AFCEA Zukunfts- und Technologieforum 2020 – Internet of (Military) Things
29. Oktober 2020

www.fkie.fraunhofer.de/afcea-zut-2020

09:00 Uhr – ca. 16:00 Uhr

Begrüßung und thematische Einführung
BG Armin Fleischmann, Vorstand AFCEA
Dr. Michael Gerz, Fraunhofer FKIE

Entwicklung und Einsatz automatisierter Systeme für zukünftige Landstreitkräfte
OTL Thomas Doll, Amt für Heeresentwicklung

Hybride Bedrohungen – Bedarfe und deren Umsetzung zur Weiterentwicklung für den Bereich Wirkung im Cyber - und Informationsraum
Maj Stefan Langnau, Kommando Cyber- und Informationsraum

Operationsszenar Aufmarsch 20xx – Spannungsfeld IoT
OTL i.G. Ruben Thiel, Kommando Feldjäger

Kaffeepause

Einsatzszenarien und Möglichkeiten einer IoT-Plattform im militärischen Umfeld
Olivier Spiess, Software AG

IoT im militärischen Kontext – Potentiale, Anforderungen und Integrationsmöglichkeiten
Christoph Fuchs, Fraunhofer FKIE

Ökosysteme als Voraussetzung für (Military) IoT
Frank Feldkeller, IBM

Mittagspause

Schwarmsysteme und automatisierte Auswertung auf Grundlage von Plattformsystemen in taktischen Szenarien
Dr. Thomas Bierhoff, Atos Information Technology GmbH

Künstliche Intelligenz und Io(M)T im Feldeinsatz
Thorsten Wujek, Steep GmbH

Erhöhung der Flottenverfügbarkeit in einem skalierbaren Betriebsmodell
Florian Dörr, Hewlett-Packard Enterprise

Kaffeepause

IoT in Desaster Recovery-Szenarien
Manas Pradhan, Fraunhofer FKIE

Der Beitrag von IoT zur Sicherheit von Großveranstaltungen
Dr. Markus Eisenhauer, Luxembourg Institute of Science and Technology

Elektronische Textilien – Ein technologischer Überblick und potenzielle Anwendungsmöglichkeiten beim Militär
Malte von Krshiwoblozki, Fraunhofer IZM

Abschlussbesprechung

Abstracts

Entwicklung und Einsatz automatisierter Systeme für zukünftige Landstreitkräfte
OTL Thomas Doll, AHEntwg ThomasManfredDoll@bundeswehr.org
Der Vortrag beschreibt auf Grundlage einer zusammengefassten Analyse zukünftiger Gefechte, wie sich die voranschreitende Automatisierung auf das Fähigkeitsspektrum der Landstreitkräfte ab 2040 auswirken wird. Hierzu wird zunächst die Entwicklung zukünftiger Remote and Automated Systems (RAS) in den drei Stufen „Mechanische Verstärkung“, „Kognitive Verstärkung“ und „Quantitative Verstärkung“ untersucht. Die Entwicklung, und letztendlich auch der Einsatz dieser Systeme zielt darauf ab, menschgeführte Strukturen so zu verstärken, dass sie in Kampfkraft, Schnelligkeit und Durchhaltefähigkeit konkurrenzfähig bleiben. Die im Folgenden behandelte zwei Stoßrichtungen-Strategie macht deutlich, dass es neben der klassischen Weiterentwicklung bestehender Systeme und Waffensysteme zwingend auch den Zweig der disruptiven Heeresentwicklung geben sollte. Nur so kann sichergestellt werden, dass auch neue, ggf. sehr wirkungsvolle Konzepte, die sich nicht an klassischen Grundsätzen und Strukturen orientieren, Eingang in den Rüstungsprozess finden. Das abschließend vorgestellte Beispiel eines „Multifunktionalen Taktischen Unmanned Aerial Systems“ untermauert diesen Ansatz und rundet den Vortrag inhaltlich ab.

Hybride Bedrohungen – Bedarfe und deren Umsetzung zur Weiterentwicklung für den Bereich Wirkung im Cyber - und Informationsraum
Maj Stefan Langnau, KdoCIR stefanlangnau@bundeswehr.org
Hybride Bedrohungen sind allgegenwärtig. Überall wird darüber gesprochen und berichtet. Für den Bereich „Wirkung im CIR“ stellen sich daraus die Fragen: • Was genau sind *heute* Hybride Bedrohungen? • Was können Hybride Bedrohungen *morgen* und *übermorgen* sein? • Wie ist der deutsche Soldat diesen Bedrohungen ausgesetzt? • Welche Elemente müssen entwickelt werden, damit der deutsche Soldat auch in Zukunft seinen Auftrag erfüllen kann? Dies alles wird immer im Kontext des IoT aus der militärischen Perspektive betrachtet. Die Smartwatch ist schließlich nicht mehr wegzudenken. Im Vortrag wird ein kurzer Überblick gegeben, wie der Bereich „Wirkung im CIR“ sich dieser permanenten Herausforderung stellt, um gegebenenfalls Denkanstöße zu geben, aber auch neue Impulse zu gewinnen.

Operationsszenar Aufmarsch 20xx – Spannungsfeld IoT
OTL i.G. Ruben Thiel, Kommando Feldjäger rubenthiel@bundeswehr.org
Verlegeoperation 20xx: Der Militärpolizist blickt auf sein Tablet und überprüft die Aufklärungsergebnisse seiner Drohne. Der Feind konnte durch Zugriff auf Überwachungskameras frühzeitig die Kräfte aufklären. Die eigentliche Marschroute wurde über Nacht unpassierbar gemacht. Das Tablet schlägt Alternativroute Charlie vor, durch Klick wird die neue Route an die Marschgruppe weitergegeben.

Flächendeckende Sensoren und automatisierte Verarbeitung ermöglichen Verlegungen in immer größeren Operationsräumen, gleichzeitig stehen durch Einsatz von IoT aber auch dem Gegner Möglichkeiten zur Verfügung, Bewegungen aufzuklären. In diesem Spannungsfeld entwickeln sich Verlegeoperationen zu Situationen, in denen der eigene Einsatz genauso wichtig wird wie die Abwehr des gegnerischen Zugriffs von IoT.

Einsatzszenarien und Möglichkeiten einer IoT-Plattform im militärischen Umfeld

Olivier Spiess, Software AG
oliver.spiess@softwareag.com

Der Begriff "Internet of Military Things" (IoMT) wird häufig auf die Bereiche „Internet of Battlefield Things" (IoBT) und „Connected Soldier" reduziert. Genauer betrachtet sind die Einsatzmöglichkeiten aber viel umfassender. So gibt es durchaus interessante Use Cases für IoT auch außerhalb von militärischen Operationen, wie z. B. „Smart Military Bases" oder die Verwaltung von zivilen Armee-Fahrzeugen (Fuhrpark Management).
In unserem Vortrag möchten wir aufzeigen, wie mit Hilfe einer IoT-Plattform sowohl die typischen Anwendungsszenarien im Einsatz, als auch die erweiterten Use Cases außerhalb von militärischen Operationen abgebildet werden können.

IoT im militärischen Kontext - Potentiale, Anforderungen und Integrationsmöglichkeiten

Christoph Fuchs, Fraunhofer FKIE

Die zunehmende Verbreitung des Internet of Things (IoT) im zivilen Umfeld und in allen Bereichen der modernen Gesellschaft hat ebenfalls Einfluss auf den militärischen Sektor. Es ergibt sich die Frage, ob IoT-Technologien auch im militärischen Einsatzfeld zur Anwendung kommen können und welcher Mehrwert dadurch potentiell erzielt werden kann. Gleichzeitig müssen die besonderen Anforderungen im Rahmen einer militärischen Nutzung und eventuell entstehende Risiken betrachtet werden.

Die Einbindung von IoT in ein militärisches Umfeld kann dabei auf unterschiedliche Arten erfolgen. Eine Möglichkeit besteht in der Übertragung und Anpassung existierender ziviler IoT-Anwendungen. Eine andere ist die Entwicklung spezifischer militärischer IoT-Geräte. Ebenfalls kann eine Nutzung vorhandener IoT-Informationen des öffentlichen Raums, insbesondere im Rahmen urbaner Operationen, erfolgen.

Im Rahmen der NATO-Forschungsgruppe IST-147 „Military Applications of Internet of Things" wurden mögliche Anwendungsbereiche für IoT-Technologien im militärischen Kontext betrachtet sowie besondere Anforderungen für deren Einsatz identifiziert. Weiterhin wurden Ansätze zur Integration in die militärische Kommunikationsinfrastruktur entwickelt. Dieser Vortrag gibt einen Einblick in die hier gewonnenen Erkenntnisse und entwickelten Konzepte.

Ökosysteme als Voraussetzung für (Military) IoT

Frank Feldkeller, IBM,
frank.feldkeller@de.ibm.com, +49 173 102 4573

Seitdem 1982 der erste Getränkeautomat seinen Dosenbestand über das Internet „gemeldet" hat, darf nunmehr im Jahr 2020 davon ausgegangen werden, dass das „Internet of Things" mehr als nur ein Trend ist. In unserer entwickelten Ökonomie ist die Nutzung der Möglichkeiten eines IoT genau das Konzept, welches die nächsten Effizienzsprünge und Funktionalitätsexplosionen verspricht.

Realisiert wird dies letztlich durch unzählige Sensoren, Protokolle, Applikationen etc., kurz Technologie, deren Leistungsfähigkeit bei immer schnelleren Entwicklungszyklen beständig steigt. Sie darf heute als Hygienefaktor für die kühnsten Ideen angesehen werden. Diesen Ideen aber ist eines gemein: Sie alle schöpfen ihren vollen Wert erst aus Ökosystemen. Aufgrund der Gesamtheit aller bei der Wertschöpfung anfallenden Aktivitäten kann eine Organisation alleine keine wesentlichen Effizienzgewinne mehr erwarten. Ganz im Gegenteil: Die stetig steigende Komplexität der Prozesse, der genutzten Geräte etc. führt dazu, dass eine Organisation alleine ceteris paribus ineffizienter werden muss. Damit kommt es entscheidend darauf an, in wie weit es gelingt, ein Ökosystem aus verschiedenen Organisationen aufzubauen und in diesem eine reibungsarme Zusammenarbeit zu kultivieren, die über alle Organisationsgrenzen der Mitglieder in diesem Ökosystem hinweg Mehrwerte schafft. Aktuelle Projekte und Studien stützen diese These und damit wird die Beantwortung einer vermeintlich einfachen Frage zur dringlichsten Aufgabe: Welche Rolle nimmt die Bundeswehr in diesem Ökosystem ein?
Der Vortrag soll anhand von aktuellen Projektreferenzen (bspw. Port of Rotterdam) und Studien (C-Suite Study 2019) Anregungen zur Diskussion jener Frage sowie nachgelagerter Implikationen für bestehende Prozesse und die gelebte Projektpraxis bieten.

Schwarmsysteme und automatisierte Auswertung auf Grundlage von Plattformsystemen in taktischen Szenarien

Dr. Thomas Bierhoff, Atos Information Technology GmbH
thomas.bierhoff@atos.net

Digitale Plattformen werden die taktische Kollaboration alliierter Kräfte (sowohl menschlich als auch maschinenzentriert) prägen, indem autonome service-orientierte Prozessketten eingerichtet werden. Durch die hohe Dynamik von taktischen Operationen und die Kritikalität von nahezu Echtzeit-Informationen sind cloud-basierte Lösungen nach derzeitigem Technologiestand nur unzureichend nutzbar bzw. entsprechen nicht den militärischen Anforderungen.
Eine Lösung bieten edge-gehostete und verteilte digitale Plattformsysteme, die durch digital automatisierte, konsistente Prozessketten den Kampf- und Einsatzwert alliierter Kräfte signifikant steigern. Dabei stellt das mobile Gefechtsfeldszenario mit dynamisch veränderlichen Netzwerkqualitäten, Verbindungsabbrüchen und Teilverfügbarkeiten von Teilnehmern und Fachanwendungen auf den unterschiedlichen Rechnerplattformen einen hohen Anspruch an ein militärisches IoT. Die Integration von proprietären Anwendungen ist elementar für die Realisierung eines ganzheitlichen „Battlefield Internet“.
Als praktisches Beispiel aus aktueller F&T der Bundeswehr stellt Atos die Studie „Erzeugung eines gläsernen Gefechtsfeldes zur Unterstützung dynamischer Operationen“ (ErzUntGlas) vor. Im Rahmen von ErzUntGlas wird ein taktisches Aufklärungs- und Führungssystems erprobt, das auf einem Schwarm von „Unmanned Aerial Systems“ (UAS) basiert. Um die geforderten fachlichen Funktionen im Rahmen von Aufklärung und Führung sowie deren operativen Mehrwert demonstrieren zu können, müssen verschiedene Fachanwendungen (z. B. BMS, BFT) sowie Kerndienste (z. B. Drohnensteuerung, taktische Kollaboration) integriert und miteinander verknüpft werden. Dies wird einerseits die Arbeitsbelastung der Kombattanten entlasten und andererseits die Streitkräfte vor Ort mit neuen digitalen Diensten und daraus abgeleiteten militärischen Fähigkeiten unterstützen.

Künstliche Intelligenz und Io(M)T im Feldeinsatz

Thorsten Wujek, Steep GmbH
thorsten.wujek@steep.de

Um den sicherheitstechnischen Herausforderungen bei der Übertragung von Sensordaten im Rahmen von drahtloser Kommunikation zu begegnen, ist gerade beim Einsatz von Io(M)T „im Feld“ der Anteil des nicht-leitungsbasierten Datenaustausches so gering wie möglich zu halten. Daher sind Konzepte wie Edge-Processing kombiniert mit Retrofitting Lösungsmöglichkeiten, um auch im Feldeinsatz komplexe, digitale Prozesse in Kombination mit alten Komponenten und Technologien zu ermöglichen. Am Beispiel von KI-Ansätzen der steep GmbH wird demonstriert, wie selbst hoch-rechenintensive Operationen in Feldeinsatzszenaren realisiert werden und nicht digital-fähige Technologien und Komponenten in eine allgemeine Digitalisierungsstrategie integriert werden können. Berücksichtigt werden hierbei Anforderungen wie große Datenmengen, Modellaktualisierungen und kurze Reaktionszeiten.

Erhöhung der Flottenverfügbarkeit in einem skalierbaren Betriebsmodell

Florian Dörr, Hewlett-Packard Enterprise
florian.doerr@hpe.com

Die Optimierung von Wartungsintervallen – insbesondere eine vorausschauende Wartung – ist in jeder Industrie eines der wesentlichen Anwendungsfälle im Kontext von IoT. Auch im militärischen Bereich stellt die Erhöhung der Einsatzfähigkeit von militärischen Flotten ein großes Potential dar. Digitale datenbasierte Dienste können einen großen Beitrag dazu zu leisten und Ressourcen optimieren.
Die Herausforderungen, derartige Projekte zu starten und zu skalieren sind jedoch vielfältig: Hohe Erwartungshaltungen an schnelle Ergebnisse, ressourcenintensive Proof-of-Concepts und sich regelmäßig ändernde Anforderungen. Ihre Erfahrung aus abgeschlossenen Projekten haben möglicherweise gezeigt, dass tatsächliche Ergebnisse mit traditionellen Projektansätzen erst spät im Entwicklungsprozess aufgezeigt werden können.
In diesem Vortrag zeigen wir pragmatische Ansätze, um Projekte zur Erhöhung der Flottenverfügbarkeit agil zu starten und zu skalieren. Dabei ist es wichtig, wesentliche Elemente schon in einer frühen Phase eines Projektes zu berücksichtigen, die eine Skalierung der Architektur und des Betriebsmodells im Hinblick auf Datenaufkommen, Anwendungsfälle und Geografie ermöglichen. Gleichzeitig muss hoher Anspruch an Sicherheit und Datensouveränität für militärische Daten berücksichtigt werden. Angereichert wird der Vortrag mit relevanten Anwendungsfällen und Technologieansätzen aus anderen Industrien.

IoT in Desaster Recovery-Szenarien

Manas Pradhan, Fraunhofer FKIE
manas.pradhan@fkie.fraunhofer.de

Desaster Recovery Operationen stellen hohe Anforderungen an alle Beteiligten, einschließlich der lokalen und internationalen Notfallhelfer, Nichtregierungsorganisationen und des Militärs. Unmittelbar nach einer Katastrophe ist eines der dringendsten Erfordernisse ein Situationsbewusstsein, damit die Ressourcen, einschließlich Personal und Hilfsgüter, priorisiert werden können, um die größte Wirkung zu erzielen und den Bedürftigsten zu helfen.
Während die Wiederaufbaumaßnahmen fortgesetzt werden, muss die Lage aufgrund der sich ändernden Bedingungen in den betroffenen Gebieten ständig aktualisiert werden. Es gibt hierzu viele Informationsquellen, darunter Berichte der Opfer sowie Beobachtungen der Einsatzkräfte. Das Lagebewusstsein kann durch Informationen aus Geräten des Internet of Things (IoT) erheblich verbessert werden, insbesondere in urbanen und zukünftigen Smart City-Umgebungen. Dieser Vortrag gibt einen Einblick in die Nutzung von IoT-Fähigkeiten zur Unterstützung von Disaster Recovery-Operationen, die gewonnenen Erkenntnisse und die entwickelten Konzepte.

Der Beitrag von IoT zur Sicherheit von Großveranstaltungen

Dr. Markus Eisenhauer, Luxembourg Institute of Science and Technology
markus.eisenhauer@gmx.net

Der Vortrag basiert auf den Erfahrungen aus dem von der EU im Rahmen eines mit 100 Mio Euro unterstützten Rahmenprogramms für großangelegte IoT-Piloten durchgeführten Projekts MONICA (»Management Of Networked IoT Wearables – Very Large Scale Demonstration of Cultural and Security Applications«), Large-scale IoT Pilot und weiteren passenden Projekten des Luxemburg Institutes of Science and Technology (LIST) zum Einsatz von IoT für Großschadensfälle. Es wird der Einsatz von robusten IoT-Technologien in Interaktion mit den Einsatzkräften in Echtzeit erläutert. Hierbei geht es nicht um die Ersetzung bestehender Sicherheitskonzepte, sondern um deren sinnvolle Ergänzung mittels neuer IoT Technologien.

Elektronische Textilien – Ein technologischer Überblick und potenzielle Anwendungsmöglichkeiten beim Militär

Malte von Krshiwoblozki, Fraunhofer IZM
Malte.von.Krshiwoblozki@izm.fraunhofer.de

Der Vortrag widmet sich folgenden Fragestellungen:

- Was sind elektronische Textilien?
- Worin bestehen die Herausforderungen bei der Entwicklung und der Industrialisierung dieser?
- Welche potenziellen Anwendungsfelder von E-Textiles spannen sich für das Militär auf?