

Arbeitsgruppe 2

Digitale Infrastrukturen als Enabler
für innovative Anwendungen

UAG Plattformen

Ergebnisbericht 2013

M2M Initiative Deutschland

Inhalt

1	Einleitung	3
2	M2M-Geschäftsmodelle unter Betrachtung der Schichtung im M2M-Eco-System (Market Layer Model)	4
2.1	Fernüberwachung und nutzungsbasierte Abrechnung als Beispiele für die Erschließung neuer Möglichkeiten für Geschäftsprozesse	6
3	Realisierungen	9
3.1	Architekturmodelle, typische Funktionen und deren Rollen	9
3.2	Geräteebene	9
3.3	Netzebene.....	11
3.3.1	LAN: Lokale Netze	11
3.3.2	WAN: Internet	11
3.3.3	WAN: Mobilfunknetze	11
3.4	Anwendungsstruktur.....	12
3.4.1	Vertikale vs. horizontale Struktur.....	12
3.4.2	Struktur der unterstützenden Anwendungen	12
3.4.3	Kommunikationsstruktur	12
3.5	Datenverarbeitung.....	13
3.6	Protokollstruktur.....	14
3.7	Vertrauen und Sicherheit	15
3.8	Zusammenfassung: Current Best Practices	17
4	M2M-Fallbeispiele	18
4.1	Fernzugriff und Fernsteuerung für Blockheizkraftwerke (BHKWs)	18
4.2	Wasserwirtschaft.....	19
4.3	Energiewirtschaft.....	20
4.4	Real Time Cargo Monitoring End-to-End Solution.....	21
4.5	Interaktion mit Maschinen, M2M als soziale Kommunikation	22
4.6	Telemetrie gewerblicher Kaffeemaschinen.....	24
4.7	Frühwarnsystem	25
4.8	Call a Bike	26
4.9	Smart Vending mit Internet-Bezahldiensten	27
5	Handlungsempfehlungen.....	28
5.1	Monitoringsystem für die M2M-Cybersicherheit (M2M-CERT)	28
5.2	Durchgängig verfügbare Mobilfunknetze für M2M-Anwendungen.....	29
5.3	Verstärkte Nutzung von M2M-Experimentier-Kits an Schulen und Hochschulen mit Industrieunterstützung	29
5.4	Förderung von M2M-Lösungen für den Mittelstand.....	29
5.5	Förderung der Ausbildung für verteilte eingebettete Systeme.....	30

1 Einleitung

Durch die immens gestiegenen technischen Möglichkeiten und die zunehmend flächendeckende Bereitstellung von Kommunikationsnetzen hat sich in den letzten Jahren der Bereich der Machine-to-Machine-Kommunikation (M2M) zu einem wichtigen Zukunftsfeld entwickelt. Die Bereitstellung heterogener Kommunikationsmöglichkeiten und vielfältiger Geräteeinbindungen bietet nicht nur Einsparungspotenzial in bestehenden Prozessen, sondern eröffnet gänzlich neue Geschäftsfelder, deren Wertschöpfung auf neuen Anwendungen beruht.

Dieser Markt ist nach heutigen Schätzungen gekennzeichnet durch einen etwa 80%igen Preisverfall bei eingebetteten Systemen über den Zeitraum der letzten fünf Jahre. Diese eingebetteten Systeme stellen oft die Schnittstellen zwischen Geräten, Sensoren, Dingen oder auch Personen und Firmennetzwerken oder auch dem Internet dar, wie es bereits in der Vision des Internets der Dinge aufgezeigt wurde. Die Economist Intelligence Unit (EIU) [1] erwartet auch nicht zuletzt dadurch den Anschluss von 12 bis 15 Milliarden zusätzlichen Geräten an das Internet bis 2020, ohne die Anrechnung von Mobilfunktelefonen und Smartphones. Auch Gartner [1] prognostiziert eine 40–50%ige Wachstumsrate für den M2M-Markt bis 2020. Derzeit ist dieser Markt noch stark fragmentiert und eine Vielzahl von speziellen Applikationen wird für verschiedenste vertikale industrielle Anwendungen einzeln entwickelt – wie beispielsweise in Transport, Logistik, Automobilindustrie oder auch Gesundheitswesen. Die Hauptbestandteile dieser Lösungen weisen jedoch starke Gemeinsamkeiten auf, die es herauszulösen und als industrieübergreifende Anwendungskomponenten universal bereitzustellen gilt. Erst dann kann in diesem Bereich die volle Marktbreite erschlossen werden, ohne bei jedem Einzelprojekt wiederholt hohe Anlaufinvestitionen aufbringen zu müssen.

Dieses Dokument zeigt die verschiedenen Geschäftsmodelle auf, die mit der Anwendung von M2M-Technologien einhergehen. Es beleuchtet Herausforderungen und Risiken und wendet sich dann einer ganzen Reihe von bereits jetzt etablierten Fallstudien zu. Diese sind in den verschiedensten Wirtschaftszweigen der heutigen Industrielandschaft in Deutschland angesiedelt. Die aufgeführten Anwendungen reichen von vernetzten Heizkraftwerken bis zur Kaffeemaschine und zeigen bereits heute die enorme Breite der Einsatzmöglichkeiten.

Das Dokument schließt mit konkreten Handlungsempfehlungen für den Standort Deutschland auf technischer, gesellschaftlicher und rechtlich-regulatorischer Ebene.

2 M2M-Geschäftsmodelle unter Betrachtung der Schichtung im M2M-Eco-System (Market Layer Model)

Das M2M-Eco-System setzt sich aus mehreren Schichten zusammen, die durch bereits existierende Marktteilnehmer (Netzbetreiber), aber auch neue Player (M2M Service Enabler) besetzt werden (siehe Abbildung 1). Die Steuerung und Datenerfassung der Maschinen erfolgt über Devices der Sensor & Chipset Supplier (Anbieter), die entweder das M2M-Access-Modul direkt integriert haben oder über ein lokales Gateway (z.B. DSL oder Mobile Router) der klassischen Telco Device Supplier (Anbieter) aggregiert werden. Das Gateway stellt dann den Access zur Verfügung und führt eventuell Anwendungen (lokale Intelligenz) zur Vorverarbeitung der Daten oder Autonomie der Anwendungen aus (Smart Device).

Der M2M Connectivity Service Provider (Carrier) stellt die Anbindung über ein Mobilfunk- oder Festnetz zur Verfügung. Bei heutigen vertikal integrierten Lösungen erfolgt die Verarbeitung der Daten sowie die Verwaltung der Devices über proprietäre Plattformen, die von segmentspezifischen M2M-Diensteanbietern

bereitgestellt werden. Hier steht eine tiefe und sehr spezifische Integration im Vordergrund.

Die enorme Anzahl der zukünftigen vernetzten Devices und vielfältigen Anwendungen verlangt jedoch nach horizontal integrierten Lösungen, die generische Funktionalitäten effizient übernehmen, Standard-Schnittstellen nutzen und Anwendungen managen.

Der M2M Service Enabler übernimmt diese Aufgaben, d.h. den Betrieb der Gateways und Devices, das Management der Nutzdaten sowie die Verwaltung der Anwendungen.

Der Application Service Provider nutzt diese Daten und den Fernzugriff auf die Maschinen für die Optimierung bestehender Geschäftsprozesse und die Einführung von neuen Geschäftsmodellen. Der Solution Integrator integriert die Lösung über die einzelnen Schichten. Hier ist Ende-zu-Ende-Know-how gefragt, angefangen vom Anwendungsfall bis hin zur Sensor-Technik.

Layer	Technology	Role	Player
Internet of Things	Cloud	- Overlapping Business Processes / Mashups	OTT Service Provider
Business Process	Business Logic	- Business Rules - Data Semantic & Analytics - Application Development & Management - Device Management	Application Service Provider
Operation	M2M Platform	- Data Reporting, APIs - Data Collection & Monitoring - Gateway Management - Security	M2M Service Enabler
WAN	Mobile- / Fixed Network	- Provisioning, Charging - SIM Card Management - Connectivity, QoS	M2M Connectivity Service Provider
LAN „Smart Device“	Gateway	- Access - App Execution & Data Pre-processing - Device Aggregation	Telco Device Supplier
Machine	Device	- Functions - Data Source & Target	Sensor- & Chipset Supplier

Note: A dashed box on the left side of the table groups the layers from 'LAN' to 'Machine' under the label 'Intra-Net of Things'. A vertical box on the right side groups the 'Application Service Provider', 'M2M Service Enabler', and 'M2M Connectivity Service Provider' under the label 'Solution Integrator'.

Abbildung 1: M2M-Eco-System
Quelle: in Anlehnung an urbato, 2013

Diese Anwendungen sind jedoch oft in sich geschlossen und verdienen daher eher den Namen „Intranet of Things“. In der obersten Schicht werden Daten marktsegmentübergreifend von Over-The-Top-Service-Providern genutzt, um damit neue Mashup-Dienste und Geschäftsmodelle, wie z.B. intermodale Mobilitäts-Dienstleistungen anzubieten. Hier sind wir im Internet of Things angekommen.

Bei dem oben genannten M2M-Eco-System ist noch zu erwähnen, dass nicht alle Schichten für eine Anwendung besetzt sein müssen, sondern dass es sich um eine Modularität handelt, welche von Fall zu Fall unterschiedliche Marktteilnehmer beinhaltet. So ist oft das Gateway in Industrielösungen vorhanden, aber nicht in Consumer-Lösungen, wo ein M2M-Device oft direkt an eine Cloud-Lösung angebunden wird.

Grundsätzlich lassen sich M2M-Geschäftsmodelle aus verschiedenen Perspektiven betrachten, der Perspektive der M2M Service Provider und der der Anwender. Beispielhafte Anwender-Geschäftsmodell-Konzepte werden im folgenden Kapitel beschrieben und anhand der Fallbeispiele in Kapitel 4 verdeutlicht.

Die M2M-Service-Provider-Geschäftsmodelle können in folgende drei Modelle gegliedert werden (siehe Abbildung 2). Beim Carrier Business Model bieten die Netzbetreiber über die reine Konnektivität zusammen mit Lösungsanbietern am Markt M2M-Anwendungen an.

Unternehmen mit einer sehr großen Anzahl von eigenen Maschinen oder Sensoren und Aktoren sehen diese Rolle als ureigen an und bauen und betreiben ihre Plattformen daher selbst (User Business Model).

Neue, meist segmentspezifische Dienste-Anbieter (M2M Service Enabler und Application Service Provider) bieten netzbetreiberunabhängig das Management der Devices, Datendienste und Anwendungen an (Service Provider Business Model). Diese sind durch die Spezialisierung auf Segmente meist vom Gateway bis hin zur Plattform vorintegriert. Ebenso entstehen am Markt M2M Service Provider, die eine generische Plattform für alle M2M-Segmente anbieten. Hier steht die einfache Integration der Devices und schnelle Implementierung von simplen Anwendungsfällen im Vordergrund.

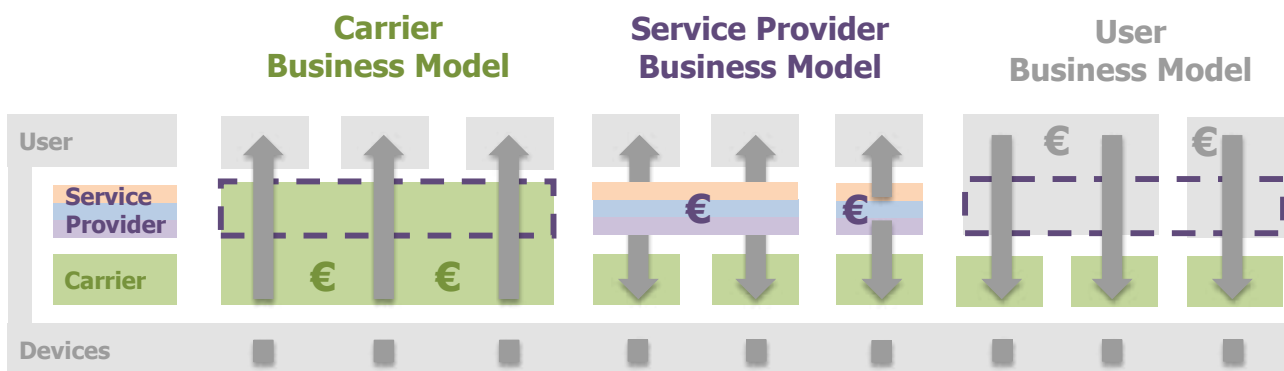


Abbildung 2: M2M-Service-Provider-Geschäftsmodelle
Quelle: urbato, 2013

2.1 Fernüberwachung und nutzungs- basierte Abrechnung als Beispiele für die Erschließung neuer Möglich- keiten für Geschäftsprozesse

Wie in Abbildung 3 dargestellt, überspannt der Grad der Ausprägung von M2M-Anwendungen einen weiten Rahmen, der von einem reinen Erfassen und Auswerten von Betriebsgrößen über die gezielte Einflussnahme auf Prozesse sowie die Auslösung und Parametrisierung betriebswirtschaftlicher Prozesse bis zur Erschließung neuer, attraktiver Anwender-Geschäftsmodelle reicht.

Attraktive und sowohl aus technischer als auch betriebswirtschaftlicher Sicht anspruchsvolle M2M-Fallbeispiele gibt es im nachfolgend beschriebenen Bereich des Remote Monitoring sowie der nutzungs-basierten Abrechnung. Bei den Beispielen werden mit Sensoren ausgestattete technische Geräte oder Anlagen über eine M2M-Konnektivätslösung zur Datenspeicherung und -auswertung angebunden. Dies erlaubt

1. die Überwachung des korrekten Betriebsverhaltens und die Erkennung von Abweichungen, auf die geeignet reagiert werden kann,
2. die kontinuierliche Auswertung von Prozessparametern und eine nachgelagerte Analyse, durch die Prozesse besser verstanden und möglicherweise in diesen vorhandene Reserven erkannt werden können,
3. eine auf in Echtzeit vorliegende Prozessdaten abgestützte Entscheidungsfindung zur fallbezogenen oder auch prediktiven Wartung,
4. die Sicherstellung der Einhaltung von Vorgaben zur Betriebssicherheit und zum Umweltschutz,
5. einen energie- und ressourcenschonenden Betrieb sowie
6. ein Qualitäts- und Compliance-Management.

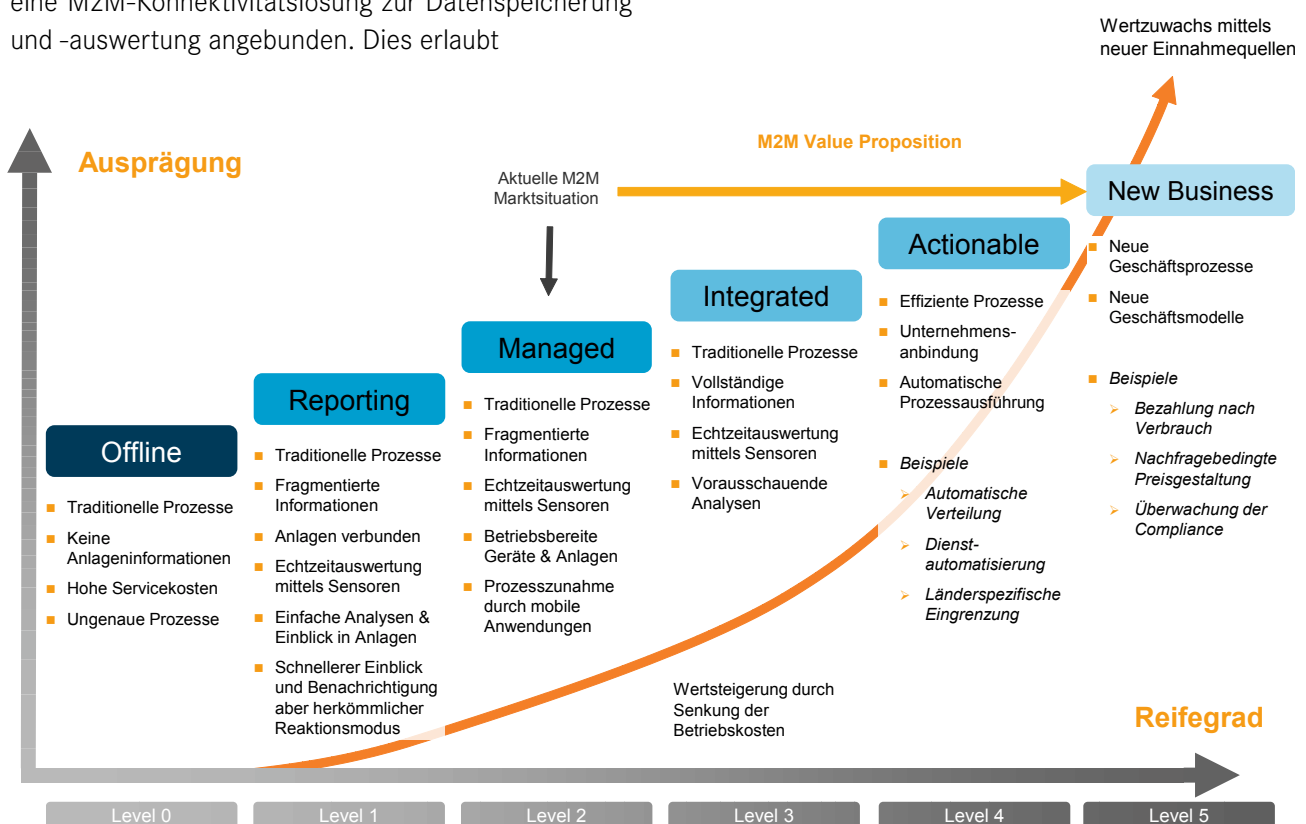


Abbildung 3: Grad der Ausprägung von M2M-Anwendungen
- M2M Maturity Model
Quelle: SAP, 2013

Ein solches Remote-Monitoring ist oft Teil einer umfassenden Remote-Service-Management-Lösung. Die nachfolgende Auflistung zeigt, dass sowohl hinsichtlich der beteiligten Beitragenden als auch der Deployment-Szenarien ein breiter Raum überspannt wird. So kann unterschieden werden bezüglich:

- beteiligter Partner
 - Lösungen im Rahmen eines einzelnen Partners, der sowohl für den zu überwachenden Prozess als auch für dessen Überwachung und die Auslösung nachgelagerter Aktivitäten verantwortlich ist,
 - Lösungen mit einem Dienstleister, der für den Prozessbetreiber die M2M-Anbindung und (Teile der) Auswertung übernimmt,
 - Lösungen mit mehr als zwei beteiligten Partnern wie z. B. dem Betreiber des Prozesses, dem Anbieter der dazu primär eingesetzten Komponenten (z. B. ein Anbieter von technischem Equipment) und einem zusätzlichen Partner, der die M2M-Anbindung, Analysen und die nachgelagerte Auslösung von Prozessen (wie z. B. Bestellungen oder Rechnungslegungen) übernimmt. Bei den beiden zuvor benannten Szenarien verschmelzen Anteile bei dem einen oder den beiden beteiligten Partnern.

- Deployment-Szenarien
 - On-Premise-Szenarien,
 - Cloud-basierte On-Demand-Szenarien,
 - Hybrid-Szenarien mit einer Kombination von On-Premise und Cloud-basierten On-Demand-Anteilen.

Abbildung 4 zeigt, dass über den gesamten Lebenszyklus (von der Entwicklung über die Inbetriebnahme bis zum kontinuierlichen Betrieb) von Lösungen überspannende Interaktionen zwischen unterschiedlichen Beteiligten möglich sind. Diese sind in ihrem Wesen auch charakteristisch für den aktuell mit großem Interesse betrachteten Ansatz der Industrie 4.0.

Technische Lösungen mit ihren Komponenten und Möglichkeiten müssen diesen heterogenen möglichen Einsatzszenarien geeignet Rechnung tragen. Dabei ergibt sich speziell ein großes Potenzial für Plattform-Lösungen, die unter Nutzung wiederverwendbarer Teile vielseitig ausgeprägt und angepasst werden und dabei ein attraktives Preis-Leistungs-Verhältnis sicherstellen können.

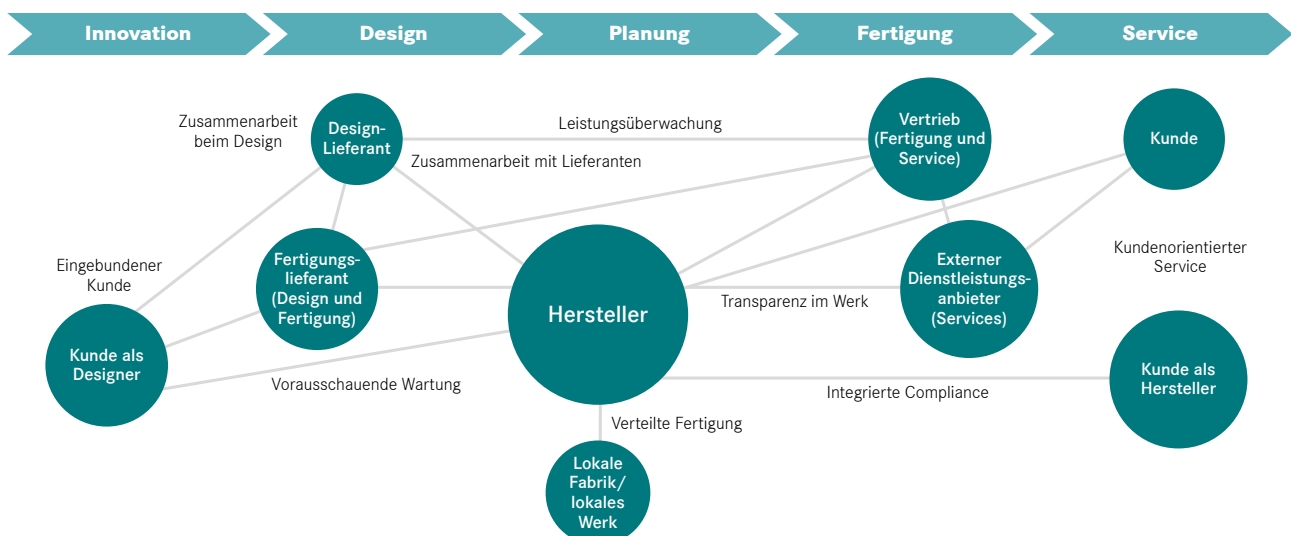


Abbildung 4: Lebenszyklus technischer M2M Lösungen
Quelle: in Anlehnung an SAP, 2013

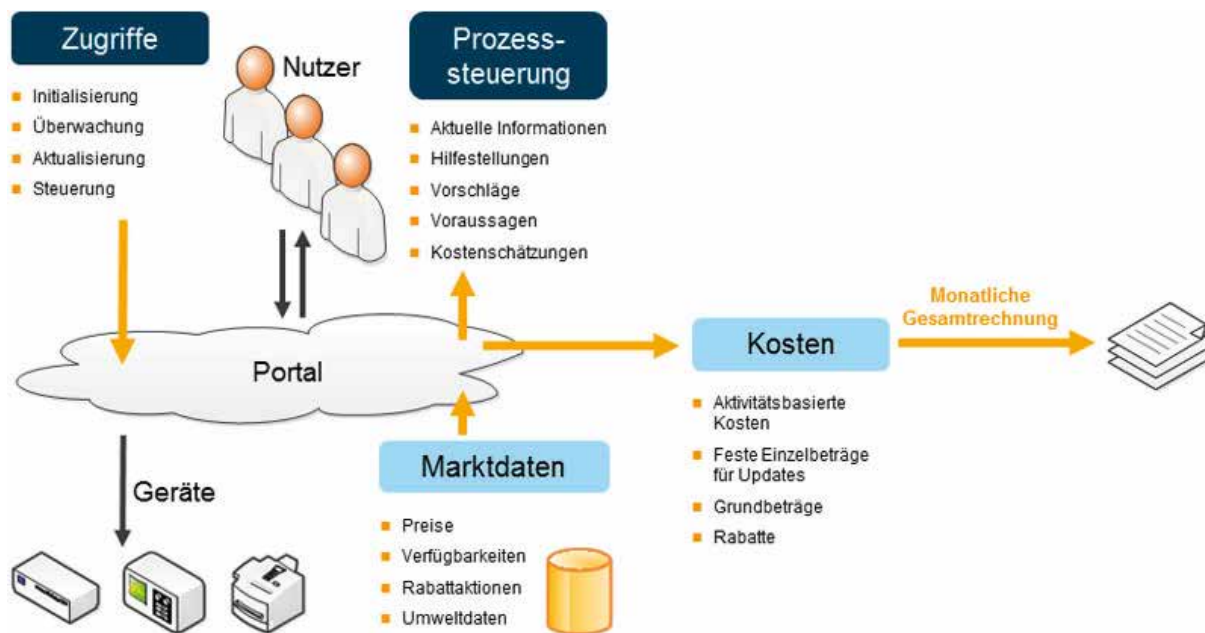


Abbildung 5: Übersichtsbild nutzungs-basierte Abrechnung
Quelle: SAP, 2013

Eine spezielle Ausprägung der so beschriebenen Szenarien stellt die nutzungs-basierte Abrechnung dar. Bei dieser werden Betriebsparameter erfasst und ausgewertet, um auf dieser Basis statt einer „flachen“ Abrechnung nutzungs- und verbrauchs- oder verschleißbasierte Abrechnungsmodelle umzusetzen (siehe Abbildung 5).

Eine zeitnahe und gegebenenfalls mit weiteren Informationen (z. B. aktuelles Energie-Angebot und Preis) verknüpfte Auswertung und Prozesssteuerung erlaubt es, dem Betreiber der Prozesse Kosten zu sparen und z. B. in vielen Fällen auch Umwelt- oder Emissions-Auflagen besser gerecht zu werden. Nicht zuletzt sind auch Umsetzungen denkbar und werden aktuell mit Partnern betrachtet und realisiert, bei denen eine Aufteilung der initial oder auch kontinuierlich für die Lösung entstehenden Kosten, aber auch der Einsparungen und Gewinne zwischen den beteiligten Partnern erfolgt. Dies hat einen unmittelbaren Bezug zu den im Dokument bereits betrachteten Geschäftsmodellen.

3 Realisierungen

3.1 Architekturmodelle, typische Funktionen und deren Rollen

Um den im vorherigen Kapitel geschilderten Herausforderungen gerecht zu werden, ist ein Gesamtsystem in Teilfunktionen und Komponenten zu unterteilen, die in Beziehungen zueinander stehen. Diese Unterteilungen und Beziehungen werden insgesamt als Architektur bezeichnet; typische Architekturen werden zu Architekturmodellen zusammengefasst, die Gemeinsamkeiten aufweisen, sich aber in Details unterscheiden können. Wesentliche Gemeinsamkeiten bestehen häufig in typischen Rollen, die von Komponenten der Architektur wahrgenommen werden müssen und die in allen Ausprägungen eines Architekturmodells wiedererkennbar vorkommen.

Ziel dieses Abschnitts ist es, solche Architekturmodelle und Rollen in knapper Zusammenfassung darzustellen und Hinweise auf aktuelle Trends und Entwicklungen zu liefern. Hierzu werden wir M2M-Systeme unter folgenden Gesichtspunkten betrachten: die Ebene des einzelnen Gerätes, die Ebene der Vernetzungstechnik an sich, die Ebene der Anwendungsstruktur, eng damit verbunden die Ebene der Kommunikation und der zugehörigen Protokolle einerseits, die Ebene der Datenverarbeitung andererseits, und letztlich die Sicherheitsebene.

Die einzelnen Ebenen sowie deren Komponenten und Beziehungen sind in Abbildung 6 dargestellt.

3.2 Geräteebene

Die Möglichkeit, einzelne Geräte in ein M2M-System einzubinden, wurde bereits im letztjährigen Bericht aufgezeigt. Derzeit sind drei aktuelle Entwicklungen interessant:

- Bisher wurde häufig der Ansatz verfolgt, eine Maschine durch ein einzelnes Gerät (Bord-Rechner, Telemetrie-Modul) in ein M2M-System einzubinden und von diesem Gerät aus diese Maschine zu steuern. In letzter Zeit ist vermehrt zu beobachten, dass eine einzelne Maschine mehrere Geräte aufweist, die jeweils separaten Zwecken dienen und die Maschine unter unterschiedlichen Aspekten in der IT-Welt repräsentieren und eventuell mehrere IP-Adressen benutzen. Dies hat Konsequenzen sowohl für die Datenverarbeitung innerhalb der Maschine als auch für die M2M-Infrastruktur als Ganzes, die ggf. die Zusammengehörigkeit dieser M2M-Geräte repräsentieren muss.
- Aus der Do-It-Yourself-Gemeinde hat sich die Bewegung der Maker Faires entwickelt, die ein erstaunliches Kreativitätspotenzial freigesetzt hat. Der M2M-Aspekt solcher Systeme wurde durch die einfache Verfügbarkeit von einbettbaren, gut programmierbaren, günstigen Systemen wie Arduino oder Raspberry Pi befeuert. Es bleibt hier zu beobachten, wie und ob sich diese Initiativen verselbstständigen und sich ggf. hieraus De-facto-Standards entwickeln oder ob sich allgemein anerkannte Standards (beispielsweise durch die IETF) durchsetzen werden. Solche De-facto-Standards können schnell in die Hochschul-ausbildung eindringen und damit die Fachkräfte der Zukunft beeinflussen. Dies kann unmittelbare Auswirkungen auf Innovationsprozesse in wesentlichen Wirtschaftsbereichen haben.
- Bisher wurde die M2M-Fähigkeit einer Maschine in vielen Fällen nachträglich durch Einbau von M2M-Geräten nachgerüstet. In letzter Zeit gibt es immer mehr Maschinen, die schon vom Maschinenhersteller mit M2M-Fähigkeiten ausgestattet werden. Dabei wird das in der Maschine vorhandene eingebettete IT-System um die Möglichkeit erweitert, mit dem Internet zu kommunizieren. Beispiele sind moderne Verkaufsautomaten oder Autos. Dies führt zu einer Änderung der Wertschöpfungskette und der Art, wie M2M-Datenverarbeitungssysteme benutzt werden.

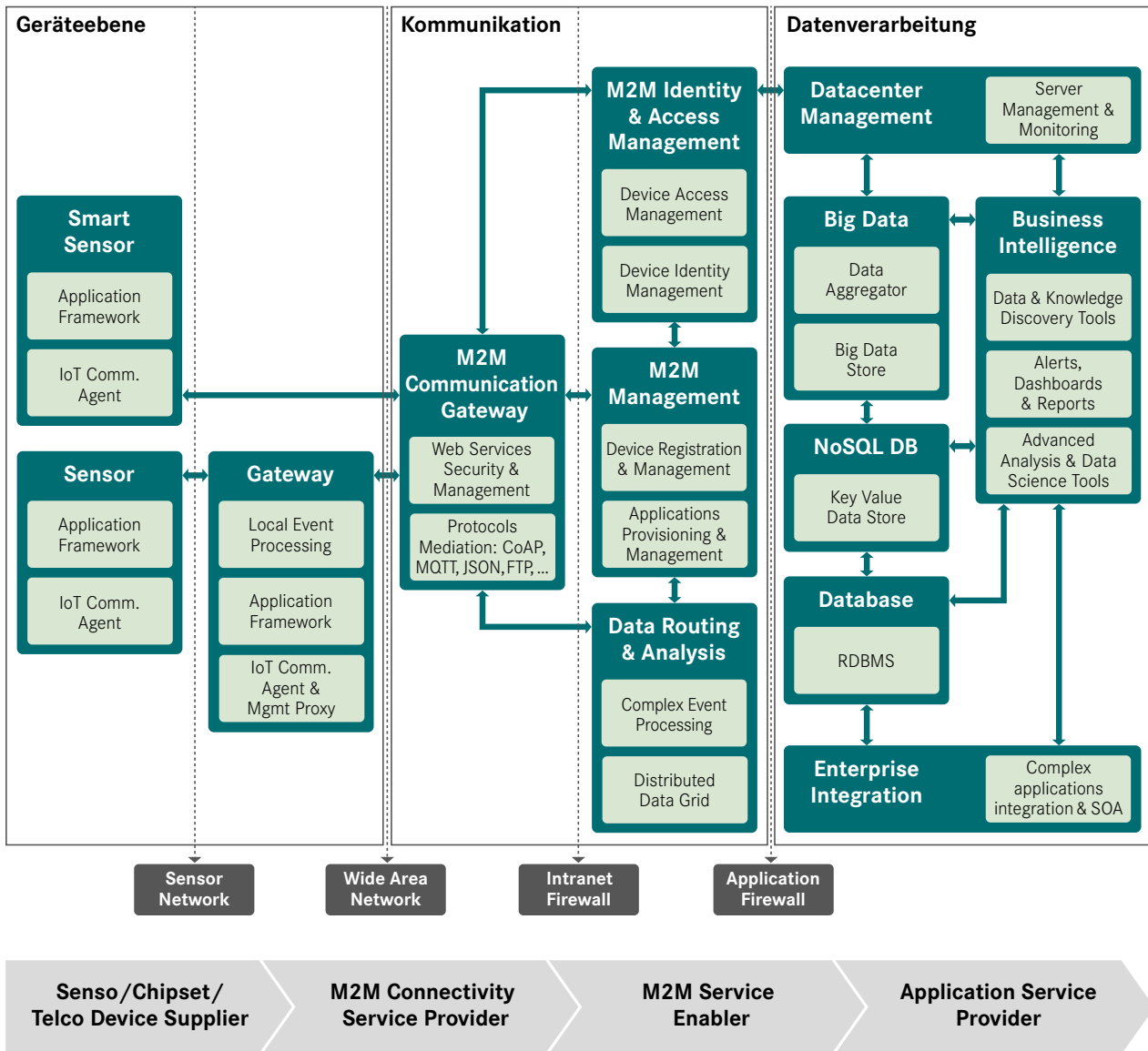


Abbildung 6: Übersicht der Komponenten und Beziehungen einer M2M-Referenz-Architektur
Im linken Teil sind die M2M-Devices bzw. M2M-Geräte (Sensoren, Aktuatoren, Sensor- und Feldbus-Gateways usw.) und das M2M-Gateway zu finden. Rechts davon ist die Cloud-Umgebung – also der Backend-Server – dargestellt. Das M2M-Gateway ist per Internet mit dem Backend-Server gekoppelt.
Quelle: in Anlehnung an ORACLE, 2013

3.3 Netzebene

3.3.1 LAN: Lokale Netze

Die lokale Vernetzung von Geräten bezeichnet unterschiedliche Systemrealisierungen und unterschiedliche Technologie. Innerhalb einer Fabrik, in der Automatisierung werden hierfür bewährte Feldbus-Systeme eingesetzt. Bei drahtloser Übertragung über kurze Reichweiten spricht man von drahtlosen Sensor-/Aktuatornetzen. Je nach konkreter Technologie stellen sich hier unterschiedliche Integrationsaufgaben – in vorhandene Standards wie in neu zu entwickelnde Systeme – für M2M-Systeme; die Alternative einer separaten Vernetzung kann strukturell einfacher, aber finanziell aufwendiger sein.

Derzeit sind die wesentlichen Herausforderungen auf diesem Gebiet eben diese Integration wie auch die Sicherheit, Planbarkeit und Durchgängigkeit einer solchen Netzinfrastruktur. Es gibt hierfür derzeit lediglich Einzellösungen; ein durchgängiges Konzept, obwohl sehr wünschenswert, liegt nicht vor – hier besteht Handlungsbedarf.

3.3.2 WAN: Internet

Solange ein M2M-Gerät nur in einem lokalen Kontext kommunizieren soll, wird eine Weitverkehrsverbindung nicht benötigt. Andernfalls kann eine solche Verbindung bereits über eine lokale Vernetzung vorliegen (beispielsweise bei Integration in eine Feldbus-Struktur mit geeigneten Gateways). Falls dies nicht der Fall ist, wird es notwendig, dass ein M2M-Gerät direkt mit dem Internet kommunizieren kann. Dies ist beispielsweise erforderlich, wenn die vom Gerät erfassten Daten in einer Cloud verarbeitet werden sollen.

In einfachen Fällen mag hier ein üblicher Internet-Zugang ausreichend sein – hierfür sind dann Standards zur Provisionierung und Konfiguration solcher Geräte zu schaffen und geeignete Konventionen und Best Practices für Sicherheit und Zugang (Authentisierung, Autorisierung) sind dringend wünschenswert.

In komplexeren Fällen mag dies nicht hinreichend sein. Dies ist insbesondere dann der Fall, wenn das M2M-Gerät Teil einer kritischen Infrastruktur ist (siehe die Beispiele im Kapitel 4 zu Verkehr/Telematik oder Wasserterversorgung). Ggf. wird hier eine bessere Dienstgüte – insbesondere höhere Verlässlichkeit, ggf. auch niedrigere Verzögerungen – erforderlich, als dies durch das übliche Internet geboten werden kann. Denkbare Ansätze wären die Schaffung von „Overlays“ über das existierende Internet, die mit entsprechenden Eigenschaften ausgestattet sind und deren Zugang kontrolliert werden kann – hier der Zugang für entsprechende M2M-Systeme. Allerdings ist das Schaffen solcher Overlays mit Dienstgütegarantien derzeit noch ebenso Forschungsgegenstand wie die dafür notwendigen Schnittstellen zur Einrichtung oder zum Beitritt zu einem solchen Overlay. Weiterhin ist zu klären, wie dies mit den Fragestellungen zur Netzneutralität interagiert.

Hier besteht offenbar Handlungsbedarf, wenn M2M – über eine „Best effort“-Lösung hinausgehend – Bestandteil von verlässlichen, kritischen Infrastrukturen werden soll.

3.3.3 WAN: Mobilfunknetze

Soll ein M2M-Gerät über ein Mobilfunknetz mit dem Internet kommunizieren, so gilt oben Gesagtes ebenfalls, allerdings in verschärfter Form, da die verfügbare Bandbreite zwischen vielen teilnehmenden Endgeräten geteilt werden muss. Viele Details dieses Szenarios wurden bereits im Dokument des Vorjahres diskutiert (Anforderungen an SIM-Karten, Tarifmodelle, die für Datenverkehr geeignet sind, auf M2M spezialisierte MVNOs, ...) und gelten im Wesentlichen unverändert fort. Auch im Kontext der Mobilfunknetze stellen sich die oben für allgemeine Weitverkehrsnetze genannten Herausforderungen weiterhin.

3.4 Anwendungsstruktur

Unabhängig von der Art der eingesetzten Geräte und der benutzten Netzstruktur ist die Frage der Anwendungsstruktur zu betrachten. Dies betrifft zunächst die Softwarearchitektur allgemein. In den folgenden Abschnitten werden (a) die Strukturierung der Kommunikationsbeziehung der verteilten Komponenten eines M2M-Systems, (b) die eingesetzten Protokolle, (c) die Strukturierung der Datenverarbeitung und (d) Sicherheitsaspekte im Detail betrachtet.

3.4.1 Vertikale vs. horizontale Struktur

Eine grundsätzliche Überlegung bei der Anwendungsstruktur betrifft die Partitionierung in Teilfunktionen und die Wiederverwendbarkeit. Eine mögliche Struktur ist dabei die sogenannte vertikale Partitionierung: Einzelne Teilmärkte, ggf. auch nur einzelne Anbieter, schaffen sich eigene technische Lösungen, die von und nach außen abgeschottet sind. Man spricht hier dementsprechend auch von vertikalen Silos. Solche Lösungen versprechen zwar kurzfristige Vorteile (beispielsweise bessere Kontrolle über eine Gesamtlösung); langfristig ist allerdings fraglich, ob hier nicht sowohl technische Möglichkeiten übersehen als auch Geschäftsmodelle verhindert werden.

Die technische Alternative ist eine horizontale Struktur, bei der technische Teilfunktionen über Branchen und Anwendungen hinweg zur Verfügung gestellt werden und dann von unterschiedlichen Anwendungen wiederverwendet werden können. Das Internet ist dabei das typische Beispiel für eine horizontale Infrastruktur: es ist transparent gegenüber der jeweiligen Anwendung. Durch die geschickte Wahl des bereitgestellten Dienstes ist das Internet für eine große Menge unterschiedlicher Anwendungen und Geschäftsmodelle zur wesentlichen Infrastruktur (und zum „Enabler“) geworden.

In solchen horizontalen Modellen ist die Wiederverwendung von Daten wie Funktionen erheblich vereinfacht und schafft Folgeinnovationen. Zusätzlich entsteht dadurch die Möglichkeit der einfachen logischen Vernetzung und weiteren Wertschöpfung – erste Modelle hierzu entstehen derzeit („M2M Mashups“

und das dazugehörige sogenannte „Plumbing“, siehe z. B. IFTTT und SmartThings Channel, <https://ifttt.com/smartthings>). Eine entsprechende Entwicklung gibt es in vertikalen Silos nicht.

Für M2M-Systeme beginnt sich diese horizontale Referenzarchitektur (als Pendant zum Internet) nur langsam herauszubilden. Hier besteht weiterer Handlungsbedarf.

3.4.2 Struktur der unterstützenden Anwendungen

M2M-Geräte kommunizieren mit M2M-Anwendungen auf einem Server. Es ist eine offene Frage, welcher Standard sich in diesem Bereich etablieren wird.

Dies bezieht sich auf mehrere Aspekte: Welches Deployment-Modell wird sich durchsetzen, ein Cloud-Modell (Platform as a Service) oder weiterhin eigenständige aufgebaute und betreute Rechner? Welche Funktionen der Service-Enabler-Ebene (siehe Abbildung 2.2-6) werden sich tatsächlich als Standard durchsetzen? Wird auf bekannte und bewährte Anwendungsserver zurückgegriffen oder lohnt es sich, spezialisierte M2M-Anwendungsserver zu schaffen? In jedem Fall fehlen hier Erfahrungen und Best Practices in größerem Maßstab, die es erlauben würden, nicht nur eine Referenzarchitektur, sondern auch einfache Referenzlösungen zu nutzen. Wir brauchen einen Standardbaukasten in Analogie zur allgemeinen LAMP-Lösung (Linux/Apache/MySQL/PHP) der Web-Anwendungen.

3.4.3 Kommunikationsstruktur

Eng verbunden mit der Frage der Anwendungsstruktur ist die Frage nach der Kommunikationsstruktur. Insbesondere ist hier wichtig, welches Gerät (präziser: welche Rolle) eine Kommunikation initiieren darf und welches in der Lage sein muss, solche Initiierungen entgegenzunehmen.

Eine flexible Möglichkeit ist, dies allen Geräten zu erlauben. Das lässt großen Spielraum, kann aber Konsequenzen für Sicherheitsanforderungen und Komplexität der Implementierung haben.

In klar definierten Szenarien kann es daher sinnvoller sein, die Aufgaben und Fertigkeiten der entsprechenden Rollen einzuschränken und z. B. einem Gerät nur zu erlauben, eine Kommunikationsverbindung zu initiieren, aber nicht, externe Kommunikationsverbindungen entgegenzunehmen. Dies kann je nach Anwendung wiederum zu Herausforderungen bei der Optimierung führen (z. B. ist eine unregelmäßige Abfrage in solchen Strukturen nur mit Aufwand möglich).

Dies wird insbesondere dann zu einer spannenden Aufgabe, wenn ein Gerät vielen unterschiedlichen Anwendungen zugeordnet ist (im Sinne der Horizontalisierung und bezüglich Geschäftsmodellen der Monetarisierung von Daten), die unterschiedliche Interaktionsmuster verfolgen. Diese Anforderung wird noch verschärft, wenn ein solches Gerät als „Gateway“ zwischen einem Weitverkehrsnetz einerseits und weiteren Geräten andererseits dienen soll. Hier sind keine Lösungen offensichtlich und es besteht Handlungsbedarf.

3.5 Datenverarbeitung

Mit der Interaktionsstruktur der einzelnen Rollen hängt die Struktur der Datenverarbeitung eng zusammen. Hier sind die Fragen des „Wo?“ und des „Wann?“ zu beantworten.

Typischerweise ist ein M2M-Gerät ein Datensammler oder ein Aktuator (oft auch beides). Die gesammelten Daten können lokal verdichtet und aufgearbeitet und ggf. auch schon lokal zur Entscheidungsfindung herangezogen werden (beispielsweise bei einfachen Regelaufgaben). Solchermaßen verdichtete Daten können dann über Weitverkehrsnetze an „Backend“-Server weitergereicht werden oder Anweisungen von dort empfangen. Für die Aufteilung solcher Aufgaben zwischen lokalen Geräten und Backend-Servern gibt es derzeit keine verlässlichen Regeln; vieles wird hier heute nach groben Schätzungen und Erfahrungswissen entschieden. Hier besteht Handlungsbedarf.

Für das Ablegen der Daten in Backend-Servern existieren wiederum viele Möglichkeiten: sei es in klassischen Datenbanken, als unstrukturierte Dateien, oder in sogenannte „NoSQL“-Datenbanken. Je nach Echtzeitanforderungen und Datenaufkommen sind Datenbanken entweder auf externen Speichermedien oder direkt im Arbeitsspeicher (In-Memory-Datenbank) realisierbar. Auch hier gibt es derzeit keine verlässlichen Entscheidungsregeln, welches System für eine bestimmte Anwendung (oder horizontale Schicht) die besten Ergebnisse liefert.

Neben der bloßen Speicherung stellt sich die Frage der Verarbeitung der Daten, insbesondere, wann welche Daten verarbeitet werden sollen. In einfachen Fällen (etwa wenn keine Zeitschranken bestehen) kann dies durch regelmäßige Verarbeitung erfolgen. In anderen Fällen muss auf Ereignisse reagiert werden, wobei das Identifizieren eines Ereignisses selbst eine komplexe Aufgabe sein kann. Hierzu eignen sich dann Systeme des sogenannten Complex Event Processing (CEP). Gerade bei einer Horizontalisierung und Datenmonetarisierung als Geschäftsmodell sind hier noch viele Fragen zu klären, z. B. die, wie CEP-Regeln formuliert werden können, die den Datenbesitz und die Zugriffsrechte respektieren, bei denen aber zusätzliche Regeln einfach eingebracht werden können, um eine weitere Anwendung zu realisieren. Konzeptionell sind hier elegante Lösungen denkbar, bei denen etwa nicht alle Daten in entfernte Clouds transportiert werden müssen, sondern bereits im Netz eine geeignete Aggregationsebene bereitgestellt werden kann (etwa durch sogenannte Network Function Virtualization realisiert). Daraus ließe sich die Vorstellung ableiten, dass an einen Datenfluss zwischen Geräten unterschiedliche Dienste angeschlossen werden können (ein „Service Bus“), die Daten konsumieren und produzieren und an geeigneter Stelle ausgeführt werden können. Die Integration von Aktuatoren in solch eine verteilte Ereignisverarbeitung samt der notwendigen Kontrollfunktionen (never trust an actuator) ist dabei unklar.

3.6 Protokollstruktur

Als letzter Baustein der technischen Umsetzung eines M2M-Systems fehlen noch geeignete Protokollstrukturen, die in unterschiedlichen Netzkontexten unterschiedliche Anwendungsstrukturen miteinander verbinden können. Dabei stehen Effizienzanforderungen (Speicherbedarf, CPU, Nachrichtengröße) häufig Forderungen nach allgemeiner Einsetzbarkeit, Wiederverwendbarkeit und Durchgängigkeit entgegen; weitere Anforderungen sind die Transportierbarkeit der Protokollnachrichten über Weitverkehrsnetze (Eignung für Tunneling oder Firewall-verträglich) und die Möglichkeit, auch Ereignisbenachrichtigung zu unterstützen.

Eine weitere Anforderung ist die Vorwärts- und Rückwärtskompatibilität, um die Lebenszyklen der M2M-Geräte untereinander und von der Server-Anwendung zu entkoppeln.

Kompromisse können hier erforderlich sein. Die folgende Aufzählung nennt entsprechend einige derzeit im Einsatz befindliche, teilweise dediziert für M2M, teilweise für allgemeine Anwendungen entwickelte Protokolle, die zunehmend in einem M2M-Kontext eingesetzt werden. Alle diese Protokolle lassen sich aus Netzsicht der Anwendungsebene zuordnen und sind damit flexibel über unterschiedliche Netztechnologien hinweg einsetzbar.

- Ein häufig eingesetztes Protokoll- und Entwurfsmuster ist der sogenannte **Representational State Transfer (REST)**, bei dem nur einfachste Nachrichten benutzt werden, um mit Informationsobjekten zu kommunizieren. Der Transport von REST-Nachrichten kann beliebig geschehen, verbreitet ist der Transport via HTTP/HTTPS, wodurch die bestehende webbasierte Infrastruktur wiederverwendet werden kann. REST ist heute der De-facto-Standard im Internet und für die Cloud.
- Das **Extensible Messaging and Presence Protocol (XMPP)** wurde für sogenannte Chat-Nachrichten und Anwesenheitsbenachrichtigungen entworfen. Die prinzipielle Ähnlichkeit der Verkehrsmuster mit vielen M2M-Anwendungen macht es auch für M2M attraktiv, zumal recht leichtgewichtige

Implementierungen mit einfacher und dennoch leistungsfähiger Infrastruktur vorliegen. Nicht offenkundig ist die weitergehende Integration in eine größere IT-Infrastruktur, die bei REST einfach gegeben ist.

- Das **Constrained Application Protocol (CoAP)** wurde, im Gegensatz zu den obigen Protokollen, dediziert für M2M- und Internet-of-Things-Szenarien entwickelt und achtet insbesondere auf Ressourceneffizienz. Es ist dazu gedacht, einfach in HTTP übersetzt zu werden (in einem Gateway), statt wie andere Protokolle innerhalb von HTTP transportiert zu werden. Dies kann Auswirkungen z. B. auf Kompatibilität mit bestehenden Firewall-Strukturen haben.
- Ähnlich wie CoAP ist **Message Queuing Telemetry Transport (MQTT)** ein dediziert für M2M-Anwendungen entworfenes Protokoll, das allerdings auf ein sogenanntes Publish/Subscribe-Paradigma ausgerichtet ist. Allerdings fehlt bisher die Unterstützung durch ein Standardisierungsgremium; es wird als De-facto-Industriestandard vorangetrieben. Es ist dazu gedacht, mit einer Web-Infrastruktur interagieren zu können.
- **Openness, Productivity and Collaboration - Unified Architecture (OPC-UA)** ist der Interoperabilitäts-Standard für hersteller- und plattformunabhängige industrielle horizontalen und vertikalen Daten- und Informationsaustausch. Als IEC62541 Norm bietet es Security by Design und die Erweiterung mit Informationsmodellen (und geht damit deutlich über ein bloßes Datenaustausch-Protokoll hinaus). OPC ist der De-facto-Standard in der Automatisierungsbranche – die Dienste sind aber branchenneutral. Er wird auch in Sensor-, Smart-Metering- und Cloud-Szenarien eingesetzt.

Insgesamt steht einem Systemarchitekten damit eine große, ggf. verwirrende Auswahl an Alternativen zur Verfügung. Dies wird noch dadurch erschwert, dass Funktionen, die im Web-Kontext allgemein üblich sind, für M2M-Systeme nicht unmittelbar oder offensichtlich zur Verfügung stehen. Beispiel dafür sind die automatisierte Entdeckung von Geräten oder deren offerierten Datendiensten. Die Analogie zu Web-Service-Beschreibungssprachen wie WSDL bzw. den dazugehörigen Entdeckungsprotokollen (wie UDDI)

drängt sich auf; es ist allerdings fraglich, ob diese Verfahren für einen M2M-Einsatz unmittelbar geeignet sind bzw. wie groß der Modifikationsaufwand ist.

Die Realisierung der Protokollstrukturen eines M2M-Gateways kann auch mit Hilfe einer OSGi-Middleware erfolgen. Wichtiges OSGi-Element ist ein Geräte-Abstraktionslayer, der protokollabhängig gestaltet ist und Protokolleigenheiten der Sensoren/Aktoren (ZigBee, Z-Wave, EnOcean, DECT etc.) gegenüber den Anwendungen in Form von Gerätezustandsobjekten (DCOs) abstrahiert, da diese in der Regel lediglich an Daten (Informationen) interessiert sind. Das geht konform mit entsprechenden Anstrengungen der Standardisierungsorganisationen OneM2M, ETSI, HGI und Broadband Forum.

Auf der Ebene der eigentlichen Anwendungsprotokolle schließlich sind wir weit davon entfernt, allgemein übliche Standards zu besitzen. Dies mag in einigen vertikalen Märkten der Fall und ggf. auch durch eine Standardisierung entstanden sein (beispielsweise der Stromzählermarkt in Deutschland und die Rolle des BSI dabei); für die allgemeine Situation ist dies aber wenig plausibel.

Wir sehen hier Handlungsbedarf im Aufbau besser dokumentierter Best Practices bei der Protokollwahl wie auch bei der Entwicklung fehlender Funktionalität wie etwa Beschreibungs- und Entdeckungsprotokolle.

3.7 Vertrauen und Sicherheit

Im Juni 2013 gab der Whistleblower Edward Snowden bekannt, dass der US-amerikanische Geheimdienst NSA (National Security Agency) und der britische Dienst GCHQ (Government Communications Headquarters) mit Hilfe einer weltweit verteilten Infrastruktur große Teile der Kommunikation auf dieser Erde überwachen. Entsprechend ist es von entscheidender Bedeutung, sowohl technische Lösungen zu finden, die ein M2M-System gegen Angreifer sichern, als auch juristische und geschäftsmodellbezogene Lösungen zu finden, die es erlauben, der technisch ggf. vorhandenen Sicherheit das notwendige Vertrauen

entgegenzubringen. Ersteres ist derzeit teilweise möglich, aber oft nicht praktikabel; Letzteres ist bei den momentanen Rahmenbedingungen (insbesondere juristischen) selbst mit großem Aufwand eine schwierige Aufgabe. Hiervon kann eine substantielle Gefahr für einen bedeutenden Innovationszweig ausgehen. **Bei der Realisierung einer M2M-Anwendung sollten daher die folgenden technischen Aspekte beachtet werden:**

- Das M2M-Gateway selbst und alle Funktionseinheiten einer M2M-Lösung, die sich in der Abbildung 6 links vom diesem Gateway befinden, basieren auf sogenannten Embedded Systemen. Für derartige Rechnerplattformen lässt sich aufgrund der relativ geringen Hard- und Softwareressourcen und weiterer Einschränkungen keine zeitgemäße IT-Sicherheit realisieren.
- Es gibt für solche Mikrorechnersysteme in der Regel keine regelmäßigen Softwareupdates. Teilweise werden erkannte Schwachstellen noch nicht einmal von den Herstellern behoben. Sicherheitslücken existieren daher häufig für die gesamte Produktlebensdauer, die in einigen Fällen mehr als zehn Jahre betragen kann.
- Die zum Einsatz kommenden eingebetteten Betriebssysteme wurden hinsichtlich möglicher Angriffe über die Kommunikationsschnittstellen nicht speziell gehärtet und werden daher zahlreiche Exploits aufweisen.
- Es existiert – falls überhaupt vorhanden – nur eine schwache Authentifizierung für Benutzerzugriffe.
- Obwohl teilweise mehr als eine IP-fähige Kommunikationsschnittstelle vorhanden ist, sind keinerlei Firewall-Funktionen vorgesehen.
- Embedded-System-Plattformen sind in der Regel völlig schutzlos gegen DoS- bzw. DDoS-Angriffe. In sehr vielen Fällen ist während und nach einem solchen Angriff die Primärfunktion – zum Beispiel eine Reglerfunktion – nicht mehr gegeben.
- Der Verbindungsaufbau eines M2M-Gateways zum Internet sollte immer vom Gateway selbst – also von innen nach außen – in die Wege geleitet werden. Die umgekehrte Richtung ist aus Sicherheitsgründen zu vermeiden. Ein Gateway, das auf Verbindungsaufbauversuche aus dem Internet wartet und

über diesen Weg entsprechende Services anbietet, lässt sich nicht gegen externe Angreifer und missbräuchliche Nutzung schützen.

- Ein Angriffsvektor in M2M-Systemen besteht in der Übernahme eines einzelnen M2M-Gerätes, mit dessen Hilfe ein Angreifer Daten fälschen oder in das gesamte M2M-System eindringen kann. Um einem solchen Angriff zu begegnen, sollte jedes M2M-Gerät oder M2M-Gateway individuelle Berechtigungen (Passwort, X.509 Zertifikat) besitzen, die dann im Angriffsfall individuell entzogen werden können. Dies ist heute in vielen Fällen nicht gegeben. Zum effizienten Betrieb bedarf es einer geeigneter Device Identity Management Komponente, wie dies in Abbildung 6 dargestellt ist.
- Wenn auf ein M2M-Gateway vom Internet aus zugegriffen werden muss, dann sollte dieser Zugriff nur innerhalb eines VPN erfolgen.
- Die Embedded-System-Baugruppen im linken Teil der Abbildung 6 werden häufig über einen längeren Zeitraum – teilweise über die gesamte Lebensdauer – mit den Werkseinstellungen betrieben. Dadurch besteht zum einen das Risiko, dass Standard-Passwörter zur Authentifizierung benutzt werden, die in im Internet veröffentlichten Benutzerhandbüchern zu finden sind – ein leichtes Spiel für potenzielle Angreifer. Zum anderen sind über die IP-Schnittstellen der Embedded-Systeme häufig Dienste verfügbar, die in einer Anwendung zwar nicht benötigt werden, aber auch nicht deaktiviert wurden.
- Rechts von der Internet-Firewall in Abbildung 6, also innerhalb einer Cloud-Umgebung, lässt sich aufgrund der Backend-Server-Hard- und Softwarestrukturen eine zeitgemäße IT-Sicherheit mit verschiedenen Firewalls und Zonenkonzepten umsetzen. Die technischen Voraussetzungen dafür sind in der Regel optimal. Rechtlich ist es hingegen etwas komplizierter. Neben der ungeklärten Fragestellung, ob man die Cloud-Dienste für eine bestimmte

M2M-Anwendung auf Servern außerhalb des deutschen oder europäischen Rechtsraums einsetzen darf, muss auf jeden Fall den Sicherheitsprozessen des IT-Infrastrukturbetreibers selbst deutlich mehr Aufmerksamkeit zuteilwerden. Diese Sicherheitsprozesse sollten idealerweise anerkannten internationalen Standards entsprechen. Zu beachten ist auch, dass sich ein Betreiber unter Umständen besonderen gesetzlichen Rahmenbedingungen (z.B. dem USA PATRIOT Act) unterordnen muss, die aus Sicht des M2M-Anwenders als kritisch einzustufen sind.

Wir sehen hier umfassenden, tiefgehenden und dringenden Handlungsbedarf auf vielen Feldern: Die Politik muss rechtliche Rahmenbedingungen schaffen, mit denen das erschütterte Vertrauen der Bevölkerung wie der Industrie wiederhergestellt werden kann; die Industrie muss transparente und vertrauenswürdige Geschäftsmodelle entwickeln. Tatsächlich kann hierin ein entscheidender Wettbewerbsvorteil entstehen: Sicherheit und Vertrauenswürdigkeit lassen sich monetarisieren – im Cloud-Kontext könnten daher gerade europäische Anbieter diesen Vertrauensvorteil ausspielen (siehe auch Kapitel 5.1 Handlungsempfehlung „Monitoringsystem für die M2M-Cybersicherheit (M2M-CERT)“).

3.8 Zusammenfassung: Current Best Practices

Vor dem Hintergrund der großen technischen, anwendungsspezifischen und strukturellen Vielfalt fällt es schwer, eine einzelne Best Practice zu identifizieren. Dennoch sind einige Trends unverkennbar, deren Tragfähigkeit auch durch Analogie zu anderen IT- und Kommunikationssystemen belegt ist:

- Horizontale Struktur: M2M-Systeme sollten aus Silos ausbrechen und sich zu horizontal strukturierten Systemen entwickeln.
- Einfach: Die verwendeten Systeme sollten möglichst einfach, mit möglichst wenigen Grundfunktionen strukturiert sein, auch wenn dabei Detailoptimierung verloren gehen mag.
- Offene Standards: M2M-Anwendungen sollten auf offenen Standards setzen und proprietäre Ansätze vermeiden.
- Offene Schnittstellen: M2M-Anwendungen sollten offene Schnittstellen zur Verfügung stellen und darauf vorbereitet sein, als Komponenten in unterschiedlichen Kontexten Daten oder Handlungen zur Verfügung zu stellen.

Obzwar entscheidend, ist es zum jetzigen Zeitpunkt allerdings nicht verantwortbar, von Best Practices bei Sicherheit zu sprechen. Hier ist noch viel zu tun.

4 M2M-Fallbeispiele

4.1 Fernzugriff und Fernsteuerung für Blockheizkraftwerke (BHKWs)

Anwendungsfeld	Intelligente Energienetze
Beschreibung des M2M-Fallbeispiels	Condition Monitoring und SSL/TLS-gesicherte Service- und Wartungsfernzugriffe auf BHKWs sowie deren Fernsteuerung durch Dritte.
Verfügbarkeitsstatus	State of the Art
Nutzen	Blockheizkraftwerke sind komplexe Maschinen. Durch die Lösung können sie ohne Spezialkenntnisse in Privathaushalten betrieben werden. Die Fernsteuerschnittstelle ermöglicht darüber hinaus ein dezentrales Energiemanagement, um beispielsweise virtuelle Kraftwerke oder Smart-Home-Lösungen zu realisieren.
Gesellschaftl. Relevanz inkl. Erklärung	Mittel – Blockheizkraftwerke verursachen recht hohe Investitionskosten.
Technische Voraussetzungen	Blockheizkraftwerk mit geeigneter Steuerung
Adressierbares Kundenpotenzial	Betreiber von Heizungsanlagen in Wohn- und Zweckbauten, Betreiber von Fertigungsstätten und Industrieanlagen
Verwandte Anwendungsfelder	Smart Services, Smart Home, Energiemanagement

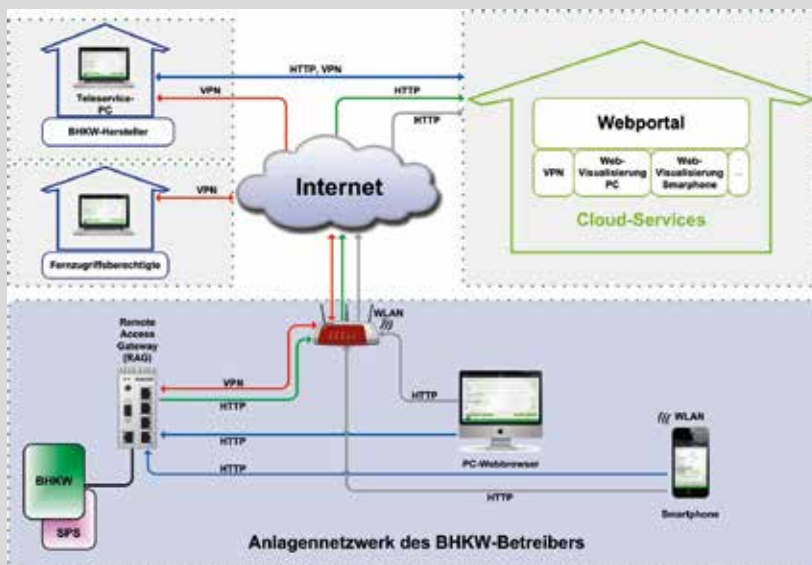


Abbildung 7: Fernzugriff und Fernsteuerung für Blockheizkraftwerke
Quelle: SSV Software Systems, 2013

4.2 Wasserwirtschaft

Anwendungsfeld	Intelligente Wasserwirtschaft – Interaktion von Geräten
Beschreibung des M2M-Fallbeispiels	580 dezentrale Geräte (Pumpen, Wasserhochbehälter, ...) verteilt auf 1.400 km. Direkte Interaktion zwischen Geräten. Leitwarte hat jederzeit optionale Kontrolle.
Verfügbarkeitsstatus	In Betrieb – Cutting edge of Technology (Pilotierung in 2012)
Nutzen	Erhebliche Einsparungen von vormals unnötigen aufwändigen ServiceEinsätzen - zusätzlich 90% Kostensenkung der Lizenz-Initialkosten.
Gesellschaftl. Relevanz inkl. Erklärung	Hoch: Innovative und branchenübergreifende Interaktion zwischen Maschinen und Diensten, basierend auf herstellerunabhängigen Interoperability-Standard OPC-UA mit integrierter Security, erzeugt erhöhte Akzeptanz.
Technische Voraussetzungen	Daten, Semantik und Kommandotransport aus den Steuerungen über Routermodems in einer geschlossenen Mobilfunkgruppe. Zusätzlich Authentifizierung/Verschlüsselung basierend auf OPC-UA. Geräte bieten UA-Server-Schnittstellen, um auf Anfragen der Leitwarte oder anderer Geräte zu antworten. Geräte agieren zusätzlich als UA-Client, um Daten zu sammeln und eigenständig die Kommunikation mit anderen Geräten zu initiieren. (Pumpe1 an Pumpe2: „Meine Wasserqualität wird schlecht, bitte übernehmen“).
Adressierbares Kundenpotenzial	Alle Branchen/alle Ebenen (vom Gerät bis zur IT-Ebene): Jeder ist daran interessiert, Daten, Dienste und deren Bedeutung einfach und sicher zwischen Geräten und Maschinen untereinander und mit der IT-Welt auszutauschen.
Verwandte Anwendungsfelder	Machine-to-Machine, Remote Service

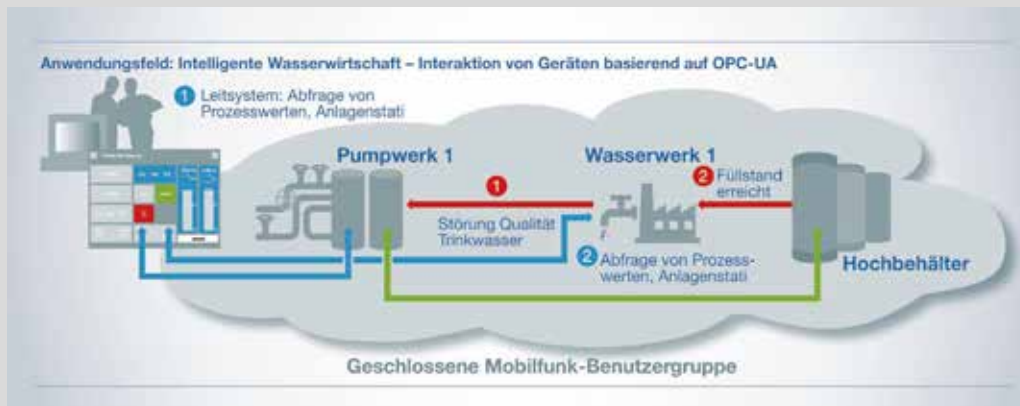


Abbildung 8: Intelligente Wasserwirtschaft – Interaktion von Geräten
Quelle: Zweckverband Wasser und Abwasser Vogtland, 2013

4.3 Energiewirtschaft

Anwendungsfeld	Smart Energy – Messung von Stromverbrauchern
Beschreibung des M2M-Fallbeispiels	6.000–10.000 dezentrale Liegenschaften sollen den Energieverbrauch messen, die Messdaten puffern und zur weiteren Analyse in die Big-Data-Cloud-Datenbank leiten.
Verfügbarkeitsstatus	Pilotierung in 2013 – Inbetriebnahme 2014
Nutzen	Genauere Kenntnis der Stromaufnahme zur Reduzierung des Verbrauchs und zur Aushandlung von Strompreisen
Gesellschaftl. Relevanz inkl. Erklärung	Hoch: Innovative und branchenübergreifende Lösung, basierend auf herstellerunabhängiger Interoperability-OPC-UA-Standard mit integrierter Security, erzeugt erhöhte Akzeptanz.
Technische Voraussetzungen	In dezentralen Liegenschaften wird pro SPS-Steuerung von unterlagerten Teilnehmern der Stromverbrauch gemessen, in der Steuerung zwischengespeichert und einmal täglich (bei Bedarf auch sofort) in die zentrale Datenablage gepusht. Die Steuerung agiert als OPC-UA-Client, die Daten werden dem UA-Server (Historic Access) mit Security und Verwendung von herstellerunabhängigen Standards in der Cloud gepusht. Der Server speichert die Daten in einer Datenbank ab. Den Mandanten stehen zur Analyse der Big Data zwei Schnittstellen zur Verfügung: direkter Zugriff in die SQL-Datenbank oder OPC-UA-HA (Historic Access).
Adressierbares Kundenpotenzial	Alle Branchen/alle Ebenen (vom Gerät bis zur IT-Ebene): Daten sammeln, puffern und weiterleiten ist eine verbreitete Aufgabe.
Verwandte Anwendungsfelder	Smart Energy, Data-Logging

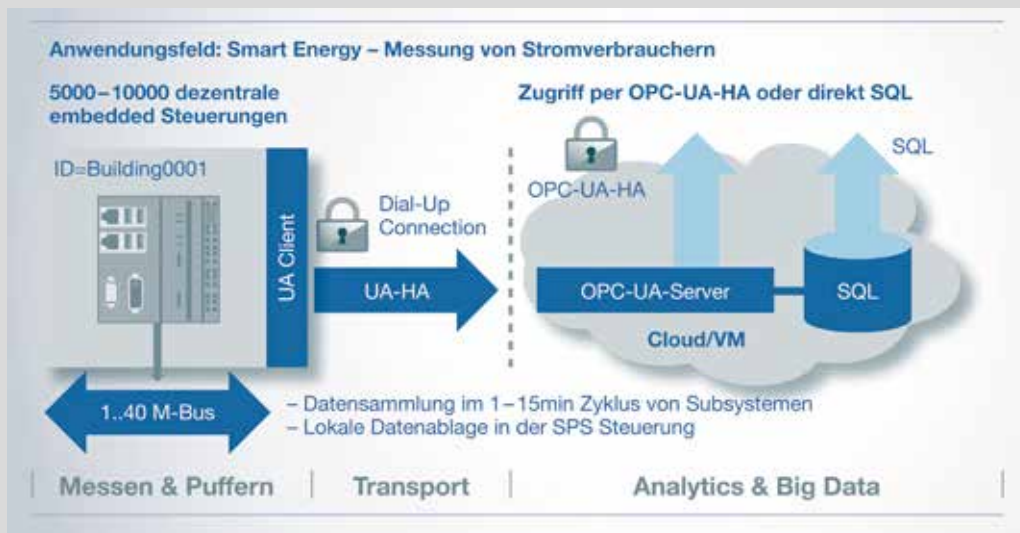


Abbildung 9: Smart Energy – Messung von Stromverbrauchern
Quelle: BECKHOFF Automation, 2013

4.4 Real Time Cargo Monitoring End-to-End Solution

Anwendungsfeld	Intelligente Verkehrsnetze – Transport & Logistik. Überwachung von Frachtgütern über zahlreiche Branchen hinweg, in denen Güter interkontinental verschifft werden.
Beschreibung des M2M-Fallbeispiels	Schlüsselfertige Echtzeit-Frachtüberwachung Ende-zu-Ende-Premium-Lösung, bestehend aus einem Tracking-Gerät, einem Web-Portal mit E-Mail-Benachrichtigungsdienst und 1st level support.
Verfügbarkeitsstatus	Pilotierung Oktober 2013, Out of Footprint
Nutzen	Flexible Lösung, da das Tracking-Gerät jederzeit außen am Container angebracht werden kann. In dem Gerät befinden sich mehrere Sensoren, die die Umgebungsbedingungen wie Temperatur, Luftfeuchtigkeit oder Erschütterungen aufzeichnen.
Gesellschaftl. Relevanz inkl. Erklärung	Mittel
Technische Voraussetzungen	siehe Abbildung 10
Adressierbares Kundenpotenzial	<ul style="list-style-type: none"> – Kunden im Fokus: die Mieter der Transportbehälter, die diese mit hochwertigen Gütern über Land und Meer versenden müssen. – Zielkunden: verantwortliche Disponenten/Supply Chain Manager.
Verwandte Anwendungsfelder	Wasser, Straße, Schiene

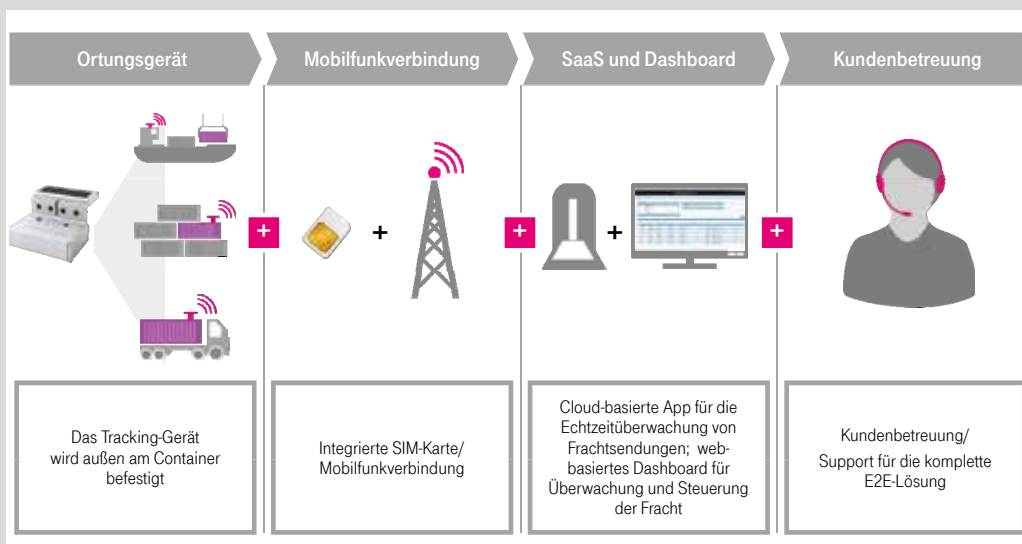


Abbildung 10: Real Time Cargo Monitoring End-to-End Solution
Quelle: Deutsche Telekom, 2013

4.5 Interaktion mit Maschinen, M2M als soziale Kommunikation

Anwendungsfeld	Sammlung von Anwendungsfällen, in denen Nutzer direkt in die M2M-Kommunikation involviert werden, z. B. um M2M-Anwendungen zu verstehen und zu bedienen. Das wird in den Anwendungsfeldern Energie, Gesundheit, Verkehr und evtl. Bildung, Verwaltung und Industrie 4.0 relevant werden.
Beschreibung des M2M-Fallbeispiels	Anwender registrieren ihre zugeordnete Geräte einmalig. Diese Geräte können unterschiedlichste Aufgaben erfüllen, vom E-Bike bis zur Waschmaschine. Wenn die Geräte eine Interaktion mit den Anwendern benötigen, senden sie eine Nachricht an eine Plattform. Diese Plattform stellt die Nachrichten der Geräte und die Antworten der Anwender in einer einfach zu bedienenden Anwendung dar, die z. B. auf Smartphones laufen kann. Ebenso werden Nutzerwünsche auf diese Weise entgegengenommen. Die Plattform kann zudem Konflikte erkennen und Anforderungen unterschiedlicher Geräte aufeinander abstimmen.
Verfügbarkeitsstatus	Vision, Pilotierung gezeigt zwischen Deutscher Telekom und Ericsson auf dem Mobile World Congress 2013 in Barcelona.
Nutzen	Einfache Bedienung und erhöhte Akzeptanz durch mehr Transparenz für die Anwender. Ergänzt zudem M2M-Anwendungen durch eine spielerische Komponente, sodass die Motivation zunimmt, sich z. B. mit Energieverbrauchsoptimierung zu beschäftigen.
Gesellschaftl. Relevanz inkl. Erklärung	Hoch: Die Interaktion von Benutzern mit Maschinen ist eine Herausforderung, die neue Ansätze erfordert. Auch um die Lernkurve für Anwender einfach zu gestalten, bietet es sich an, weit verbreitete Interaktionsformen, wie sie in sozialen Netzen eingesetzt werden, für die Kommunikation mit Maschinen zu nutzen. Geschieht dies zudem anwendungsübergreifend, also beispielsweise zur Steuerung von Standheizungen genauso wie zum Einschalten von Licht, wird die Kommunikation mit Maschinen als sehr natürlich empfunden.
Technische Voraussetzungen	Kommunikationsschnittstellen (Mobilfunk, WLAN, Bluetooth) in den Geräten, Interoperabilitätsstandards wie OPC-UA, OSGi, UPnP und andere sowie eine entsprechende Serverplattform. Da es sich hier um noch prototypenhafte/visionäre Produkte an der Schwelle zur Marktreife handelt, können verschiedene Lösungen eingesetzt werden. Alle Branchen/alle Ebenen (vom Gerät bis zur IT-Ebene): Daten sammeln, puffern und weiterleiten ist eine verbreitete Aufgabe.
Adressierbares Kundenpotenzial	Jeder Bürger ist interessiert an einer einfachen Art und Weise, mit Maschinen zu kommunizieren, also alle Bürger.
Verwandte Anwendungsfelder	Wie oben beschrieben.



Abbildung 11: Interaktion mit Maschinen, M2M als soziale Kommunikation
Quelle: Ericsson, 2013

4.6 Telemetrie gewerblicher Kaffeemaschinen

Anwendungsfeld	Interaktionen mit Maschinen
Beschreibung des M2M-Fallbeispiels	Ende-zu-Ende-Lösung zur automatischen Meldung von Zählerständen und Fehlercodes aus der Ferne; Stichwort Condition Monitoring.
Verfügbarkeitsstatus	State of the Art, in Betrieb
Nutzen	Das Auslesen der Zählerstände gibt Informationen über Kaffeeverbrauch, Verbrauchsmaterialien und notwendige Services. Aktuelle Maschineneinblicke geben Hinweise auf evtl. zukünftige Fehlerzustände und damit im Vorfeld zu vermeidende Ausfallzeiten. Zudem: Steigerung der Service-Qualität, wertvolle Hinweise für Neukonstruktionen durch Langzeitbeobachtungen, Vermeidung von Fahrwegen durch Einsparung unnötiger Einsätze und bessere Tourenplanung, Wettbewerbsvorteile durch Vorreiterrolle, Optimierung von Prozessen, neue Dienstleistungen und Geschäftsmodelle.
Gesellschaftl. Relevanz inkl. Erklärung	Mittel, da nur indirekter Nutzen. Jedoch werden Maschinen-Zuverlässigkeiten generell erhöht.
Technische Voraussetzungen	Die Maschine sollte über eine Schnittstelle zum Auslesen der Protokolle verfügen.
Adressierbares Kundenpotenzial	Hersteller von Maschinen, die einer Überwachung unterliegen bzw. die von Ferne kontrolliert werden sollen. Betreiber von entsprechenden Maschinen.
Verwandte Anwendungsfelder	Remote Control, Remote Service

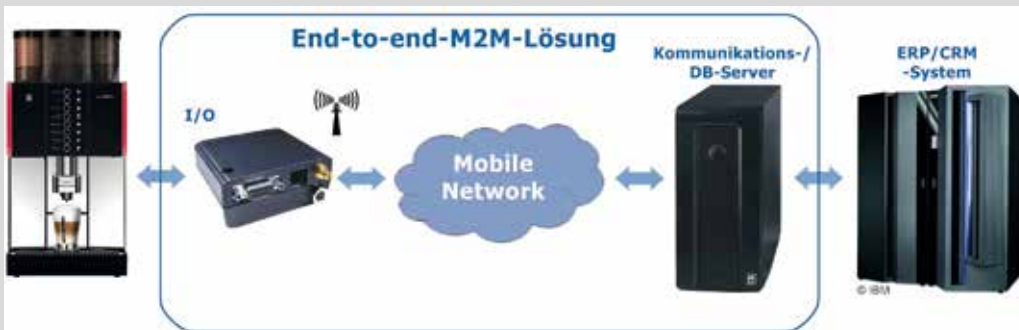


Abbildung 12: Telemetrie gewerblicher Kaffeemaschinen

Quelle: MC Technologies, 2013

4.7 Frühwarnsystem

Anwendungsfeld	Industrie 4.0/Do It Yourself
Beschreibung des M2M-Fallbeispiels	Im Sommer 2013 mussten in Deutschland aufgrund von Überschwemmung und Hochwasser große Eigentumsverluste hingenommen werden. Der Student Wilhelm Kirchgässner arbeitet an einem Hochwasserfrühwarnsystem, das über ein Social Network alarmiert.
Verfügbarkeitsstatus	M2M-Pilotprojekt mit bestehenden Industrie-Produkten von Phoenix Contact, die ursprünglich nicht für diese Lösung entwickelt wurden.
Nutzen	Schnelle Alarmierung über ein Social Network. Das M2M-Produkt alarmiert die Social-Network-Gruppe.
Gesellschaftl. Relevanz inkl. Erklärung	Das Projekt zeigt, dass immer mehr interessante M2M-Produkt- und Geschäftsideen entstehen, die M2M gezielt nutzen und das Potenzial haben, unser Leben dauerhaft zu verbessern.
Technische Voraussetzungen	Keine. Alle „Bausteine“ sind bereits vorhanden. Diese müssen nur richtig zusammengesetzt werden.
Adressierbares Kundenpotenzial	Breites öffentliches Publikum
Verwandte Anwendungsfelder	Übertragung von diversen Sensordaten aus dem Bereich Umweltmesstechnik



Abbildung 13: Hochwasserfrühwarnsystem, das über ein Social Network alarmiert
Quelle: PHOENIX CONTACT, 2013

4.8 Call a Bike

Anwendungsfeld	Fahrradverleihsysteme als Ergänzung und Erweiterung des ÖPNV
Beschreibung des M2M-Fallbeispiels	Automatisierte Fahrradverleihsysteme benutzen bisher kabelgebundene Datenverbindungen, was hohe Investitionen erfordert und unflexibel ist. Oder sie verwenden den Nutzer als Mittler zur Datenübertragung, was fehleranfällig und kompliziert für den Kunden ist. M2M-Übertragung der Fahrdaten vereinfacht maßgeblich die Benutzung des Systems, senkt die Investitionskosten deutlich und erhöht entscheidend die Flexibilität.
Verfügbarkeitsstatus	In Betrieb mit unterschiedlichen Systemausprägungen
Nutzen	Die Vereinfachung der Kundenprozesse erschließt neue Nutzergruppen, denen das bisherige System zu kompliziert war. Die Nutzungszahlen steigen dadurch im deutlich zweistelligen Prozentbereich. Durch verstärkte Präsenz des Produkts kommt ein Selbstläufereffekt in Gang, der zu weiter steigenden Fahrzahlen führt.
Gesellschaftl. Relevanz inkl. Erklärung	Integration in bestehende Verkehrsverbünde wird ermöglicht und innovative Fahrradverleihsysteme übernehmen eine Vorreiterrolle für zukünftige Verkehrskonzepte.
Technische Voraussetzungen	Flächendeckende Bereitstellung von Mobilfunk in ausreichender Qualität, um Daten in Echtzeit auszutauschen, inklusive der notwendigen Rückfallebenen bei Störungen.
Adressierbares Kundenpotenzial	Alle Bürger die mobil sein, aber nicht die dafür nötigen Geräte besitzen wollen.
Verwandte Anwendungsfelder	Verkehrsmittel und technische Geräte für eine zeitweilige Nutzung



Abbildung 14: Call a Bike
Quelle: Deutsche Bahn, 2013

4.9 Smart Vending mit Internet-Bezahldiensten

Anwendungsfeld	Internet-Bezahldienste und Automaten verbinden (Mashup)
Beschreibung des M2M-Fallbeispiels	Kunden können an Verkaufsautomaten mit ihrem Smartphone Produkte auswählen und bezahlen. Der gesamte Kaufvorgang wird über das Smartphone abgewickelt. Dies gilt auch für die Bezahlung, die in diesem Anwendungsfall über den Internet-Bezahldienst PayPal durchgeführt wird. Abschließend wirft der Automat das bezahlte Produkt aus, ferngesteuert über ein eingebautes Telemetrie-Modul. Durch diese Kombination von M2M und Internet-Diensten sind weitere M2M-Anwendungen denkbar, zum Beispiel Gutscheine oder Echtzeit-Sonderangebote auf dem Smartphone.
Verfügbarkeitsstatus	Pilot an einer Universität mit der Cumulocity GmbH und einem Automatenaufsteller
Nutzen	Gegenüber konventionellen bargeldlosen (auch NFC-basierten) Bezahlsystemen bietet die Kombination von Internet-Bezahldienst mit M2M eine Reihe von Vorteilen: Der Kunde bewegt sich in einer ihm vertrauten Umgebung, seinem Smartphone und den dort vorhandenen Bezahldienst-Apps. Dieses Vertrauen führt zu einer höheren Akzeptanz der bargeldlosen Bezahlung. Des Weiteren ist der Investitionsbedarf des Automatenbetreibers gering, da keine Installation von bargeldlosen Bezahlsystemen wie z. B. von (NFC-) Kartenlesern notwendig ist. Auch sind die Transaktionskosten von Internet-Bezahldiensten günstiger als bei herkömmlichen Kreditkarten.
Gesellschaftl. Relevanz inkl. Erklärung	Mittel
Technische Voraussetzungen	Die Maschinen sollten mit einem Telemetrie-Modul ausgestattet sein.
Adressierbares Kundenpotenzial	Hersteller von Automaten mit Bezahlungsfunktionen wie Warenautomaten, Kaffeemaschinen, Recycling-Maschinen.
Verwandte Anwendungsfelder	Wie oben beschrieben.



Abbildung 15: Smart Vending mit Internet-Bezahldiensten
Quelle: Cumulocity, 2013

5 Handlungsempfehlungen

Im Kapitel M2M-Geschäftsmodelle und besonders im Kapitel Realisierungen wurde bereits auf unterschiedliche Aspekte des Handlungsbedarfs hingewiesen, deren Bearbeitung sehr wichtig für die erfolgreiche Einführung der M2M-Technologie ist. Das Kapitel M2M-Fallbeispiele verdeutlicht diesen Bedarf anhand von exemplarischen M2M-Lösungen.

Im Folgenden sind darüber hinaus übergeordnete Handlungsempfehlungen aufgeführt, deren Umsetzung im Wirkungsbereich der Bundesregierung, des IT-Gipfels und der zuständigen Branchenverbände liegt.

An dieser Stelle sei auch auf Handlungsempfehlungen im Rahmen anderer M2M-Initiativen hingewiesen, zum Beispiel auf die Thesen für „Cyber Physical Systems“ in der IKT.NRW Roadmap 2020.¹

Aus den obigen Fallbeispielen, Geschäftsmodellen und Realisierungen sind die folgenden Handlungsempfehlungen abgeleitet.

5.1 Monitoringsystem für die M2M-Cybersicherheit (M2M-CERT)

Cyberattacken können immense Schäden anrichten. Ein Monitoringsystem, das Meldungen auf freiwilliger Basis entgegennimmt und einer breiten Öffentlichkeit zur Verfügung stellt, hilft erkannte Schwachstellen zu beseitigen und das Sicherheitsniveau der M2M-Anwendungen insgesamt zu verbessern.

Ausgangssituation:

Unzählige M2M-Anwendungen kommunizieren inzwischen per Internet bzw. nutzen internetbasierte Dienste. Viele davon sind sogar Bestandteil kritischer Infrastrukturen, zum Beispiel das Lastmanagement in elektrischen Versorgungsnetzen. Bei den meisten

Anwendungen wurde dem Schutz gegen Cyberangriffe nicht allzu viel Aufmerksamkeit gewidmet.

Maßnahmenempfehlungen:

1. Aufbau eines M2M-CERT sowie Betrieb einer Website mit Alarmmeldungen und Hinweisen zu erkannten Schwachstellen, akuten Bedrohungen und Bedrohungsrisiken, die für Betreiber und Anbieter von M2M-Anwendungen und Systemen von Bedeutung sind.
2. Organisation einer Meldestelle, um registrierten Benutzern die Möglichkeit zu bieten, Vorfälle und relevante Sachverhalte zu melden, die dann gemäß dem Traffic Light Protocol (TLP) behandelt werden.
3. Realisierung eines Verfahrens, um anonyme Meldungen entgegenzunehmen, zu analysieren und bei Eignung auf der M2M-CERT-Website zu veröffentlichen.
4. Zusammenarbeit mit anderen Organisationen auf nationaler und europäischer Ebene, zum Beispiel dem CERT der European Union Agency for Network and Information Security (ENISA) und dem European Cybercrime Centre (EC3).
5. Laufendes Auswerten aktueller Alarmmeldungen der ICS-CERT-Website des U.S. Department of Homeland Security.
6. Realisierung und Weiterentwicklung geeigneter Maßnahmen (z. B. M2M-Honeypots), um ein möglichst präzises Bild der jeweils aktuellen Angriffskonzepte zu erhalten.

Aus Sicht der Projektgruppe sollte die Umsetzung durch das BSI (Bundesamt für Sicherheit in der Informationstechnik) erfolgen, weil dort einschlägige Erfahrungen vorliegen.

¹ IKT.NRW Roadmap 2020, ITK Cluster NRW, November 2013. URL: http://ikt.nrw.de/fileadmin/user_upload/Dokumente/IKT_Roadmap/IKT-NRW_Roadmap_2020.pdf (03.12.2013)

5.2 Durchgängig verfügbare Mobilfunknetze für M2M-Anwendungen

Ausgangssituation:

Viele intelligente M2M-Anwendungen entfalten ihren wesentlichen Nutzen erst bei durchgängig verfügbaren mobilen Breitbandnetzen.

Maßnahmenempfehlungen:

Es müssen Anreize und regulatorische Rahmenbedingungen geschaffen werden, um in Zukunft nicht nur 100% der Bevölkerung (Breitbandstrategie der Bundesregierung), sondern auch 100% der geografischen Fläche Deutschlands abzudecken, sowie die Voraussetzungen zu schaffen, M2M-spezifische Lösungen zu realisieren. Dabei wird die global eingesetzte LTE-Technologie mit sehr geringen Latenzzeiten nicht nur als Festnetz-Breitband-Ersatz, sondern als Basis-Technologie der M2M-Datenübertragung eine wesentliche Rolle spielen.

Aus Sicht der Projektgruppe sollten diese Anforderungen im Kontext der Breitbandstrategie der Bundesregierung umgesetzt werden.

5.3 Verstärkte Nutzung von M2M-Experimentier-Kits an Schulen und Hochschulen mit Industrieunterstützung

Ausgangssituation:

M2M-Experimentier-Kits bzw. DIY-Plattformen wie Raspberry Pi und Arduino ermöglichen die Entwicklung von kostengünstigen M2M-Anwendungen und bieten die Chance eines schnellen Markteintritts.

Maßnahmenempfehlungen:

In Zusammenarbeit mit der Industrie sollten durch den Einsatz von M2M-Experimentier-Kits innovative M2M-Anwendungen entwickelt werden. Preise und Prämierungen für gut gemachte und innovative

M2M-Anwendungen können den Weg vom Experimentierfeld in die kommerzielle Anwendung und eventuell Firmengründung ebnen. Hackathons und Innovations-Kits für den Mittelstand zur Erzielung von Grundfertigkeiten, die auch zertifiziert werden könnten, wären erste Ansätze dazu. Eine abgestimmte und vernetzte Palette von Einzelmaßnahmen, unterstützt von Wirtschaft, Politik (mittels Förderprogrammen) und Hochschulen kann mit überschaubaren Mitteln eine Menge bewirken. Durch diese Einzelmaßnahmen werden Impulse für neue M2M-Anwendungen geschaffen sowie die Innovationsfähigkeit der Industrie gestärkt und für neue Herausforderungen wie das Next-Gen-Internet und Industrie 4.0 vorbereitet.

Eine vernetzte Palette von Einzelmaßnahmen sollte aus Sicht der Projektgruppe zwischen Ministerien (z. B. BMF) und Industrieverbänden (z. B. M2M Alliance, BITKOM, ZVEI) abgestimmt werden.

5.4 Förderung von M2M-Lösungen für den Mittelstand

Ausgangssituation:

Die Einführung von M2M-Anwendungen wird oft erschwert durch hohe anfängliche Integrationsaufwendungen, Datensicherheitsbedenken und fehlende Übersicht über M2M-Dienstleistungsangebote. Dies trifft den Mittelstand härter als beispielsweise Automobilhersteller, Energieversorger oder große Maschinenbauer, da diese die Mittel und das Know-how haben, ihre M2M-Anwendungen und Plattformen aus eigenen Ressourcen heraus zu finanzieren, zu entwickeln und zu betreiben. Smart und Connected Services werden zukünftig ein wesentlicher Bestandteil von Produkten sein und neue Lösungen und Geschäftsmodelle ermöglichen. Daher ist die Investition in die Basistechnologie M2M heute von entscheidender Bedeutung für die Wettbewerbsfähigkeit von morgen.

Maßnahmenempfehlungen:

Wir empfehlen den weiteren Ausbau der Innovationsförderung für M2M-Lösungen für den Mittelstand, wie

beispielsweise im ZIM-KN-Projekt (Zentrales Innovationsprogramm Mittelstand) „Sichere M2M-Kommunikationslösungen für mittelständische industrielle Anwender“. Bei derartigen ZIM-Projekten stehen Innovationen wie energieautarke Sensoren und intelligente und sichere Gateways im Vordergrund.

Darüber hinaus sollte jedoch auch ein Marktpenetrationsprogramm für M2M-Lösungen angeboten werden.

Hierzu sind aus unserer Sicht die Förderkonzepte des BAFA (Bundesamt für Wirtschaft und Ausfuhrkontrolle) gut geeignet, die bereits Energiemanagementsysteme bzw. Querschnittstechnologien fördern oder Wirtschaftsförderung für den innovativen Schiffsbau und weitere Technologien bieten.

Folgende Förderleistungen/Zuschüsse sollten dabei für M2M angeboten werden:

- Beratungsleistungen zur Konzeption von M2M-Diensten und -Geschäftsmodellen,
- Informationsveranstaltungen und Workshops für mehr Transparenz der Lösungsanbieter und Austausch mit dem Mittelstand,
- Fördermittel für die Einführung von M2M-Lösungen,
- Markterschließungsprogramme,
- Förderung von Leuchtturmprojekten.

5.5 Förderung der Ausbildung für verteilte eingebettete Systeme

Ausgangssituation:

Die erfolgreiche Entwicklung von M2M-Systemen erfordert Ingenieure und Informatiker, die über die Grenzen ihres jeweiligen Faches hinaus ausgebildet sind und die Eigenarten von Hardware und Software, die Erfordernisse der Integration von Software und Hardware, der Architektur eines verteilten und vernetzten Gesamtsystems, der regelgerechten Entwicklung von großen Software-Systemen, wie auch die rechtlichen und regulatorischen Rahmenbedingungen verstehen und in einem industriellen Entwicklungsprozess zum Einsatz bringen könnten. Hierzu gibt es erste Ansätze in der Hochschulausbildung, aber das Thema ist bisher nicht in der notwendigen Breite präsent. Sowohl in der Erstausbildung wie in der beruflichen Weiterbildung fehlen hier Angebote, um die Konkurrenzfähigkeit der deutschen Industrie sicherzustellen.

Maßnahmenempfehlungen:

Wir empfehlen daher, die Entwicklung solcher Aus- und Weiterbildungsmaßnahmen gezielt zu unterstützen und Universitäten und Industrie die gemeinsame Möglichkeit zu geben, solche Maßnahmen zu erarbeiten. Dies kann z. B. durch finanzielle Unterstützung im Rahmen von Zuwendungen oder Projekten geschehen. Zusätzlich sollten Aktivitäten unterstützt werden, die solche Berufsfelder bereits in den Schulen fördern und attraktiv darstellen können.

Hier könnten etwa Einzelmaßnahmen von Hochschulen, aber auch Aktivitäten etwa der Gesellschaft der Informatik und von 4ING (<http://www.4ing.net>) unterstützt werden.

Weiterführende Literatur

- [1] Uwe Kubach, IEEE INTERNATIONAL CONFERENCE ON COMMUNICATIONS, 9-13 JUNE, BUDAPEST, HUNGARY, URL: http://www.ieee-icc.org/2013/5.M2M_ICC_2013-06-11.pdf (05.12.2013)
- [2] Machine-to-Machine-Kommunikation - eine Chance für die deutsche Industrie, AG2 M2M Initiative Deutschland, Stand: November 2012. URL: <http://www.it-gipfel.de/IT-Gipfel/Navigation/mediathek,did=522484.html> (03.12.2013)
- [3] Embedded Mobile Whitepaper Embedded Mobile Guidelines Release 3 28 March 2012. URL: http://www.gsma.com/connectedliving/wp-content/uploads/2012/03/GSMA-Whitepaper-Embedded-Mobile-Guidelines-Release_31.pdf (03.12.2013)
- [4] "Smarter Apps for Smarter Phones" Version 0.14 February 2012. URL: <http://www.gsma.com/technicalprojects/smarter-apps-for-smarter-phones> (03.12.2013)
- [5] Mobilfunk – Datenübertragung in der Industrie, ISBN 978-3-00-037386-2. URL: <http://www.phoenixcontact.de/m2m> (03.12.2013)
- [6] IKT.NRW Roadmap 2020, ITK Cluster NRW, November 2013. URL: http://ikt.nrw.de/fileadmin/user_upload/Dokumente/IKT_Roadmap/IKT-NRW_Roadmap_2020.pdf (03.12.2013)

Herausgeber
Arbeitsgruppe 2 des Nationalen IT-Gipfels (AG2)
„Digitale Infrastrukturen als Enabler für innovative Anwendungen“

Ergebnisbericht 2013
M2M-Initiative Deutschland

Das Jahrbuch 2013/2014
„Digitale Infrastrukturen – Schwer-
punkte und Zielbilder für die Digitale
Agenda Deutschlands“ sowie
weitere Dokumente der AG2 sind
als Download frei erhältlich unter

www.it-gipfel.de

Mitglieder der Projektgruppe M2M-Initiative Deutschland



Dr. Christoph Bach (Leitung)
Ericsson GmbH

Dr. Ralf Ackermann
SAP AG

Prof. Dr.-Ing. Gerd Ascheid
RWTH Aachen University, UMIC Research Centre

Gerrit Boysen
PHOENIX CONTACT Electronics GmbH

Martin Braband
Tixi.Com Telecommunication Systems GmbH

Guido Burchartz
Avantgarde Business Solution GmbH

Guido Burger
ORACLE Deutschland B.V. & Co. KG

Guido Dartmann
RWTH Aachen University, UMIC Research Centre

Wolfgang Dorst
Bundesverband Informationswirtschaft, Telekommunikation und
neue Medien e.V. (BITKOM)

Joachim Dressler
Sierra Wireless Deutschland GmbH

Lars Dürkop
Hochschule Ostwestfalen-Lippe

Karl-Heinz Erdt
DB Rent GmbH

Marco Fiene
MC-Technologies GmbH

Jens Grebner
Siemens AG

Bernd Gross
Cumulocity GmbH

Jürgen Hase
Deutsche Telekom AG

Dr. Jörg-Michael Hasemann
T-Systems International GmbH

Stefan Hoppe
OPC Foundation

Prof. Dr. Holger Karl
Universität Paderborn

Dr. Ingolf Karls
Intel Mobile Communications GmbH

Andreas Kleinert
ProSyst Software GmbH

Prof. Dr. Uwe Kubach
SAP AG

Ulf Moorfeld
Deutsche Telekom AG

Jens Mühlner
T-Systems International GmbH

Dr. Norbert Niebert
Ericsson GmbH

Dr. Johannes Prade
Nokia Solutions and Networks GmbH & Co. KG

Stephan Reim
PHOENIX CONTACT Electronics GmbH

Ronaldo Robl
Cinterion Wireless Modules GmbH

Axel Sommer
DB Kommunikationstechnik GmbH

Henning Trsek
Hochschule Ostwestfalen-Lippe

Dr. Frederic Ufer
Verband der Anbieter von Telekommunikations- und
Mehrwertdiensten e.V. (VATM)

Dietmar Urban
urbato GmbH

Stefan Vaillant
Cumulocity GmbH

Klaus-Dieter Walter
SSV Software Systems GmbH

Johannes Wust
Hasso-Plattner-Institut für Softwaresystemtechnik GmbH