵

Eine Folge davon ist, dass häufig parallele Kommunikationswege eröffnet werden, indem z. B. über das Mobilfunknetz oder über Internet und Messenger-Apps Bilder und Videos ausgetauscht werden. Diese Art der Nutzung stellt ein einfaches Beispiel dafür dar, wie heute schon bestehende – aber nicht feuerwehreigene Netze – von der Feuerwehr im Sinne der Einsatzkoordination und -dokumentation genutzt werden.

Eine wachsende Bedeutung erfahren bei Feuerwehren auch software- und app-basierte Systeme zur mobilen Führungsunterstützung. Der größte Mehrwert solcher Lösungen besteht in der online-Vernetzung zwischen dem Einsatzort und der Leitstelle oder anderen Informationsquellen wie z. B. dem Zugriff auf aktuelle Datenbanken oder andere Echtzeit-Daten im Internet. Beispiele solcher in der Praxis schon eingesetzter Führungsunterstützungssysteme sind z. B. die Berliner „FireApp“, das Mobile Feuerwehr Informationssystem der Berufsfeuerwehr Duisburg (MoFIS) oder das

⁵ Zu Datenübertragungsraten im BOS-Funk siehe auch Kapitel 5

Führungsunterstützungssystem „FireScout“. Führungskräfte können damit z. B. mobil und live Daten zum Einsatzort und zum Status der alarmierten Einheiten abrufen. (Bäker 15.11.18; Baumann 2010; Schmehl 05.12.2018)

Die genannten Anwendungen basieren alle auf dem drahtlosen Austausch von einsatzrelevanten Daten. Wesentliche Grundlage für die Funktion ist meist ein schneller Internetzugang. Offene WLAN-Netze, die ggf. am Einsatzort verfügbar sind, stellen einen solchen Zugangspunkt zum Internet her und sind damit grundsätzlich zur Datenübertragung geeignet.

4.2 Anwendungsbereich Überwachung von Einsatzkräften

Die Überwachung von Einsatzkräften erfolgt heute noch hauptsächlich analog im Rahmen der nach Feuerwehr-Dienstvorschrift 7 vorgeschriebenen Atemschutzüberwachung, bei der Daten zum Aufenthaltsort sowie zum Restdruck der eingesetzten Pressluftatmer nur in relativ großen Zeitabständen (bis zu 10 min bzw. 1/3 der Einsatzzeit) mündlich übertragen und dann schriftlich erfasst werden. (FwDV 7) Vitaldaten, wie z. B. Herz- oder Atemfrequenz, werden meist überhaupt nicht erfasst. Ob und wie exakt der Aufenthaltsort vorgehender Einsatzkräfte erfasst wird, hängt maßgeblich von der Frequenz und Genauigkeit der mündlichen Rückmeldungen sowie deren Dokumentation ab. Vereinzelt werden heute schon elektronische Systeme zur Atemschutzüberwachung eingesetzt. Bei den bekannten Systemen werden allerdings keine Ortungsdaten, sondern lediglich technische Daten der Pressluftatmer (Restdruck und die daraus errechnete verbleibende Einsatzzeit) übertragen. (Dräger o. J.a; MSASafety o. J.; Dräger o. J.b)

Fast 40 % der Verletzungen im Einsatz passieren beim Innenangriff, bei dem Feuerwehrkräfte unter Atemschutz in ein Gebäude eindringen müssen. (DGAUM 2018) Wesentlicher Sicherheitsfaktor für die Einsatzkräfte im Innenangriff ist eine funktionierende Kommunikation nach „draußen“. Immer wieder kommt es – z.B. durch Abbrüche der Funkverbindung oder durch Missverständnisse – zu schweren Unfällen. Tragische und prominente Beispiele stellen zum einen der tödliche Atemschutzunfall von Brandmeister Stampe in Köln im Jahr 1996 oder der Tod zweier Feuerwehrleute in Tübingen im Jahr 2005 dar. In beiden sowie vielen anderen Fällen waren die Aufenthaltsorte der verunglückten Kollegen nicht zu jeder Zeit bekannt, sodass die Rettung jeweils verzögert wurde. (BD Maurer et al. 1996; Unfallkommission "Tübingen" 2006)

Eine Live-Übertragung der genannten, sicherheitsrelevanten Daten der vorgehenden Trupps könnte ggf. eine deutliche Verbesserung der Sicherheit für die Einsatzkräfte darstellen. Insbesondere die Ortung von Einsatzkräften stellt eine Anwendung dar, die auch im Hinblick auf Ereignisse der Vergangenheit dazu geeignet erscheint, tödliche Atemschutzunfälle zu vermeiden.

Neben der Überwachung von Einsatzkräften sind aber auch eine Vielzahl weiterer Anwendungen denkbar, so zum Beispiel die Übertragung von Bildern einer Helmkamera oder von anderen Mess- und Sensordaten. Die Anwendungen beruhen alle auf demselben Schema: Der digitalen Erfassung der Daten des vorgehenden Trupps, deren Übertragung zu einem oder mehreren „Überwachungsposten“ und die dortige Überwachung bzw. Verarbeitung.

Die genannten Beispiele verdeutlichen zum einen die besondere Bedeutung einer stabilen Sprach-Kommunikation im Atemschutzeinsatz. Zum anderen zeigt sich, dass die automatisierte Übertragung zusätzlicher Daten verglichen mit dem Status Quo einen möglichen Sicherheitsgewinn darstellen kann. Daraus ergibt sich der Bedarf, neben dem BOS-Funk auch alternative Datenübertragungsmöglichkeiten zu prüfen.

Betriebe und Gebäude sind heute häufig mit flächendeckenden, offenen WLAN-Netzen ausgerüstet, verfügen also über eine vorhandene Infrastruktur zur Datenübertragung. Ein konkreter, denkbarer Anwendungsfall für offene WLAN-Netze wäre in diesem Fall die Möglichkeit, Daten (Vital- Ortungs- und technische Daten) von vorgehenden Trupps in Bereichen mit WLAN über diese Netze zu übertragen und an eine überwachende Stelle (z.B. Atemschutzüberwachung) zu senden.

4.3 Zusammenfassung der Anwendungsbereiche

Zusammenfassend zeigt sich, dass sowohl bei der Einsatzkoordination und -dokumentation, als auch bei der Überwachung von Einsatzkräften drahtlose sowie möglichst breitbandige Datenübertragungswege einen Mehrwert darstellen können.⁶ In der Einsatzkoordination und -dokumentation wird dieser durch einen an der Einsatzstelle vorhandenen Internetzugriff ermöglicht. Für die Überwachung von Einsatzkräften könnten Kommunikationsnetze, die auch an ausgedehnten Einsatzstellen eine möglichst flächendeckende Übertragung von Daten vorgehender Trupps ermöglichen, einen Vorteil ergeben. In beiden Fällen ist grundsätzlich auch die Nutzung von offenen WLAN-Netzen theoretisch denkbar. Die Anwendungsbereiche werden für die vorliegende Arbeit wie folgt definiert.

Tabelle 1: Anwendungsbereiche, für die die Nutzung offener WLAN-Netze geprüft werden soll

Anwendungsbereich	Beschreibung
Einsatzkoordination und -dokumentation	Offenes WLAN soll vorrangig dafür genutzt werden, einen schnellen Internetzugriff bereitzustellen, um am Einsatzort digitale Führungsmittel, wie z.B. Führungsunterstützungssysteme, einzusetzen.
Überwachung der Einsatzkräfte	Offenes WLAN soll vorrangig dafür genutzt werden, sicherheitsrelevante Daten vorgehender Einsatzkräfte (Vitaldaten, technische Daten, Ortungsdaten) am Einsatzort (z.B. in ausgedehnten Gebäuden) zu einer überwachenden Einheit zu übertragen.

5 Stand der Technik

Zur mobilen Übertragung von Daten werden heute bei der Feuerwehr unterschiedliche Kommunikationswege genutzt. Standard-Kommunikationsmittel ist der digitale TETRA-BOS-Funk. Großer Nachteil des BOS-Funks sind die niedrigen Datenübertragungsraten. Die Bundesnetzagentur gibt diese mit 9,6 - 28,8 kBit/s an. (Bundesnetzagentur o. J.) Für bestimmte Anwendungen, bei denen breitbandigere Übertragungswege erforderlich sind,

⁶ Der Begriff „breitbandig“ steht in dieser Arbeit für Übertragungswege mit hohen Datenübertragungsraten, z.B. zur Übermittlung von Bildern und Videos

wird daher schon heute auf andere Übertragungswege wie Mobilfunk oder auch WLAN zurückgegriffen. Im Folgenden werden für unterschiedliche Anwendungsbereiche sowohl der Stand der Technik, als auch ggf. in der Erprobungsphase befindliche Projekte beschrieben und vorgestellt.

5.1 Mobile Führungsunterstützungssysteme

Mobile Führungsunterstützungssysteme sind oft so konfiguriert, dass sie zur Datenübertragung unterschiedliche Kanäle nutzen können. Die im vorangegangenen Kapitel erwähnte Berliner „FireApp“ nutzt handelsübliche Tablets als Hardware. Somit stehen zur Datenübertragung auch die gängigen, von der privaten Nutzung bekannten Wege wie Mobilfunk, WLAN und Bluetooth zur Verfügung. Die Mobilfunkanbindung verfügt dabei über eine Verschlüsselung, die in die SIM-Karte integriert ist. Damit wird ein unbefugter Datenzugriff verhindert. (Bäker 15.11.18) Das Führungsunterstützungssystem FireSCOUT nutzt wahlweise Mobilfunk, WLAN oder eine Satellitenanbindung. (Baumann 2010) Beim Duisburger System MoFIS (Mobiles Feuerwehr Informationssystem) erfolgt die Datenübertragung auf der Wache über ein gesichertes WLAN-Netz. Unterwegs nutzt das System eine speziell abgesicherte Mobilfunkverbindung. (Schmehl 05.12.2018)

5.2 Digitale Atemschutzüberwachung

Bestehende Systeme zur digitalen Atemschutzüberwachung („Telemetrie“) der Firmen Auer und Dräger nutzen eigene Funknetze, die im Innern von Gebäuden durch das Setzen von Repeatern erweitert werden können. Offene WLAN-Netze werden zur Übertragung der Daten nach Angaben der Unternehmen nicht verwendet, auch zukünftig ist das nicht vorgesehen.⁷ (Linge 22.10.18; Lenz 22.10.18) Projekte, die sich mit der Verbesserung der Sicherheit vorgehender Atemschutztrupps beschäftigen, wie z. B. die unter Beteiligung des IdF NRW sowie des Fraunhofer-Instituts durchgeführten Projekte „Koordinator“ und „Landmarke“, setzen zur Übermittlung von Daten auf eigene „Ad-Hoc-Netze“, die am Einsatzort aufgebaut werden. (FIT o.J.; Helm et al. 2014)

5.3 Übermittlung von Vitaldaten

Zur Übertragung von Vitaldaten der Einsatzkräfte gibt es eine Reihe von Projekten, wie u. a. das im Rahmen des Sicherheitsforschungsprogramms der Bundesregierung durchgeführte Projekt „SensProCloth“, in dem durch Sensorik in der Einsatzkleidung wichtige Daten erfasst und zu einer überwachenden Stelle gesendet werden. Die Datenübertragung wird auch hier durch eigene Funknetze sichergestellt, wobei die Einsatzkräfte selbst als Repeater wirken. (Gödde und Wessels 2011) Ähnlich stellt sich die Datenübertragung im Projekt SAFE dar, das die Integration intelligenter Telemetrie in Feuerwehreinsatzkleidung zum Ziel hatte. (BBK 2011) Der Einsatz eines solchen Systems im Feuerwehreinsatz über die Testphase hinaus ist nicht bekannt.

5.4 Übertragung von Bild- und Videomaterial

Ein interessanter Anwendungsfall bei der Datenübertragung im Feuerwehreinsatz besteht auch in der Übertragung von Bild- oder Videodateien, z. B. vom vorgehenden Trupp zur

⁷ Im Anhang B befindet sich beispielhaft für die Firma Dräger eine Übersicht über die genutzten Datenübertragungskanäle

Führungskraft. Das Produkt „BOS-Cam“ der Fa. BOS-Connect, mit dem Bilder vom Einsatzort in Echtzeit übertragen werden können, nutzt für die Übertragung eine Mobilfunkverbindung oder alternativ ein vor Ort über das Fahrzeug aufgebautes Ad-Hoc-WLAN-Netz. (Nicklas 06.11.2018) Bei einem Projekt unter Beteiligung der Feuerwehr Darmstadt zum Thema „Bodycams für Feuerwehrleute“ wird ebenfalls auf eine Mobilfunkverbindung zurückgegriffen. (Heeg 2018)

5.5 Ortung von Einsatzkräften

Die Ortung von Einsatzkräften ist heute in der Feuerwehrpraxis noch nicht verbreitet. Allerdings gibt es verschiedene Feuerwehren, die sich im Rahmen von Projekten mit dieser Thematik befassen bzw. befasst haben. Die Werkfeuerwehr BASF in Ludwigshafen arbeitet an einem Projekt, bei dem alle Anlagen in Form von digitalen Gebäudeplänen erfasst werden sollen. Laufwege der Einsatzkräfte sollen, ausgehend von einem Referenzpunkt, über in einem Gerät verbaute Bewegungssensoren nachverfolgt werden. Eine Übermittlung der Daten über WLAN wurde aufgrund der unzureichenden WLAN-Abdeckung nicht verfolgt. (Urban 16.10.18)

Die Berliner Feuerwehr war an einem Projekt beteiligt, bei dem ebenfalls Ortungsdaten der Einsatzkräfte erfasst und versendet werden sollten. Das Projekt FeuerWhere basierte auf eigenen Datenübertragungsmodulen, die Nutzung offener WLAN-Netze wurde nicht geprüft. Im Ergebnis wurden noch zu viele Ungenauigkeiten bei der Ortung festgestellt, so dass aus dem Projekt keine Umsetzung in der Praxis hervorging. (Berliner Feuerwehr 2010; Harz 22.10.2018)

5.6 Sonderfall WLAN-Ortung

Das Thema Ortung stellt im Zusammenhang mit WLAN einen Sonderfall dar: WLAN-Netze sind nicht nur grundsätzlich als potenzielle Übertragungswege von (Ortungs-)Daten denkbar, sondern sie sind auch „direkt“ zur Ortung von Personen geeignet. So gibt es, z. B. in Flughäfen oder Shoppingcentern, sogenannte „Indoor-Tracking“-Lösungen, um Laufwege von Kunden oder Passagierströme nachzuverfolgen. Zur Ortung werden Technologien wie Bluetooth, GPS, RFID aber auch WLAN verwendet. Die Lokalisierung von Personen bzw. Personenströmen kann dabei zum einen über die Erkennung eingeloggter WLAN-fähiger Geräte, oder über das so genannte „Fingerprinting“ erfolgen, bei dem die Position anhand der verfügbaren WLAN-Signalstärke über eine App errechnet werden kann. Dafür sind allerdings im Vorfeld Referenzmessungen erforderlich. (infsoft o.J.; Fraunhofer IIS 2018; Favendo o.J.) Die Genauigkeit der Ortung über WLAN wird mit 5-15 m angegeben. (infsoft o.J.)

In Deutschland ist z.B. der Frankfurter Flughafen mit einem solchen System zur Indoor-Ortung ausgestattet. (Häusler 22.10.2018) Internetkonzerne wie z.B. Google nutzen die WLAN-Ortung, um die Standortgenauigkeit auch im Freien zu verbessern. Um die dafür notwendige Datenbasis zu generieren, werden öffentliche Bereiche nach verfügbaren Funknetzen „gescannt“. (FAZ 2010)

5.7 Trend zu eigenen Ad-Hoc- und Mobilfunknetzen

Grundsätzlich ist anhand der o.g. Anwendungsbeispiele erkennbar, dass der Trend bei der Wahl der Datenübertragungswege im Feuerwehreinsatz entweder hin zu eigenen,

kontrollierbaren Ad-Hoc-Netzen geht, oder aber Mobilfunknetze verwendet werden. Die gezielte Nutzung offener WLAN-Netze findet nicht statt. Dieser Trend ist auch in einer Reihe weiterer Projekte im Feuerwehrbereich erkennbar, die nicht unter die genannten Überschriften fallen. In einem Projekt aus dem Jahr 2010 wurden Behandlungsplätze mit vor Ort aufgebauten Ad-Hoc-WLAN-Netzen ausgestattet. (Temmler 2010) Der Mobilfunkanbieter Vodafone beteiligte sich an einem Projekt, bei dem Schlauchkupplungen mit WLAN-Sendern ausgestattet wurden und so ein Ad-Hoc-Netzwerk aufgebaut wurde. (Vodafone 2018) Eine andere Möglichkeit besteht darin, Einsatzfahrzeuge so auszustatten, dass sie vor Ort eigene Kommunikationsnetze aufbauen können (z. B. Markland 2016). In den USA soll ein eigenes, für Rettungskräfte „reserviertes“ LTE-Mobilfunknetz aufgebaut werden, das alle 50 US-Staaten abdeckt. So soll den Rettungskräften eine unabhängige und leistungsfähige Kommunikation ermöglicht werden. (Nichols 2017)

5.8 Zusammenfassung Stand der Technik

Zusammenfassend zeigt sich, dass sich die Nutzung von Systemen, die auf mobiler Datenübertragung beruhen, auch bei der Feuerwehr mehr und mehr durchsetzt. Anwendungen, die einen Internetzugriff erfordern, nutzen dafür häufig die bestehenden Mobilfunknetze. Systeme, die den lokalen Austausch von Daten am Einsatzort ermöglichen, nutzen meistens eigene Funknetze, die zum Teil auch auf dem WLAN-Standard basieren. Insgesamt werden eigene, kontrollierbare Netze (BOS-Funk, eigene Funknetze) soweit möglich bevorzugt. Offene WLAN-Netze finden heute keine konkrete Anwendung.

Einen Sonderfall im Zusammenhang mit WLAN-Netzen stellt die Möglichkeit dar, Personen über WLAN in Gebäuden direkt zu orten. Solche Lösungen sind jedoch heute nur vereinzelt in Bereichen anzutreffen, wo die Daten für Betreiber einen Mehrwert darstellen, z. B. in Flughäfen oder Shoppingcentern.

6 Anforderungen aus Sicht der Feuerwehr

Leitfrage: Welche Anforderungen muss ein offenes WLAN-Netz erfüllen, damit die Feuerwehr es nutzen kann?

Um beurteilen zu können, ob offene WLAN-Netze im Feuerwehreinsatz genutzt werden können, muss in einem ersten Schritt ein Beurteilungsmaßstab definiert werden. In diesem Kapitel werden deshalb übergeordnete Punkte benannt, die vor einer möglichen Nutzung offener WLAN-Netze geprüft werden müssen. Im Anschluss erfolgt anhand der genannten Anforderungen eine Bewertung, ob die Nutzung möglich und sinnvoll ist.

6.1 Allgemeine Anforderungen

Es ist offensichtlich, dass ein Ausfall von Gerätschaften und Equipment der Feuerwehr im Einsatz schwerwiegende Folgen haben kann. Aus diesem Grund sollen technische oder organisatorische Maßnahmen dafür sorgen, Ausfälle möglichst zu vermeiden. Dies gilt auch für die Kommunikationsmittel, die z. B. durch eine batteriegepufferte, unterbrechungsfreie Stromversorgung (USV) der BOS-Funk Basisstationen abgesichert werden. (BDBOS o.J.) Die wesentlichste Anforderung an Einsatzmittel der Feuerwehr ist deshalb – einfach formuliert – „sie müssen funktionieren“. Dies schließt sowohl technische, konzeptionelle als auch finanzielle Aspekte ein. Ebenso spielt die Bedienbarkeit eine wesentliche Rolle.

Bei der Nutzung fremder Netze – wie es offene WLAN-Netze sind – ist kein direkter Einfluss und damit auch keine Kontrolle dieser Anforderungen durch die Feuerwehr gegeben. Somit muss sorgfältig geprüft werden, ob auch diese Netze für die Feuerwehr im o. g. Sinne „funktionieren“. Dabei muss allerdings differenziert werden: Nicht jede Nutzung durch die Feuerwehr bedeutet automatisch, dass die höchsten Anforderungen erfüllt werden müssen. Während manche Anwendungen immer und unbedingt funktionieren müssen, sind andere möglicherweise nur als sinnvolle Ergänzung zu sehen. Die im Folgenden genannten Anforderungen sind daher, je nach Anwendung, unterschiedlich zu gewichten.

6.2 FwDV 800

Die wachsende Bedeutung sogenannter Informations- und Kommunikationsmittel (IuK) im Feuerwehreinsatz und die immer wieder aufkommende Frage, welche Anforderungen an diese gestellt werden müssen, beschäftigt auch nationale feuerwehernahe Gremien, wie den Ausschuss Feuerwehrangelegenheiten, Katastrophenschutz und zivile Verteidigung (AFKzV). Daher wurde im März 2018 die neue Feuerwehr-Dienstvorschrift 800 „Informations- und Kommunikationstechnik im Einsatz“ genehmigt und den Ländern zur Einführung empfohlen. (Block 2018) In einzelnen Bundesländern, z. B. Nordrhein-Westfalen (NRW), ist die FwDV schon durch einen Erlass des Innenministeriums NRW in Kraft gesetzt worden und damit bindend.⁸ Mitglieder der Arbeitsgruppe waren u. a. Feuerwehrleute mit Sachverstand im Bereich der Kommunikationstechnik. Damit soll gewährleistet werden, dass sowohl technische als auch taktische Belange ausreichend berücksichtigt werden. Die FwDV widmet sich auch dem Thema „WLAN“, welches als eines von vielen möglichen Kommunikationsmitteln für die Feuerwehr aufgeführt wird. (FwDV 800) Durch den Leiter der Arbeitsgruppe, Klaus Block (IM NRW), wurde zudem bestätigt, dass auch die Nutzung von offenen WLAN-Netzen bei der Erarbeitung sowie Formulierung der Anforderungen thematisiert wurde. (Block 08.11.2018)

Aufgrund ihrer Aktualität sowie der o.g. Punkte wird die FwDV 800 als grundsätzlich geeignet angesehen, um Anforderungen an fremde Netze – in diesem Falle offene WLAN-Netze – zu definieren.

Folgende Punkte werden in der FwDV 800 als wesentlich für die Auswahl von IuK-Mitteln genannt: *Verfügbarkeit, Bandbreite, Reichweite, Schnelligkeit, Grad der Geheimhaltung sowie Sicherheit und Wiederherstellung im Einsatzfall.*

Des Weiteren werden Einsatzgrundsätze beschrieben. Die folgenden sind für die Bewertung des Einsatzes von offenen WLAN-Netzen besonders relevant:

- IuK-Mittel sind u. a. gegen Sabotage und Ausfall der Energieversorgung zu sichern.
- Es ist IuK-Technik einzusetzen, welche die Vertraulichkeit, Verfügbarkeit und Integrität der Daten gewährleistet.
- Es sind Maßnahmen zu treffen, die den unbefugten Informationszugang verhindern (z. B. durch Verschlüsseln).

⁸ Runderlass des Ministeriums für Inneres und Kommunales NRW (- 73-52.06.04 -) vom 11.9.2012, letztmalig geändert durch Runderlass vom 17. August 2018

In der FwDV 800 ist auch konkret die Nutzung „fremder“ IuK-Netze beschrieben. Danach ist die Nutzung solcher Netze nur zulässig, wenn keine eigenen IuK-Netze zur Verfügung stehen.

Die allgemeinen sowie die in der FwDV 800 genannten Anforderungen werden für die vorliegende Arbeit in drei übergeordneten Punkten zusammengefasst. Anhand dieser Punkte wird im kommenden Kapitel die Möglichkeit der Nutzung offener WLAN-Netze durch die Feuerwehr beurteilt.

Tabelle 2: Grundsätzliche Anforderungen, die bei der Nutzung offener WLAN-Netze geprüft werden müssen

Anforderung	Konkretisierung
Verfügbarkeit	Vorhandensein, Ausfallsicherheit, Funktion, Bedienbarkeit, Kompatibilität, ...
Leistungsfähigkeit	Bandbreite, Schnelligkeit, Reichweite, ...
Datensicherheit	Grad der Geheimhaltung, Schutz vor unbefugtem Informationszugang, ...

7 Gegenüberstellung von Anforderungen und Leistungsmerkmalen

In diesem Kapitel werden die in den vorhergehenden Kapiteln beschriebenen Anforderungen mit den Leistungsmerkmalen offener WLAN-Netze verglichen. Hierbei wird im Wesentlichen auf Informationen aus den durchgeführten Experteninterviews zurückgegriffen. Die Leitfrage für dieses Kapitel lautet: *Können offene WLAN-Netze die Anforderungen erfüllen?*

7.1 Verfügbarkeit offener WLAN-Netze

Die Frage nach der Verfügbarkeit von offenen WLAN-Netzen muss aus mehreren unterschiedlichen Perspektiven erfolgen. Im Wesentlichen stellen sich zwei Fragen: Zum einen ist entscheidend, wie verbreitet überhaupt offene WLAN-Netze sind, also wie groß letztendlich die Chance ist, dass am Einsatzort ein solches Netz zur Verfügung steht. Zum anderen muss beantwortet werden, ob die Netze, auch wenn sie vorhanden sein sollten, im Einsatzfall auch funktionieren und damit für die Feuerwehr nutzbar sind.

7.1.1 WLAN-Abdeckung

Die Abdeckung von offenen WLAN-Netzen im öffentlichen Raum in Deutschland wurde in Kapitel 3.2 beschrieben. Es zeigt sich, dass öffentliche WLAN-Netze zwar mehr und mehr ausgebaut werden, allerdings längst nicht flächendeckend verfügbar sind. Oft beschränkt sich der Ausbau auf Großstädte und Ballungsräume. Zudem existiert eine Vielzahl unterschiedlicher Netzanbieter. Eine abschließende Übersicht über alle verfügbaren offenen WLAN-Netze existiert nicht.

Über die Abdeckung offener WLAN-Netze in Betrieben kann keine verlässliche Aussage getroffen werden. Es ist davon auszugehen, dass insbesondere größere Betriebe mit Büro- und Verwaltungsnutzung ihren Kunden und Mitarbeitern häufig offene WLAN-Netze zur Verfügung stellen. Zu beachten ist dabei, dass in größeren Bürogebäuden oder auch

Einkaufszentren durch die Vielzahl unterschiedlicher Nutzer auch eine Vielzahl unterschiedlicher WLAN-Netze existieren können. Es kann nicht davon ausgegangen werden, dass solche Gebäude flächendeckend mit einem einzigen, zusammenhängenden WLAN-Netz ausgestattet sind.

Hieraus lässt sich zusammenfassend feststellen, dass die Abdeckung mit offenen WLAN-Netzen insgesamt lückenhaft ist und weder im öffentlichen Raum noch in Betrieben garantiert werden kann. Letztendlich ist es Stand heute mehr oder weniger dem Zufall überlassen, ob am Einsatzort ein offenes WLAN zur Verfügung steht oder nicht. Eine wesentliche Anforderung im Sinne der Verfügbarkeit aus Sicht der Feuerwehr ist damit nur bedingt erfüllt.

7.1.2 Nutzbarkeit offener WLAN-Netze für die Feuerwehr

Der zweite Betrachtungspunkt betrifft die Nutzbarkeit eines vorhandenen Netzes im Einsatz für die Feuerwehr. Hierbei spielen die Punkte Ausfallsicherheit sowie der Anmeldevorgang eine wesentliche Rolle.

Die WLAN-Technik ist nach Angaben von WLAN-Netzbetreibern rein für den „Consumer-Bereich“ entwickelt worden, dient also primär dazu, private Haushalte mit schnellem, „kabellosen“ Internetzugriff auszustatten. Für die Feuerwehr relevante Themen wie Hochverfügbarkeit, Stabilität und Ausfallsicherheit spielten bei der WLAN-Entwicklung eine untergeordnete Rolle. Auch sind die WLAN-Frequenzen offen und frei verfügbar und daher störanfällig. So kann ein WLAN-Netz z.B. durch andere elektromagnetische Wellen wie Bluetooth oder Mikrowellenstrahlung gestört werden. Im Vergleich zum Mobilfunkstandard LTE bezeichnen Experten WLAN als deutlich weniger robust. (BSI o.J.; Wiedemann 18.10.2018; Andric 18.10.2018)

Ein zusätzliches Problem stellen die Einflüsse des Ereignisses wie z. B. Feuer und Rauch, dar. Bestehende WLAN-Netze verfügen über keine unabhängige Stromversorgung, so dass bei Stromausfall durch das Ereignis oder durch das Stromlosschalten durch die Feuerwehr auch das WLAN-Netz abgeschaltet wird. Da keine direkte Kontrolle über das Netz besteht, kann auch eine Sabotage oder eine Abschaltung aus anderen Gründen nicht kontrolliert oder verhindert werden. Dem Einsatzgrundsatz aus der FwDV 800, dass IuK-Mittel gegen Sabotage und Ausfall der Energieversorgung zu sichern sind, kann somit nicht ausreichend Rechnung getragen werden, da eine ausreichend lange Nutzung im Brandfall nicht garantiert ist. (Wiedemann 24.10.2018; Harz 22.10.2018; Andric 18.10.2018) Zum Teil wird diese Einschätzung auch durch Studien belegt: Hofmann et al. (2006) untersuchten den Einfluss von Rauch auf die Leistungsfähigkeit von Standard WLAN-Netzen. Hier konnte festgestellt werden, dass Rauch einen zwar nur geringen, aber dennoch messbar negativen Einfluss auf die Übertragungsreichweite hat.

Ein weiteres großes Problem in Bezug auf die Nutzbarkeit durch die Feuerwehr stellt der Anmeldevorgang dar, der notwendig ist, um sich mit einem offenen WLAN-Netz zu verbinden. Meist erfolgt bei der Anmeldung an einem offenen WLAN-Netz eine Weiterleitung auf so genannte „Landing Pages“. Bevor das WLAN genutzt werden kann, müssen hier z. B. Nutzungsbedingungen akzeptiert oder sogar Angaben zur Person gemacht werden. Diese Tatsache verhindert, dass Geräte, die z.B. nicht über ein Display verfügen, sich automatisch in ein offenes WLAN-Netz einbuchen können. Zudem ist die Nutzungsdauer oft auf einen bestimmten Zeitraum begrenzt. Die Einschränkungen durch Anmeldeseiten und begrenzte Nutzungsdauer werden von den befragten Experten übereinstimmend als sehr problematisch

angesehen. (Ruthmann 08.11.2018; Wiedemann 18.10.2018; Maue 16.10.2018; Andric 18.10.2018) Um die Problematik zu umgehen, müssten bestimmte Geräte vorher einzeln im jeweiligen WLAN registriert werden. Die Nutzung wäre dann allerdings auch nur auf die registrierten Geräte im jeweiligen Netz beschränkt. Ein praktisches Beispiel für die genannte Problematik stellt ein Projekt der Feuerwehr Wesel dar, bei dem offene WLAN-Netze genutzt werden sollten, um im Einsatz auf eine „Behördencloud“ zugreifen zu können. Das Projekt wurde u.a. aufgrund der geringen Verfügbarkeit, häufiger Ausfälle und der komplizierten Einbuchungsmechanismen verworfen. (Bruckmann 22.10.18)

Ein übergeordnetes Problem hinsichtlich der Nutzbarkeit offener WLAN-Netze stellt die schon beschriebene Tatsache dar, dass es eine Vielzahl unterschiedlicher WLAN-Betreiber und -Netze gibt, oftmals auch auf engem Raum. Dies macht eine zentrale Kontrolle über Art und Verfügbarkeit der Netze in der Praxis unmöglich. Außerdem kommt es zu einer Potenzierung der genannten Probleme, wenn z. B. im Verlauf eines Einsatzes zwischen unterschiedlichen Netzen gewechselt werden muss.

7.2 Leistungsfähigkeit offener WLAN-Netze

Wenn offene WLAN-Netze von der Feuerwehr genutzt werden sollen, um große Datenmengen schnell übertragen zu können, müssen die Netze dementsprechend leistungsfähig sein. Grundsätzlich war die WLAN-Technologie lange Zeit dadurch gekennzeichnet, dass sie im Vergleich zu anderen Übertragungsstandards eine breitbandige Übertragung ermöglichte. Der Mobilfunk hat hier in den letzten Jahren allerdings stark aufgeholt. (Karcher 2014) Trotzdem ist WLAN – wie im privaten Bereich täglich festzustellen ist – grundsätzlich geeignet, Bilder und Videos, also große Datenmengen, zu übertragen.

Diese Leistungsfähigkeit ist bei offenen WLAN-Netzen allerdings nur mit Einschränkungen gegeben. Dies hat mehrere Gründe. Zum einen hängt es sehr stark vom einzelnen Netzbetreiber ab, ob und wie oft die Netze gewartet und aktualisiert werden. Dadurch kann es vorkommen, dass Hotspots nicht mehr den neuesten Standards entsprechen und die erwartete Leistungsfähigkeit nicht zur Verfügung steht. (Wiedemann 18.10.2018; Andric 18.10.2018) In jedem Fall wird die Leistungsfähigkeit des WLAN-Netzes immer von der schwächsten Stelle limitiert, also z. B. von der Qualität der Anbindung ans Internet.

Hotspots werden im öffentlichen Bereich meist durch viele Personen gleichzeitig genutzt. Sie können deshalb so konfiguriert sein, dass dem einzelnen Nutzer nur ein Teil der gesamten Bandbreite zur Verfügung steht. Bei mehreren eingeloggten Benutzern „konkurrieren“ alle Nutzer um die Bandbreite, wodurch für den Einzelnen nur noch ein Bruchteil der theoretisch verfügbaren Leistung zur Verfügung steht. (HMWEVL 2017)

Die in Kapitel 3 genannten theoretischen Datenübertragungsraten werden somit von offenen WLAN-Netzen in der Praxis kaum erreicht. Im Free WiFi Aachen werden z.B. Datenübertragungsraten von 10 Mbit/s bis 50 Mbit/s erreicht. Für den öffentlichen Raum entspricht dies nach Angaben des Netzbetreibers schon einem vergleichsweise breitbandigen Angebot. (Ruthmann 08.11.2018)

Eine zusätzliche Problematik ergibt sich aus der geringen Reichweite der WLAN-Netze. Dadurch kann das WLAN-Netz immer nur an einem lokal sehr begrenzten Ort genutzt werden. Große Flächen oder Gebäude bieten oft keine unterbrechungsfreie Abdeckung, auch wenn mehrere Zugangspunkte zum Einsatz kommen. Wenn Daten über einen längeren

Weg – z. B. zur Leitstelle – ausgetauscht werden sollen, muss das lokale WLAN immer mit einer weiteren drahtlosen oder kabelgebundenen Technologie ergänzt werden.

Zusammenfassend lässt sich sagen, dass die Bandbreite zwar grundsätzlich eine Stärke der WLAN-Technologie ist, bei offenen WLAN-Netzen allerdings eine Vielzahl negativer Einflussfaktoren dazu führen kann, dass nur ein Bruchteil dieser Leistung in der Praxis für die Feuerwehr zur Verfügung steht.

7.3 Datensicherheit offener WLAN-Netze

Eine weitere Anforderung an offene WLAN-Netze betrifft die Sicherheit der übertragenen Daten. An dieser Stelle soll hierzu eine allgemeine Einschätzung getroffen werden. Eine Bewertung, welche Daten als kritisch oder unkritisch in Bezug auf die Datensicherheit anzusehen sind, erfolgt nicht.

In Deutschland existiert eine eigene Behörde, die sich mit Fragen der IT-Sicherheit auseinandersetzt. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) sieht in der Nutzung offener WLAN-Netze ein erhöhtes Sicherheitsrisiko, sofern keine weiteren Maßnahmen getroffen werden. Immer dann, wenn Daten unverschlüsselt übertragen werden, besteht die Möglichkeit für Dritte, Daten abzuhören oder Schadsoftware einzuschleusen. (BSI o.J.) Es ist jedoch technisch möglich, eine Verschlüsselung im Router einzurichten, dafür müssen die Nutzer allerdings vorher bekannt sein. Da öffentliche Hotspots möglichst unbeschränkten Zugriff ohne vorherige Anmeldung bieten sollen, eignet sich hier praktisch nur die unverschlüsselte Konfiguration, was zum genannten Risiko führt. Die Lösung dieses Sicherheitsproblems kann darin bestehen, eigene, vom Netzanbieter unabhängige Ende-zu-Ende-Verschlüsselungen zu benutzen. Hierfür muss auf dem WLAN-fähigen Gerät des Benutzers z. B. eine VPN-Software installiert werden. Diese verschlüsselt die Daten und verhindert dadurch einen Zugriff durch Dritte. (Sauter 2018; MWIDE NRW 2018) Das BSI empfiehlt allen Nutzern öffentlicher Hotspots die Absicherung über VPN. (BSI o.J.)

Es zeigt sich, dass offene WLAN-Netze grundsätzlich als relativ unsicher zu betrachten sind. Allerdings kann durch geeignete Maßnahmen die Datensicherheit deutlich erhöht werden. Letztlich wird damit der Nutzer des offenen Hotspots in die Verantwortung genommen, sich und seine Daten durch zusätzliche Maßnahmen selbst zu schützen. Wenn diese Voraussetzungen erfüllt werden, können Daten auch über offene WLAN-Netze sicher übertragen werden.

8 Bewertung der Nutzbarkeit offener WLAN-Netze

Leitfrage: Für welche Anwendungen ist die Nutzung offener WLAN-Netze im Feuerwehreinsatz geeignet?

Die Gegenüberstellung von Anforderungen und Leistungsmerkmalen in Kapitel 7 hat gezeigt, dass die Nutzung offener WLAN-Netze im Feuerwehreinsatz einige Hürden mit sich bringt. Die wesentlichsten Punkte werden hier nochmals übersichtlich aufgelistet:

[1] Es ist keine flächendeckende Verfügbarkeit offener WLAN-Netze gegeben.

[2] WLAN-Netze sind anfällig gegen Störungen und können im Einsatzfall leicht ausfallen.

- [3] Die Leistung (Bandbreite) offener WLAN-Netze liegt oft deutlich unter der theoretisch möglichen Leistung. Die Gründe dafür sind vielfältig (z. B. Aufteilung auf viele Benutzer, veraltete Hardware, Engpass bei der Anbindung ans Internet).
- [4] Durch eine Vielzahl von Hotspot-Anbietern sind die Leistungsmerkmale vorhandener offener WLAN-Netze sehr uneinheitlich. Somit variieren die Rahmenbedingungen für die Nutzung je nach Netz stark.
- [5] Die Anmeldeseiten („Landing Pages“) führen dazu, dass WLAN-fähige Geräte sich nicht automatisch anmelden können.
- [6] Die Nutzungsdauer offener WLAN-Netze ist oft automatisch begrenzt.
- [7] Die Datensicherheit kann nur durch eine zusätzliche Verschlüsselungstechnologie im Endgerät sichergestellt werden.

8.1 Nutzung zur Einsatzkoordination und -dokumentation

In Kapitel 4.1 wurde definiert, dass der größte Vorteil offener WLAN-Netze zur Einsatzkoordination und -dokumentation im Wesentlichen darin besteht, einen schnellen Internetzugang zur Verfügung zu stellen.

Insbesondere aufgrund der im vorangegangenen Kapitel genannten Punkte [1]-[4] ist die Nutzung eines offenen WLAN-Netzes zum Zweck eines schnellen Internetzugriffs als nur bedingt geeignet zu betrachten. Die unkontrollierbaren Rahmenbedingungen führen dazu, dass sich erst im Einsatz vor Ort zeigt, ob ein WLAN-Netz verfügbar – also vorhanden *und* nutzbar – ist. Ebenso ist vorher nicht klar, ob die Leistungsfähigkeit zum Zeitpunkt der Nutzung für die jeweilige Anwendung ausreichend ist.

Die Punkte [5]-[7] sind für diese Anwendung zwar als hinderlich, allerdings je nach Einsatzsituation als weniger kritisch zu bewerten. Wenn z. B. Tablets oder PCs verwendet werden, können die Nutzungsbedingungen akzeptiert werden und die Anmeldeseiten stellen ggf. kein größeres Problem dar. Nach dem Ablauf der Nutzungsdauer kann sich erneut eingebucht werden. Zur Datensicherheit können einfache Technologien, wie VPN-Clients, verwendet werden, die im Bereich der Datenübertragung bei der Feuerwehr ohnehin gängig sind.

Immer dann, wenn ein offenes WLAN-Netz also verfügbar und nutzbar ist und die Sicherheitsvorkehrungen getroffen wurden, spricht auch nichts gegen dessen Nutzung. Diese kann vor allem dann hilfreich sein, wenn z. B. alternative Datenübertragungsmöglichkeiten wie LTE oder Satellit geringere Bandbreiten aufweisen oder in einem ausgedehnten Gebäude kein Mobilfunkempfang besteht. Bei einsatzkritischen Anwendungen müssen allerdings immer Alternativen vorhanden sein, so dass die Nutzung offener WLAN-Netze immer nur als zusätzliche Möglichkeit zur Verfügung stehen darf. Insgesamt wird die Nutzung offener WLAN-Netze zur Einsatzkoordination und Dokumentation i. S. der Definition in dieser Arbeit als ***in Einzelfällen bedingt geeignet*** bewertet.

8.2 Nutzung zur Überwachung der Einsatzkräfte

Die mögliche Nutzung offener WLAN-Netze zur Überwachung von Einsatzkräften, wurde in Kapitel 4.2 so definiert, dass darüber Daten (z. B. Vitaldaten, technische Daten) von einem mobilen, vorgehenden Trupp zu einer überwachenden Einheit gesendet werden.

Auch hier ergibt sich aus den Punkten [1]-[4], dass ein offenes WLAN-Netz – wenn überhaupt – nur als Zusatzoption gesehen werden kann. Die Begründung deckt sich hier mit der aus Kapitel 8.1, allerdings sind Probleme bei der Überwachung von Einsatzkräften noch schwerwiegender zu bewerten, als bei der Koordination und Dokumentation, da daraus eine unmittelbare Gefahr für die Einsatzkräfte resultieren kann. Weiterhin kommt erschwerend hinzu, dass die vorgehenden Trupps an der Einsatzstelle mobil sind und sich dadurch möglicherweise von Netz zu Netz bewegen müssen. Eine stabile Verbindung scheint deshalb nahezu ausgeschlossen.

Im Gegensatz zur Nutzung gemäß Kapitel 8.1 stellen bei der Nutzung zur Überwachung von Einsatzkräften insbesondere die Punkte [5] und [6] eine große Hürde dar. Wenn Geräte sich nicht automatisch ins WLAN einloggen können und/oder die Nutzungsdauer begrenzt ist, kann keine Überwachung sichergestellt werden.

Die Datensicherheit (Punkt [7]) stellt bei dieser Anwendung zwar ebenso ein lösbares Problem dar, wenn verwendete Geräte eigene Verschlüsselungstechnologien verwenden. Vor dem Hintergrund der genannten Ausschlusskriterien, fällt dieser Punkt hier jedoch nicht ins Gewicht.

Insgesamt wird die Nutzung offener WLAN-Netze zur Überwachung von Einsatzkräften i. S. der Definition in dieser Arbeit als **nicht geeignet** bewertet.

8.3 Diskussion

Die Bewertung in den beiden vorangegangenen Kapiteln hat gezeigt, dass die Problematik bei der Nutzung offener WLAN-Netze insbesondere darin begründet ist, dass keine „kontrollierbaren Bedingungen“ vorliegen, also keinerlei Einfluss auf Verfügbarkeit und Leistungsfähigkeit der Netze besteht. Für den Großteil der Anwendungsfälle stellt dies eine wesentliche Einschränkung bzw. den Grund für einen Ausschluss der Nutzung dar.

Im Umkehrschluss kann allerdings daraus auch folgende Aussage abgeleitet werden: Wenn in Einzelfällen die Hürden umgangen werden können, kann auch eine Nutzung der offenen WLAN-Netze möglich sein. Dies könnte insbesondere dort der Fall sein, wo ohnehin kontrollierbare Bedingungen vorliegen oder im Rahmen von gemeinsamen Vorplanungen mit dem Netzbetreiber oder „Besitzer“ des WLAN-Netzes bestimmte Dinge zugesichert werden. Denkbare Anwendungsfälle sind z. B.:

- Kontrollierbare Bereiche mit zentralem Zugriff, z. B. Werke oder Flughäfen, in denen es ohnehin WLAN-Netze „aus einer Hand“ gibt, und Schnittstellen zur Feuerwehr sowie die „Absicherung“ der Netze vorgeplant werden können.
- Großveranstaltungen, bei denen im Rahmen einer Vorplanung und Abstimmung mit dem Netzbetreiber Ressourcen für die Feuerwehr bereitgestellt werden, z. B. Versorgung einer temporären Einsatzleitung der Feuerwehr mit WLAN über einen öffentlichen Hotspot
- Große Sonderobjekte, bei denen ggf. schon in der Planungsphase in Zusammenarbeit mit Betreibern Schnittstellen zwischen Feuerwehr und geplantem WLAN-Netz festgelegt werden können.⁹

⁹ Zum Teil entsprechen solche Lösungen dann nicht mehr dem eigentlichen Charakter „offener“ WLAN-Netze.

9 Fazit

In dieser Arbeit wurde gezeigt, dass bei Feuerwehren grundsätzlich ein wachsender Bedarf an Möglichkeiten zur mobilen Datenübertragung am Einsatzort besteht. Auch für die beiden bearbeiteten Anwendungsbereiche „Einsatzkoordination und -dokumentation“ sowie „Überwachung der Einsatzkräfte“ stellt die Digitalisierung eine große Chance dar. Immer mehr digitale Führungsunterstützungs- und Überwachungssysteme sind heute schon erfolgreich im Einsatz. Die Übertragung aller Daten kann mit dem Tetra-BOS-Funk zurzeit nicht sichergestellt werden. Zur Kompensation setzen Hersteller entweder auf eigene Funknetze oder das Mobilfunknetz. Offene WLAN-Netze werden nicht berücksichtigt.

Nach der in dieser Arbeit durchgeführten Gegenüberstellung von Anforderungen und Leistungsmerkmalen offener WLAN-Netze kann ein eindeutiges Fazit gezogen werden. Für die beschriebenen Anwendungsfälle sind offene WLAN-Netze im Feuerwehreinsatz aus heutiger Sicht nicht oder nur bedingt geeignet. Hauptgrund dafür sind eine Vielzahl von Hürden, insbesondere bei den Themen Verfügbarkeit und Leistungsfähigkeit, durch die auch wesentliche Anforderungen der FwDV 800 (Informations- und Kommunikationstechnik im Einsatz) nicht erfüllt werden. Es ist klar erkennbar, dass WLAN-Netze für den „Consumer-Bereich“ und nicht für sicherheitskritische Bereiche wie den der Feuerwehr entwickelt wurden.

Durch die Vielzahl unterschiedlicher Netze und Anbieter und die damit verbundenen stark schwankenden Rahmenbedingungen ist es nicht möglich, sich als Feuerwehr gezielt auf die Nutzung offener WLAN-Netze vorzubereiten. Außerdem stehen z. B. mit dem Mobilfunk, Alternativen zur Verfügung, die im Vergleich deutlich stabiler und verbreiteter sind und in der Praxis heute schon z. T. höhere Datenübertragungsraten ermöglichen. Mit dem kommenden Mobilfunkstandard 5G werden diese nochmals deutlich steigen. Dadurch ist der Mehrwert einer WLAN-Nutzung im Einsatz – wenn überhaupt – insgesamt sehr gering.

Ausnahmen, bei denen offene WLAN-Netze einen Mehrwert darstellen können, stellen Situationen dar, in denen kontrollierbare Rahmenbedingungen vorliegen. Denkbar sind hier Bereiche wie Flughäfen oder Bahnhöfe, die ggf. über zentral gesteuerte Netze verfügen und somit gezielte Absprachen oder Vorbereitungen und definierte Schnittstellen ermöglichen. Auch gemeinsame Vorplanungen, z.B. mit städtischen Hotspot-Anbietern für Großereignisse oder Betreibern großer Sonderobjekte sind denkbar.

Für die Feuerwehr ergibt sich daraus die grundsätzliche Empfehlung, keine großen Anstrengungen oder Investitionen zu tätigen, um sich auf die Nutzung offener WLAN-Netze als Möglichkeit zur Datenübertragung am Einsatzort einzustellen. Lediglich in den genannten Einzelfällen sollten sich Feuerwehren der Ressource „offenes WLAN-Netz“ bewusst sein und möglichst frühzeitig durch Gespräche mit den Netzbetreibern „abstecken“, inwiefern eine Kooperation möglich und sinnvoll ist.

9.1 Alternativen

Weitreichendere Chancen könnten sich ergeben, wenn WLAN-Netze nicht wie in dieser Arbeit als Datenübertragungsmöglichkeit genutzt werden sollen, sondern den Einsatzkräften direkt Infos über das Gebäude oder darin befindliche Personen zur Verfügung stellen können. Die in Kapitel 5.6 kurz angeschnittenen Möglichkeiten zur Personenortung stellen einen Anwendungsbereich dar, der für die Feuerwehr einen erkennbaren Mehrwert darstellen

könnte. Wenn Daten über den Aufenthaltsort von Personen ohnehin schon vorliegen, muss es Wege geben, dass diese auch von der Feuerwehr „mitgenutzt“ werden. Heute ist das z. T. schon in Flughäfen und Shoppingcentern der Fall, zukünftig werden solche Daten im „Smart Home“ flächendeckend verfügbar sein. Für solche Bereiche ist dann sogar eine Übertragung auf Einsatzkräfte und deren Überwachung denkbar. Auch das heute schon mögliche „Auslesen“ eines WLAN-Netzes mittels geeigneter Netzwerkanalysertools könnte für die Feuerwehr hilfreich sein, wenn dadurch Informationen zu ggf. im Gebäude befindlichen Personen zur Verfügung gestellt werden. Letztendlich bietet es sich an, sich mit dem Thema WLAN-Ortung als Feuerwehr intensiver auseinanderzusetzen, und Möglichkeiten durch Praxistests konkret auszuloten.

9.2 Ausblick

Für die Zukunft ist davon auszugehen, dass sich offene WLAN-Netze weiter verbreiten und auch der Anteil der offenen im Vergleich zu geschlossenen WLAN-Netzen wachsen wird. Zu vermuten ist jedoch, dass sich die bestehenden Hürden, diese Netze als Datenübertragungsmöglichkeiten für die Feuerwehr zu nutzen, dabei nicht wesentlich verändern werden.

Um die Nutzung offener WLAN-Netze zukünftig zu vereinfachen, bestehen lediglich theoretische Lösungsansätze. So könnten Anbieter von WLAN dazu gebracht werden, eigene, nur von Einsatzkräften nutzbare Kanäle einzurichten. Dasselbe könnte auch in privaten Haushalten geschehen, indem Privatpersonen ihre WLAN-Netze für Rettungskräfte öffnen. Eine Verpflichtung zur Umsetzung solcher Maßnahmen erscheint aus heutiger Sicht jedoch unrealistisch, auch im Hinblick auf den überschaubaren Mehrwert, der daraus entstünde. Der rasante Fortschritt der Digitalisierung führt dazu, dass immer wieder neue Datenübertragungsstandards entwickelt werden. Schon heute ist WLAN im Hinblick auf die Nutzbarkeit durch die Feuerwehr nicht die führende Technologie und wird das vermutlich auch zukünftig nicht sein. In vielen Bereichen stellt der Mobilfunk – auch mit der Aussicht auf 5G – die bessere Alternative dar.

In Anbetracht der wachsenden Datenmengen kann daher die Empfehlung nur lauten, sich als Feuerwehr darauf einzustellen, zukünftig möglichst flexibel die jeweils beste vorhandene Verbindung zu nutzen – also auf sogenannte Multi Channel-Lösungen zu setzen. Dazu werden Geräte benötigt, die intelligent die beste Verbindung – ob nun WLAN, Mobilfunk, Satellit oder ein anderer Kanal – erkennen und intelligent zwischen den „Channels“ wechseln. Über gesicherte Clouds können die Daten dann den Nutzern zur Verfügung gestellt werden.

Durch die Möglichkeit der flexiblen Nutzung vorhandener und zukünftiger Kanäle wird es der Feuerwehr einfacher gelingen, „vor die Lage zu kommen“ und nicht mit großem zeitlichen und finanziellen Aufwand auf Infrastrukturen zu setzen, die schnell „veraltet“ sind.

Parallel dazu muss es eine Analyse der Datenströme geben, die zukünftig im Feuerwehreinsatz von Bedeutung sein werden, und mit welcher Priorität diese im Einsatz vorliegen bzw. übertragen werden müssen. Erst wenn festgelegt ist, welche Daten einsatzkritisch sind, und welche „nur“ als zusätzliche, hilfreiche Information dienen, ist es möglich, eine differenzierte Aussage darüber zu treffen, welche Kanäle dafür nutzbar sind und welche Anforderungen an diese zu stellen sind.

Quellenverzeichnis

Andric, Ivan (18.10.2018): Experteninterview, durchgeführt vom Verfasser. Gruppenleiter Systemberatung, NetCologne Gesellschaft für Telekommunikation mbH.

Bäker, Linnart (15.11.18): persönliche Kommunikation. Brandreferendar, Mitentwickler der FireApp, Berliner Feuerwehr.

Baumann, Heinz (2010): Datenabfrage am Einsatzort. Online-Führungsunterstützung. In: *Schweizerische Feuerwehr-Zeitung* 136 (11), S. 56–57.

BBK (2011): Semipermeable Anzüge für Einsatzkräfte - SAFE. Abschlussbericht Teilvorhaben FKZ 13N9810: Grundlegende Untersuchung zur Integration intelligenter Telemetrie in Schutzzanzügen. Hg. v. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. Online verfügbar unter https://www.bbk.bund.de/DE/Service/Fachinformationsstelle/Informationsangebote/Forschungsberichte/ForschungsprogrammSicherheitsforschung/Integrierte%20Schutzsysteme/SAFE/SAFE_node.html, zuletzt geprüft am 10.12.2018.

BD Maurer; BA Backes; BA Jungverdorben; OBM Kolberg; Schwägergen; BD Kircher et al. (1996): Schlußbericht der Unfallkommission zum Einsatz Kierberger Straße 15, 06.03.1996, 13.42 Uhr. Köln. Online verfügbar unter <https://www.atemschutzunfaelle.de/download/Unfaelle/Stampe/u19960306-koeln-abschlussbericht.pdf>, zuletzt geprüft am 07.12.2018.

BDBOS (o.J.): Netzhärtung. Hg. v. Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben. Online verfügbar unter https://www.bdbos.bund.de/DE/Fachthemen/netzhaertung/netzhaertung_node.html, zuletzt geprüft am 08.12.2018.

Berliner Feuerwehr (2010): FeuerWhere - Sichere und effiziente Ortung von Einsatzkräften durch Sensornetze. Schlußbericht der Berliner Feuerwehr im Verbundprojekt FeuerWhere. Hg. v. Berliner Feuerwehr. Online verfügbar unter <http://edok01.tib.uni-hannover.de/edoks/e01fb12/728467933.pdf>, zuletzt geprüft am 31.10.2018.

Block, Klaus (2018): Feuerwehr-Dienstvorschrift 800: Informations- und Kommunikationstechnik im Einsatz. Die neue FwDV 800 ist den Ländern zur Einführung empfohlen. In: *BRANDSchutz* 72 (7), S. 554–557.

Block, Klaus (08.11.2018): persönliche Kommunikation. Ministerium des Innern des Landes Nordrhein-Westfalen. Leiter der Arbeitsgruppe FwDV/DV 800/810.

BMWi (o.J.): Netzpolitik. Bundesministerium für Wirtschaft und Energie. Online verfügbar unter <https://www.bmwi.de/Redaktion/DE/Dossier/netzpolitik.html>, zuletzt geprüft am 13.12.2018.

Bruckmann, Benjamin (22.10.18): persönliche Kommunikation. Feuerwehr Wesel.

BSI (o.J.): IT-Grundschutz. NET.2.1 WLAN-Betrieb. Hg. v. Bundesamt für Sicherheit in der Informationstechnik. Online verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompodium/bausteine/NET/NET_2_1_WLAN-Betrieb.html?nn=10137160#doc10095872bodyText1, zuletzt geprüft am 02.11.2018.

- Bundesnetzagentur (o. J.): BOS - der digitale Bündelfunk basierend auf TETRA. Online verfügbar unter <https://emf2.bundesnetzagentur.de/pdf/BOS-BNetzA.pdf>, zuletzt geprüft am 09.11.2018.
- DGAUM (2018): Smarte Schutzausrüstungen im Feuerwehreinsatz. Deutsche Gesellschaft für Arbeitsmedizin und Umweltmedizin e.v. Online verfügbar unter https://www.dgaum.de/kommunikation/pressemitteilungen/meldung/?tx_ttnews%5Btt_news%5D=216&cHash=699ecfb10723a5f575a5b7fe66cd28cc, zuletzt aktualisiert am 09.10.2018, zuletzt geprüft am 10.11.2018.
- Dörner, Stefan (2016): Deutschland blamiert sich als WLAN-Wüste. In: *WELT*, 16.03.2016. Online verfügbar unter <https://www.welt.de/wirtschaft/webwelt/article153354781/Deutschland-blamiert-sich-als-WLAN-Wueste.html>, zuletzt geprüft am 02.11.2018.
- Dräger (o. J.a): Atemschutzüberwachung. Dräger PSS Merlin System. Online verfügbar unter https://www.draeger.com/de_de/Fire-Services/Products/Personal-Protection-Equipment/Breathing-Apparatus/Control-Boards/PSS-Merlin-System, zuletzt geprüft am 04.12.2018.
- Dräger (o. J.b): Genutzte Systeme zur Datenübertragung. Unveröffentlichte Präsentation.
- Eisele, Daniel; Grigorjew, Olga; Matzner, Tobias; Morlok, Tina; Nebel, Maxi; Ochs, Carsten et al. (2017): White Paper Privatheit in öffentlichen WLANs. Spannungsverhältnisse zwischen gesellschaftlicher Verantwortung, ökonomischen Interessen und rechtlichen Anforderungen. Hg. v. Murat Karaboga, Michael Friedewald, Regina Ammicht Quinn, Marit Hansen, Jessica Heesen, Thomas Hess, et al. Karlsruhe (Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt). Online verfügbar unter <http://hdl.handle.net/11159/823>.
- Favendo (o.J.): Shopping in Bewegung. Wie Positionierung, Indoornavigation und personalisiertes mobile Marketing den stationären Handel in Bewegung bringen. Hg. v. Favendo GmbH. Online verfügbar unter https://www.favendo.com/wp-content/uploads/2017/04/favendo_shopping-in-bewegung_de-1.pdf, zuletzt geprüft am 09.11.2018.
- FAZ (2010): Street View scannt WLAN: Google sammelt Daten von privaten Netzwerken. In: *Frankfurter Allgemeine Zeitung*, 22.04.2010. Online verfügbar unter <https://www.faz.net/aktuell/technik-motor/digital/street-view-scannt-wlan-google-sammelt-daten-von-privaten-netzwerken-1971267.html>, zuletzt geprüft am 10.12.2018.
- FIT (o.J.): Landmarke. Navigationsunterstützung für Feuerwehrleute. Fraunhofer-Institut für Angewandte Informationstechnik. Online verfügbar unter <https://www.fit.fraunhofer.de/de/fb/ucc/projects/landmarke.html>, zuletzt aktualisiert am 02.11.2018, zuletzt geprüft am 02.11.2018.
- Fraunhofer IIS (2018): RSSI - Received Signal Strength Indication. Die autarke Lokalisierungstechnologie für Städte und Gebäude. Hg. v. Fraunhofer-Institut für Integrierte Schaltungen. Online verfügbar unter <https://www.iis.fraunhofer.de/de/ff/lv/lok/tech/feldstaerke/rssi/tl.html>, zuletzt geprüft am 09.11.2018.

FwDV 100: Feuerwehr-Dienstvorschrift 100. Führung und Leitung im Einsatz. Ausgabe März 1999. Hg. v. AFKzV.

FwDV 7: Feuerwehr-Dienstvorschrift 7. Atemschutz. Ausgabe August 2004. Hg. v. AFKzV.

FwDV 800: Feuerwehr-Dienstvorschrift 800. Informations- und Kommunikationstechnik im Einsatz. Ausgabe November 2017. Hg. v. AFKzV.

Gödde, Florian; Wessels, Martin (2011): SensProCloth. Systemintegrierte sensorische Schutzkleidung für Feuerwehr und Katastrophenschutz. Teilprojekt: Erfassung und Weitermeldung von physiologischen Zustandsparametern und Umgebungsbedingungen mit Ortung zur Einleitung von Hilfsmaßnahmen. Hg. v. Branddirektion der Landeshauptstadt Stuttgart. Online verfügbar unter <http://edok01.tib.uni-hannover.de/edoks/e01fb12/729004171.pdf>, zuletzt geprüft am 02.11.2018.

Harz, Bernhard (22.10.2018): Experteninterview, durchgeführt vom Verfasser. Abteilungsleiter Informationstechnik, Berliner Feuerwehr.

Häusler, Joseph (22.10.2018): persönliche Kommunikation. Project Manager, infsoft GmbH.

Heeg, Thiemo (2018): Bodycams sollen Feuerwehrleuten mehr Überblick geben. Pilotprojekt in Darmstadt. In: *Frankfurter Allgemeine*, 15.11.2018. Online verfügbar unter www.faz.net/aktuell/wirtschaft/feuerwehr-darmstadt-bodycams-gegen-das-unfallchaos-15892877.html, zuletzt geprüft am 30.11.2018.

Hegemann, Lisa (2018): Sie haben hier immer noch kein WLAN, oder? Kommentar zum BGH-Urteil. In: *Zeit Online*, 26.07.2018. Online verfügbar unter <https://www.zeit.de/digital/internet/2018-07/bgh-urteil-offenes-wlan-stoerer-haftung-hotspots>, zuletzt geprüft am 02.11.2018.

Helm, Jan; Dyrks, Tobias; Wulle, Matthias; Betz, Matthias (2014): Der Atemschutzeinsatz in der Zukunft. Diskussion eines neuen Nachrichten-Übermittlungssystems. In: *BRANDSchutz* (4), S. 289–294.

Hesse, Michael (2018): Freies Wlan ist Mangelware. Die Deutschen leben im Internet-Mittelalter. In: *Kölner Stadt-Anzeiger*, 01.11.2018. Online verfügbar unter <https://www.ksta.de/panorama/freies-wlan-ist-mangelware-die-deutschen-leben-im-internet-mittelalter-31527170>, zuletzt geprüft am 02.11.2018.

HMWEVL (2017): Leitfaden Öffentliche WLAN-Netze in Kommunen. Hg. v. Hessisches Ministerium für Wirtschaft, Energie, Verkehr und Landesentwicklung. Online verfügbar unter https://www.breitband-in-hessen.de/mm/Leitfaden_WLAN_final.pdf, zuletzt geprüft am 08.11.2018.

Hofmann, Philipp; Kuladinithi, Koojana; Timm-Giel, Andreas; Görg, Carmelita; Bettstetter, Christian; Capman, Francois; Toulosy, Christian (2006): Are IEEE 802 Wireless Technologies Suited for Fire Fighters?

infsoft (o.J.): Indoor Positionsbestimmung und Indoor Navigation mit WLAN. Hg. v. Infsoft GmbH. Online verfügbar unter <https://www.infsoft.com/de/technologie/sensorik/wlan>, zuletzt geprüft am 10.11.2018.

Karcher, Harald (2014): WLAN versus Mobilfunk. 10 Gigabit/s auf dem Handy - wer macht das Rennen? Hg. v. Computerwoche. Online verfügbar unter

<https://www.computerwoche.de/a/10-gigabit-s-auf-dem-handy-wer-macht-das-rennen,3065939>, zuletzt geprüft am 02.11.2018.

Landefeld, Klaus (2014): Verbreitung und Nutzbarkeit von WLAN, WLAN-Zugangspunkten sowie öffentlicher Hotspots in Deutschland. Hg. v. Verband der deutschen Internetwirtschaft e.V. (eco Microresearch). Online verfügbar unter https://www.eco.de/wp-content/blogs.dir/eco-microresearch_verbreitung-und-nutzung-von-wlan1.pdf, zuletzt geprüft am 03.10.2018.

Lenz, Gilbert (22.10.18): persönliche Kommunikation. Key Account Manager Telemetry, SCBA & Gallet, MSA Deutschland GmbH.

Linge, Guido (22.10.18): persönliche Kommunikation. Vertriebsingenieur, Dräger Safety AG & Co. KGaA.

Markland, David (2016): High speed in-vehicle networks for fire apparatus. In: *International Fire Fighter* (51), S. 70–72.

Maue, Manfred (16.10.2018): Experteninterview, durchgeführt vom Verfasser. Geschäftsführer AWADES GmbH & Co. KG Leitstellenplanung.

MSASafety (o. J.): Atemschutz. alpha Personal Network. Online verfügbar unter <http://de.msasafety.com/Isolieratemschutz/Überwachungsanlagen/alpha-Personal-Network/p/000010001900001353>, zuletzt geprüft am 04.12.2018.

MWIDE NRW (2018): Leitfaden öffentliches WLAN in NRW. im Auftrag des Ministeriums für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen. 1. Auflage. Hg. v. Kompetenzzentrum Gigabit.NRW. Online verfügbar unter https://gigabit.nrw.de/images/PDFs/Leitfaden/Leitfaden_oeffentliches_WLAN_in_NRW.pdf, zuletzt geprüft am 02.11.2018.

NetCologne (2017): Digitalisierungs-Offensive für Köln: NetCologne investiert 100 Mio. Euro. Online verfügbar unter <https://www.netcologne.de/ueber-uns/unternehmen/presse/mitteilung/digitalisierungs-offensive-fuer-koeln-netcologne-investiert-100-mio-euro-18622/>, zuletzt geprüft am 07.12.2018.

Nichols, Shaun (2017): US cops, firefighters to get new emergency wireless network – AT&T to get \$6.5bn. Telco lands mega-deal to host first responders broadband. Online verfügbar unter https://www.theregister.co.uk/2017/03/30/new_att_comms_network_for_cops_firefighters/, zuletzt geprüft am 03.10.2018.

Nicklas, Gero (06.11.2018): persönliche Kommunikation. Geschäftsführer BOS Connect GmbH.

Ruthmann, Guido (08.11.2018): Experteninterview, durchgeführt vom Verfasser. Leiter Corporate Network / Systemberatung, NetAachen GmbH.

Sauter, Martin (2018): Grundkurs mobile Kommunikationssysteme. LTE-Advanced Pro, UMTS, HSPA, GSM, GPRS, Wireless LAN und Bluetooth. 7. Auflage. Wiesbaden: Springer Vieweg (SpringerLink Bücher). Online verfügbar unter <http://dx.doi.org/10.1007/978-3-658-21647-4>.

Schmehl, Frank (05.12.2018): persönliche Kommunikation. Brandrat, Feuerwehr Duisburg.

Temmler, Mirko (2010): WLAN bei Großschadenslagen. Technische Kommunikation auf dem Behandlungsplatz. In: *Im Einsatz* 17, S. 38–41.

Truthän, Stefan (12.11.2018): Experteninterview, durchgeführt vom Verfasser. Geschäftsführender Gesellschafter, hhpberlin Prüfgesellschaft für Brandschutz mbH.

Unfallkommission "Tübingen" (2006): Bericht zum Einsatz Tübingen, Reutlinger Straße 34/1 am 17. Dezember 2005. Hg. v. Innenministerium Baden Württemberg. Online verfügbar unter <https://www.atemschutzunfaelle.de/download/Unfaelle/u20051217-tuebingen-bericht-unfallkommission.pdf>, zuletzt geprüft am 07.12.2018.

Urban, Vincent (16.10.18): persönliche Kommunikation. Werkfeuerwehr BASF, Ludwigshafen.

Vodafone (2018): Ein Fall für die Feuerwehr. Sichere Kommunikation im Katastrophenfall. Hg. v. Vodafone GmbH. Online verfügbar unter <https://www.vodafone.de/featured/digital-life/ein-fall-fuer-die-feuerwehr-sichere-kommunikation-im-katastrophenfall/>, zuletzt aktualisiert am 09.11.2018.

Wiedemann, Robert (18.10.2018): Experteninterview, durchgeführt vom Verfasser. Portfoliomanagement Geschäftskunden, HotSpot & Mobile Solutions bei Telekom Deutschland GmbH.

Wiedemann, Thomas (24.10.2018): persönliche Kommunikation. Leiter der Fachgruppe Führung und Kommunikation, THW Ortsverband Ofterdingen.

Anhang

- Anhang A: Aufgabenstellung für die vorliegende Arbeit
- Anhang B: Abbildungen
- Anhang C: Übersicht über die Experteninterviews und sonstigen Anfragen
- Eidesstattliche Erklärung

Anhang A: Aufgabenstellung für die vorliegende Arbeit

Institut der Feuerwehr Nordrhein-Westfalen		
Institut der Feuerwehr NRW, Postfach 4967, 48028 Münster		Datum: 21.09.2018
Herr Max Schmid Beuelsweg 5 a 50733 Köln		Aktenzeichen Z2-5-2-05 bei Antwort bitte angeben
		Nicole Krüler Telefon 0251 3112-4202 Telefax 0251 3112-4299 pruefungsamt@idf.nrw.de
 Ausbildung für das zweite Einstiegsamt der Laufbahngruppe 2 des höheren feuerwehrtechnischen Dienstes hier: Facharbeit		
Sehr geehrter Herr Schmid,		
nachstehend teile ich Ihnen das Thema der Facharbeit mit:		
Nutzung von offenen WLAN-Netzen im Feuerwehreinsatz Sowohl im betrieblichen Umfeld als auch in den Kommunen finden offene WLAN-Netze eine rasche Verbreitung. Wie können Feuerwehren diese neuen Datenübertragungswege für die Überwachung der Einsatzkräfte (Atemschutz, Vitaldaten, Technische Daten, ...), der Einsatzkoordination und -dokumentation nutzen?		
Ich bitte um Vorlage der Arbeit in dreifacher Ausfertigung (zwei gebundene Exemplare und ein Exemplar als pdf-Datei auf CD) spätestens drei Monate nach Erhalt dieses Schreibens.		
Die mit dem Facharbeitsthema ausgehändigte Lizenzvereinbarung ist mit der Facharbeit einzureichen.		
Mit freundlichen Grüßen		
		Dienstgebäude und Lieferanschrift: Wolbecker Str. 237 48155 Münster Telefon 0251 3112-0 Telefax 0251 3112-1099 poststelle@idf.nrw.de www.idf.nrw.de
		Öffentliche Verkehrsmittel: Buslinien 11, 22, R22, R32, N84, Hauptbahnhof Münster (Bussteig A) bis Haltestelle „Institut der Feuerwehr“

Abbildung 3 – Anhang: Aufgabenstellung für die vorliegende Arbeit

Anhang B: Abbildungen

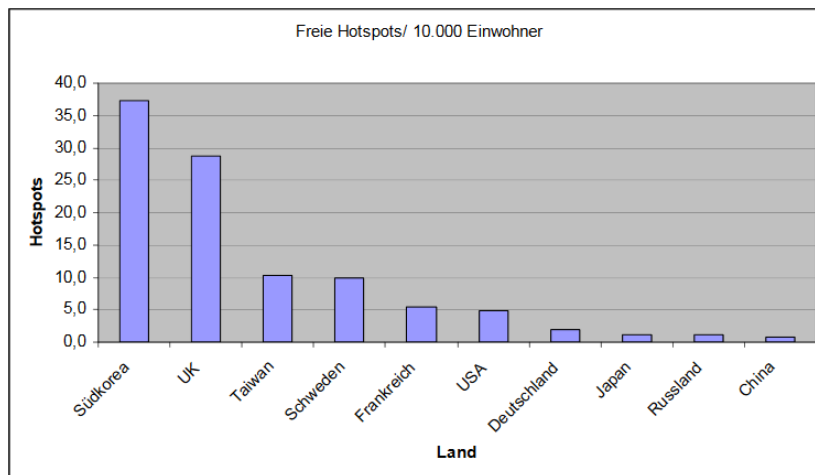


Abbildung 4 – Anhang: Freie Hotspots pro 10.000 Einwohner im 4. Quartal 2014 im Vergleich (Quelle: Landefeld 2014)

Welche Systeme werden genutzt? **Dräger**

Kommunikation	HART® 	Der weit-genutzte HART® Kommunikationsstandard, erlaubt digitale Kommunikation zwischen verschiedenen Detektoren, geteilt über einen Datenbus.
	WirelessHART 	
	GSM network 	GSM ist der Standard für das voll-digitale Mobilfunknetz. Es wird genutzt, um Daten zur oder von der Cloud zu transferieren
	Bluetooth 	Mit dem industriellen Bluetooth Standard können Geräte bis zu einer Distanz von 25 Metern miteinander kommunizieren.
Geodaten	LoRa 	LoRa steht für long-range wide-area network. LoRa ist ein neuer Standard für das Internet der Dinge.
	GPS 	GPS, der Standard für ein globales, satellitengestütztes Navigationssystem, kann verwendet werden, um Gegenstände in einer Industrieanlage zu lokalisieren.
	Beacon 	Standard, basierend auf Bluetooth Low Energy (BLE), eingeführt von Apple zur Lokalisierung in geschlossenen Räumen

Abbildung 5 – Anhang: Beispiel für die von der Firma Dräger genutzten Technologien zur Datenübertragung (Quelle: Dräger o. J.b)

Anhang C: Übersicht über die Experteninterviews und sonstigen Anfragen

Für die vorliegende Arbeit wurden im Rahmen von Experteninterviews mehrere Experten aus den Bereichen BOS, IT-Sicherheit und WLAN-Netzbetreiber ausgewählt und befragt. Schwerpunkt der Interviews war jeweils die Einschätzung, ob und unter welchen Voraussetzungen offene WLAN-Netze durch die Feuerwehr genutzt werden können. Die folgende Tabelle stellt die Zuordnung der ausgewählten Experten zu ihrem beruflichen Hintergrund dar.

Tabelle 3 – Anhang: Im Rahmen der Arbeit befragte Experten mit Zuordnung zum beruflichen Hintergrund sowie dem Schwerpunkt der jeweiligen Expertise

Befragte Experten	BOS	Netzbetreiber	IT-Experte
R. Wiedemann - Portfoliomanagement Geschäftskunden, HotSpot & Mobile Solutions, Telekom Deutschland GmbH		x	
M. Maue – Geschäftsführer AWADES GmbH & Co. KG Leitstellenplanung	x		x
I. Andric – Gruppenleiter Systemberatung, NetCologne GmbH		x	
B. Harz – Abteilungsleiter Informationstechnik, Berliner Feuerwehr	x		
G. Ruthmann – Leiter Corporate Network / Systemberatung, NetAachen GmbH		x	
S. Truthän – Geschäftsführender Gesellschafter, hhpberlin Prüfungsgesellschaft für Brandschutz mbH	x		x

Zusätzlich zu den Experteninterviews wurden zur Informationsbeschaffung eine Reihe weiterer schriftlicher und mündlicher Anfragen durchgeführt. Im Folgenden werden nur die Anfragen aufgeführt, deren Ergebnisse in die vorliegende Arbeit eingeflossen sind.

- Linnart Bäker, Brandreferendar, Entwickler der FireApp, Berliner Feuerwehr
- Frank Schmehl, Brandrat, Entwickler des MoFIS, Berufsfeuerwehr Duisburg
- Thomas Wiedemann, Leiter Fachgruppe Führung und Kommunikation, THW OV Ofterdingen
- Vincent Urban, Werkfeuerwehr BASF, Ludwigshafen
- Gero Nicklas, Geschäftsführer BOS-Connect GmbH
- Guido Linge, Vertriebsingenieur Dräger Safety AG & Co. KGaA
- Gilbert Lenz, Key Account Manager MSA Deutschland GmbH
- Joseph Häusler, Project Manager Infsoft GmbH
- Benjamin Bruckmann, Feuerwehr Wesel
- Dr. Klaus Block, Innenministerium Nordrhein-Westfalen

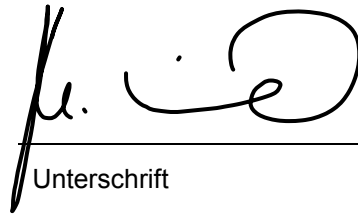
(Anmerkung: Die Interviewpartner und sonstigen Anfragen sind hier aus Gründen der Übersichtlichkeit nochmals zusammenfassend dargestellt. Sämtliche Quellen werden auch im Text und im Quellenverzeichnis genannt.)

Eidesstattliche Erklärung

Hiermit versichere ich, dass ich die vorliegende Facharbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Alle Ausführungen, die anderen Quellen wörtlich oder sinngemäß entnommen wurden, sind kenntlich gemacht. Die vorliegende Facharbeit war in gleicher oder ähnlicher Fassung noch nicht Bestandteil einer Prüfungsleistung.

Köln, 21.12.2018

Ort, Datum



Unterschrift