Mit Innovationen Zukunft gestalten

IKT.NRW

Cluster Informations- und Kommunikationstechnologie

KOMMUNIKATIONSNETZE FÜR CYBER PHYSICAL SYSTEMS

NORDRHEIN-WESTFALEN AUF DEM WEG ZUM DIGITALEN INDUSTRIELAND

ExzellenzNRW

Cluster Nordrhein-Westfalen

IKT.NRW
SCHRIFTENREIHE

Die Studie "**Kommunikationsnetze für Cyber Physical Systems**" erörtert die technisch-wissenschaftlichen Hintergründe der neuen Herausforderungen durch Cyber Physical Systems für das Design von Kommunikationsnetzen sowie die Innovationspotenziale für Unternehmen und Hochschulen in NRW.

Autor
Prof. Dr. Christian Wietfeld
Technische Universität Dortmund
Lehrstuhl für Kommunikationsnetze
christian.wietfeld@tu-dortmund.de
www.cni.tu-dortmund.de

Danksagung
In die Studie sind hilfreiche Kommentare und Anregungen der Mitglieder der IKT.NRW-Arbeitsgruppe „Kommunikationsnetze“ eingeflossen, für die ich mich an dieser Stelle ausdrücklich bedanken möchte.

Die Studie spiegelt die Meinung des Autors wider.

Hintergrund
Diese Studie ist Teil der IKT.NRW Schriftenreihe "NRW auf dem Weg zum digitalen Industrieland". Die Beiträge der Schriftenreihe ergänzen die unter dem gleichnamigen Titel erschienene IKT.NRW Roadmap 2020 – entweder aus der Perspektive einer IKT-Basistechnologie oder einer der NRW-Schlüsselbranchen.

Herausgeber
Clustermanagement IKT.NRW
V. i. S. d. P. Monika Gatzke
c/o SiKoM – Institut für Systemforschung der Informations-, Kommunikations- und Medientechnologie
Bergische Universität Wuppertal
Rainer-Gruenter-Str. 21
42119 Wuppertal

Wuppertal, November 2013

INHALT

01
EINLEITUNG

Die praktisch universelle Verfügbarkeit von Kommunikationsnetzen ermöglicht es, technische Geräte und Systeme unterschiedlichster Art weiträumig miteinander zu vernetzen und zu steuern. So entstehen ganz neue Möglichkeiten der Automatisierung komplexer, verteilter technischer Systeme, die mit folgenden zugespitzten Visionen beispielhaft skizziert werden können:

- **„100% CO2-freie Energie: 24-Stunden-365 Tage“:** Durch die zuverlässige Vernetzung von regenerativen Energiequellen, -speichern und -verbrauchern soll es gelingen, die elektrische Energieversorgung so weit wie möglich auf regenerative

„A cyber-physical system (CPS) is an integration of computation with physical processes. Embedded computers and networks monitor and control the physical processes, usually with feedback loops where physical processes affect computations and vice versa. As an intellectual challenge, CPS is about the intersection, not the union, of the physical and the cyber. It is not sufficient to separately understand the physical components and the computational components. We must instead understand their interaction.“ (Definition nach Lee/Seshia [1]).

Energiequellen umzustellen und gleichzeitig Ausfälle durch Engpässe und Überlastungen zu vermeiden.

- **„Industrie 4.0“:** Durch die effiziente Vernetzung von Produktions- und Logistikprozessen über mehrere Wertschöpfungsstufen hinweg, werden Produkte fortlaufend an die Kunden- und Markterfordernisse angepasst, und gleichzeitig Energiebedarf und Umweltbelastung minimiert.
- **„Grüne Welle für alle“:** Effizienter und sicherer Straßenverkehr ohne Ampeln, Staus und Unfälle, weil die Teilnehmer im Verkehr so vernetzt sind, dass Kollisionen frühzeitig erkannt und vermieden werden können.
- **„Cyber-unterstützter Operationssaal“:** Durch den Einsatz von vernetzten Operationsassistenzsystemen wird es möglich, komplexe medizinische Eingriffe an Patienten auch unter Beteiligung von räumlich entfernten Spezialisten durchzuführen.

Die so entstehenden Systeme optimieren durch Informations- und Kommunikationstechnik das Zusammenspiel von Sensorik („Beobachten der Umgebung“) und Aktorik („Agieren mit der Umgebung“). Sie werden als Cyber Physical Systems (CPS) bezeichnet. Die CPS-spezifischen Anforderungsprofile erfordern neuartige Lösungsansätze für die Hardware- und Software-komponenten sowie die Kommunikationsnetze der Cyber Physical Systems.

Die nachfolgend vorgestellte Studie adressiert die besonderen Herausforderungen in Bezug auf die Vernetzungsaspekte. Hierzu werden zunächst die CPS-spezifischen Anforderungen an die Netztechnik beleuchtet. Der Darstellung des Stands der Technik und der daraus abgeleiteten CPS-spezifischen Innovationsfelder folgt eine Diskussion zu einer grundlegenden Designentscheidung: Können öffentliche Netzinfrastrukturen verwendet werden oder sind nur spezialisierte Netze in der Lage, CPS-Anforderungen vollständig erfüllen zu können? Anhand von aktuellen Forschungsaktivitäten werden konkrete Umsetzungskonzepte für CPS anhand unterschiedlicher Anwendungsfelder beispielhaft beschrieben.

02
NEUE SPIELREGELN
KOMMUNIKATIONSNETZE IN CYBER PHYSICAL SYSTEMS

IKT-Infrastrukturen werden aktuell und auch in Zukunft am intensivsten von Web- und Video-Datenverkehr beansprucht. Hierbei steht insbesondere die max. verfügbare Datenrate als Hauptqualitätskriterium im Vordergrund und dient auch als wesentliche Motivation für den Ausbau der IKT-Infrastruktur im B2C-Bereich. Für Anwendungen von Unternehmen und Verwaltungen (B2B) sind Sicherheitsmechanismen (Authentifizierung, Verschlüsselung), Interoperabilität und Verfügbarkeitsanforderungen von großer Relevanz.

Diese Qualitätsanforderungen spielen auch für CPS eine wichtige Rolle, jedoch unter vollkommen anderen Rahmenbedingungen. Die Abbildung 1 illustriert anhand der Top3-Anforderungskriterien qualitativ, dass durch CPS ganz neue Herausforderungen für IKT-Infrastrukturen und damit entsprechender Innovationsdruck entsteht.

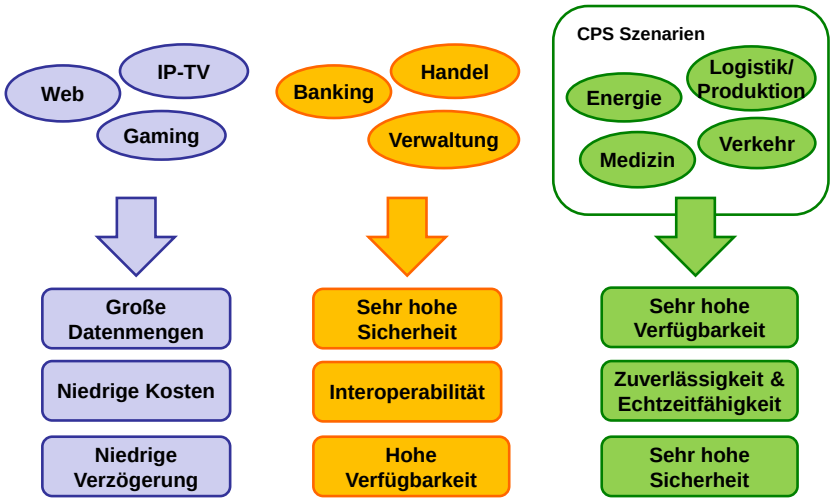

Abbildung 1: Top3-Anforderungskriterien von CPS an Kommunikationsnetze im Vergleich zum klassischen B2C- und B2B-Umfeld (qualitativ)

DATENRATEN FÜR CPS RELEVANT, ABER NICHT ERSTE PRIORITÄT

Cyber Physical Systems sind vor allem durch die Kommunikation zwischen technischen Systemen gekennzeichnet, auch als *Machine-to-Machine*-(M2M)-Kommunikation bezeichnet. Hierbei geht es nur in Ausnahmefällen um die Übertragung sehr großer Datenmengen durch einzelne Netzknoten. Vielmehr ist es oft notwendig, im Verhältnis zu aktuellen Unternehmens- und Endkundendiensten Sensordaten oder Steuerbefehle mit vergleichsweise geringen durchschnittlichen Datenraten zu übertragen. So erzeugt die Übertragung eines Fußballspiels in HD-Qualität in 90 Minuten eine Datenmenge von über 15 GB während in der gleichen Zeit bei einer Übertragung von Stromverbrauchsdaten durch *Smart Meter* nur einige 100 kB entstehen. Bei zunehmendem Steuerungsbedarf steigen die CPS-spezifischen Datenvolumina an, parallel hierzu wächst auch die Datenmenge für Web-/Video-anwendungen stetig. Auch wenn man die weiter zunehmende Menge der Netzknoten („Internet der Dinge“) berücksichtigt, erscheinen die CPS-spezifischen Kommunikationsdienste im Verhältnis zu den stetig wachsenden Datenmengen der Web- und TV-Anwendungen bezüglich der Datenmengen in aktuelle Infrastrukturen integrierbar.

ZUVERLÄSSIGKEITSANFORDERUNGEN DAGEGEN UM GRÖSSENORDNUNGEN HÖHER

Die Herausforderung beim Entwurf geeigneter IKT-Infrastrukturen für Cyber Physical Systems liegen somit nicht primär im Bereich der pro Netzknoten zu transportierenden Datenmengen sondern vielmehr in der **Verfügbarkeit** der Kommunikationsanbindung unter herausfordernden Rahmenbedingungen (siehe Abbildung 1). Ein Vergleich macht die Größenordnungen deutlich: Das deutsche Stromnetz hat eine Verfügbarkeit von 99,97 % [2], während für eine IP-Anbindung im B2B-Bereich über ein SLA (Service Level Agreement) 99+% zugesichert werden. Im Mobilfunkbereich sind Verfügbarkeitswerte von 98+% typisch. Dies illustriert, dass aktuelle IKT-Infrastrukturen nur mit ergänzenden Maßnahmen für CPS nutzbar sind, wenn anspruchsvolle Dienstanforderungen garantiert werden müssen.

Aber auch anhand von weiteren Kriterien wird das neue Anforderungsprofil deutlich:

- CPS umfassen technische Großgeräte (z.B. Kraftwerke, mobile Fahrzeuge), die automatisiert gesteuert werden. Fehlerhaft oder auch zu spät übertragene Sensordaten und Steuerbefehle können zu erheblichen Schäden für Personen und Gegenständen führen. Daher sind immer sehr hohe Anforderungen an die Zuverlässigkeit und oft ebenso an die Echtzeitfähigkeit der Kommunikationsverbindungen zu stellen. Gleichzeitig sind die Übertragungswege durch geeignete Sicherheitsmechanismen vor Angriffen durch Dritte zu schützen.
- CPS sind oft mobil und müssen daher drahtlos, auch bei hohen Geschwindigkeiten und an abgelegenen Orten, vernetzt werden können. Somit sind hohe Anforderungen nicht nur an die zeitliche sondern auch die räumliche Verfügbarkeit (zeitlich/räumlich) zu erfüllen.
- CPS werden oft in besonders störanfälligen Umgebungen betrieben und erfordern daher besonders robuste Übertragungswege.

NEUARTIGE KOMMUNIKATIONSPARADIGMEN: INVERS ASYMMETRISCH UND GRUPPEN-ORIENTIERT

Cyber Physical Systems folgen dabei neuartigen Kommunikationsparadigmen und erfordern spezifische **Kommunikationsdienste zur verteilten Kommunikation**:

Innerhalb eines Cyber Physical Systems müssen Daten zwischen steuernden Komponenten und ausführenden Komponenten (Aktorik) übertragen werden. Dies sind einerseits Daten, die physikalische Zustände der Systeme beschreiben (Sensordaten) oder die Steuerbefehle enthalten. Anders als in der klassischen Weitverkehrskommunikation ist hier die bilaterale, exklusive Verknüpfung zweier Kommunikationspartner (***Point-to-Point***, z.B. zwei Menschen, die ein Telefonat führen, oder auch eine Verbindung zwischen einem Endgerät und einem Server) nur eine Variante der Kommunikation. Vielmehr sind hier auch Dienste gefragt, mit denen gleichzeitig mehrere Systemkomponenten in Gruppen angesprochen werden können (***Broadcast/Point-to-Multipoint/Gruppenkommunikation***), um z.B. Systemzustände zeitnah zu steuern. Ein weiterer Unterschied zu bisherigen Kommunikationswegen ist das asymmetrische Sende-/Empfangsprofil, welches invers zu klassischen Internetdiensten vor allem den Uplink (Sensordaten) belastet. Die dezentrale Steuerung eines CPS erfordert Gruppenkommunikationsdienste und ggf. auch die direkte Kommunikationen zwischen einzelnen Devices (Device-to-Device-Kommunikation).

FLEXIBILITÄT UND SKALIERBARKEIT

Aufgrund ihrer Heterogenität und der sich noch nicht gefestigten Anforderungsprofile erfordern CPS Skalierbarkeit in vielerlei Hinsicht (siehe Abbildung 2):

- Die **Anzahl** der beteiligten Kommunikationsknoten variiert über mehrere Größenordnungen, je nach spezifischer Ausprägung des CPS können Millionen von Kommunikationsknoten beteiligt sein.
- Die **räumliche Ausdehnung** beginnt auf der Ebene eines Fahrzeugs oder Haushalts und endet bei einem weltumspannenden CPS z.B. für die Luftfahrt.
- Während der Normalbetrieb des CPS mit relativ geringen Datenmengen aufgrund von regelmäßig ausgetauschten Statusmeldungen verbunden ist, können die zu übertragenden **Datenmengen** in kritischen Systemzuständen lawinenartig zu einem Vielfachen ansteigen.
- Analog zu den Datenmengen sind auch die Anforderungen an die **Echtzeitfähigkeit** der zu übertragenden Nachrichten variabel: gerade in kritischen Systemzuständen muss sehr schnell reagiert werden und somit die Verzögerung des Netzes trotz gleichzeitig ansteigendem Datenverkehr minimiert werden.

- Die **Werthaltigkeit** einer im CPS-System übertragenen Steuernachricht kann von wenigen Cent bis hin zu Mill. Euro variieren (z.B. wenn statt einem Tiefkühlschrank eine instabile Turbine geregelt werden muss).
- Bei der Integration von CPS-Diensten in öffentliche Netzinfrastrukturen muss es möglich sein, die gegenseitige **Beeinflussung zwischen CPS-Diensten und den Human-to-X Diensten** (Sprache, Web, etc.) zu steuern und situationsangemessen Dienste zu priorisieren.

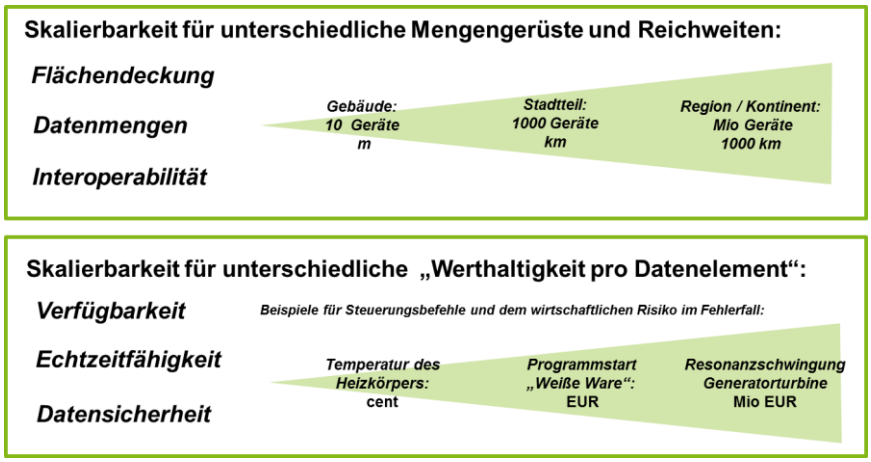

Abbildung 2: Notwendige Skalierbarkeit der Kommunikationsnetze für CPS.

RESSOURCENEFFIZIENZ UND WIRTSCHAFTLICHKEIT

Beim Entwurf von Kommunikationsstrategien für Cyber Physical Systems spielt darüber hinaus die **Ressourceneffizienz** im Hinblick auf **Volumen, Gewicht, Energieverbrauch** und die **Spektrumsnutzung** (bei drahtloser Vernetzung) eine große Rolle.

Weiterhin ist die Verwendung von **standardisierten Schnittstellen** wichtige Grundvoraussetzung für die internationale **Interoperabilität** der Komponenten unterschiedlicher Hersteller und Betreiber in einem Gesamtsystem. Die so entstehenden, CPS-übergreifenden Economies-of-Scale und Auswahlmöglichkeiten für CPS-Betreiber (Multi-Vendor) sind wichtige Kriterien von Investitionsentscheidungen.

Innerhalb eines Cyber Physical Systems sind **Kostenaspekte für Aufbau und Betrieb** des Kommunikationsnetzes von besonderer Bedeutung. Angesichts der engen Integration von Kommunikationskomponenten mit den oft durch längerfristigen Investitionszyklen gekennzeichneten, weiteren Komponenten eines Cyber Physical Systems ist die **Kostenbetrachtung über den gesamten Nutzungszeitraum des CPS** durchzuführen. Die **langfristige technische Unterstützung** ist dabei im Angesicht der schnellen

Innovationszyklen für IKT-Komponenten oft vor allem eine kommerzielle Fragestellung.

MEHRWERTDIENSTE UND ANWENDERFREUNDLICHKEIT

Die Steuerung eines CPS erfordert oft die Kenntnis der geographischen Position des CPS Devices. Daher ist es unter dem Aspekt der Kosten und des Ressourceneinsatzes ein besonders interessanter Aspekt, dass Kommunikationskomponenten auch für weitergehende **Mehrwertdienste** genutzt werden können, so z.B. für die Lokalisierung oder auch Materialcharakterisierung.

Die Anwender von CPS in z.B. Energietechnik, Medizin oder Verkehr sind oft nicht primär IKT-Spezialisten, sondern diese betrachten die IKT als unterstützende Komponente zur Erfüllung ihrer eigentlichen Aufgaben. Da sowohl Experten (Ärzte) wie auch Endnutzer (z.B. Patienten) sehr intensiv und tagtäglich mit CPS in Berührung kommen, ist es essentiell, dass der Netzbetrieb durch eine weitgehende Selbstorganisation sehr anwenderfreundlich erfolgt.

Kriterium	Smart Grid	Verkehr	Medizintechnik
Hohe Verfügbarkeit (zeitlich/räumlich)	++		
Hohe Zuverlässigkeit	++		
Echtzeitfähigkeit	++		
Hohe Sicherheit	++		
Interoperabilität	++		
Verteilte Kommunikation	++		
Hohe Knotendichte	++		
Sehr große Datenmengen	+		++
Große räumliche Ausdehnung	++		+
Langer Lebenszyklus	++	+	
Extreme Formfaktoren	+	++	
Hohe Mobilität	O	++	+
Optimierter Energiebedarf	+	+	++
Bedarf für Mehrwertdienste (Lokalisierung)	O	++	

Tabelle 1 : Beispiele für variierende CPS-Anforderungsprofile an Kommunikationsnetze: viele Gemeinsamkeiten, aber auch relevante Unterschiede

CPS-ANFORDERUNGSPROFILE: VIELE GEMEINSAMKEITEN, ABER AUCH RELEVANTE UNTERSCHIEDE

Je nach Anwendung unterscheidet sich das Anforderungsprofil hinsichtlich der Priorisierung einzelner Aspekte. In der vorstehenden Tabelle 1 wurden die oben genannten Anforderungskriterien charakteristischer Cyber Physical Systems in einer Übersicht qualitativ beispielhaft gewichtet:

- Energiesysteme / Smart Grid
- Automatisierte Verkehrssysteme
- Medizintechnik

03
NETZTECHNIK
CPS-SPEZIFISCHER INNOVATIONSBEDARF

Der Aufbau eines Kommunikationsnetzes wird typischerweise in Form eines Schichtenmodells beschrieben, welches es erlaubt, die unterschiedlichen Aufgaben eines Kommunikationsnetzes auf unterschiedliche Lösungsansätze abzubilden. So entsteht ein Kommunikationsnetz durch das Zusammenfügen unterschiedlichster Komponenten und Werkzeuge. Nachfolgend sollen die notwendigen Innovationen von Kommunikationstechniken für CPS in diesem Sinne diskutiert werden.

Dabei soll hier auf drei Funktionsblöcke fokussiert werden (siehe Abbildung 3):

- Übertragungstechnik: wie werden die Daten physikalisch übertragen (primär Schichten 1 und 2)
- Netzprotokolle: wie werden unterschiedliche Knoten des Netzes Ende-zu-Ende verknüpft (primär Schichten 3 und 4)
- Anwendungsspezifische Dienste und Datenformate: wie wird das Kommunikationsnetz für das Cyber Physical System nutzbar gemacht (primär Schichten 5 bis 7)

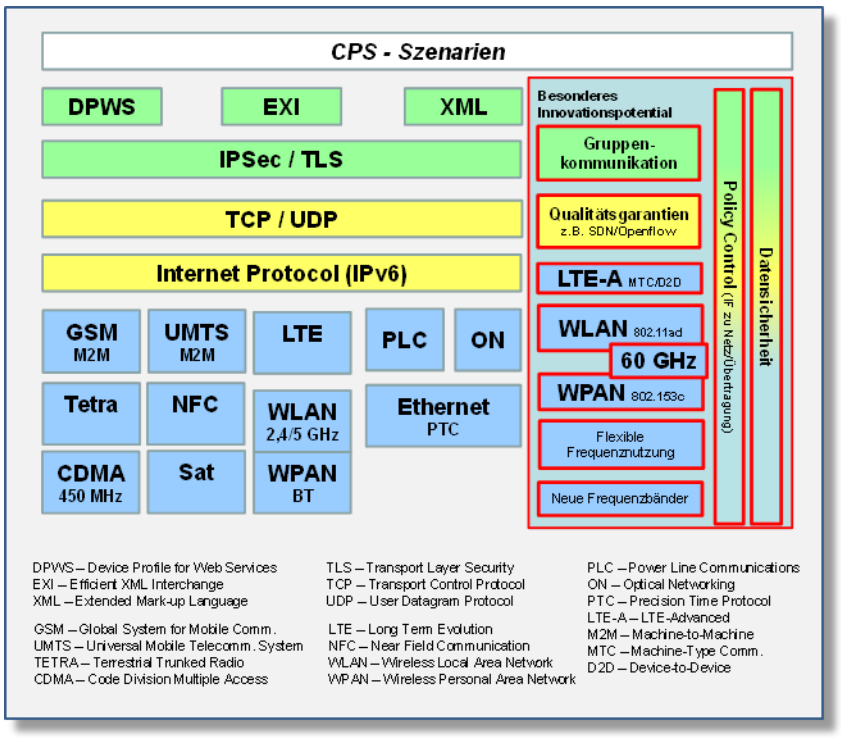

Abbildung 3: Ausgewählte Lösungskomponenten und Bereiche mit besonderem Innovationspotential

Nachfolgend werden zunächst aktuelle Entwicklungstrends diskutiert, um danach besonders relevante Forschungsfelder zu identifizieren.

ETHERNET DURCHDRINGT ALLE BEREICHE DER DRAHTGEBUNDENEN, LOKALEN VERNETZUNG

Hinsichtlich der physikalischen **Übertragungstechnik** wurde in der Vergangenheit für Systeme, die als Vorformen von CPS betrachtet werden können, vollständig neue, industriesparten-spezifische Lösungen definiert und eingeführt. Seit einigen Jahren lässt sich allerdings beobachten, dass die verschiedenen Ethernet-Ausprägungen ausgehend von der Verbreitung im IT-Bereich zunehmend auch für vernetzte Steueraufgaben mit Echtzeitanforderungen herangezogen werden [3].

FALLBEISPIEL: ETHERNET FÜR DIE INTERNE VERNETZUNG IM AUTOMOBIL

In der Automobiltechnik ist der sog. **CAN**-Bus (Controller Area Network) für die Vernetzung von Systemkomponenten im Automobil Stand der Technik. Die in den 1990er-Jahren als Industriestandard spezifizierte CAN-Bus-Technik erfüllt die Anforderungen nach einer Echtzeitkommunikation und abgestufter Priorisierung von Nachrichten (z.B. sicherheitskritische Nachrichten werden höher priorisiert als Nachrichten zu komfort-bezogenen Funktionen) bei gleichzeitig ressourceneffizienter Vernetzung durch ein von allen Systemkomponenten gemeinsam genutztes Kabel. Die CAN-Technik stößt allerdings angesichts der immer weiter zunehmenden Integration intelligenter Komponenten an Kapazitätsgrenzen. Die Nachfolgetechnik **Flexray**-Technik setzt sich allerdings bisher nur zögerlich durch (siehe Abbildung 4). Denn auch bei der Vernetzung des Systems Automobil wird heute zunehmend **Ethernet**technik eingesetzt [4]. Während die Ethernettechnik zunächst dazu dient, den für die Multimediadaten genutzten **MOST**-Bus zu ersetzen, werden die breitbandigen Übertragungsmöglichkeiten zunehmend auch für bildbasierte Assistenzsysteme genutzt [5]. Auch wenn es zu früh ist, von einer Ablösung spezifischer Bussysteme zu sprechen, so ist die immer weitergehende Nutzung der **Ethernet**technik, die um Echtzeitfähigkeit und Priorisierungsmöglichkeiten erweitert wurde,

aktuell ein wichtiger Trend in der Automobilindustrie und in vielen weiteren Industriezweigen.

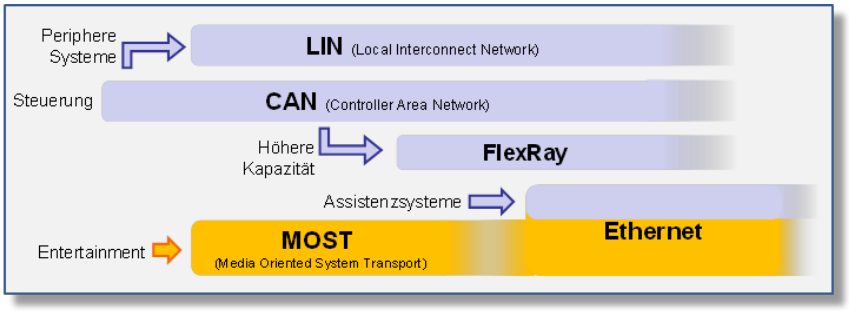

Abbildung 4: Entwicklungstrend in Richtung Ethernet am Beispiel „Automobile Bussysteme“

ETHERNET BEREITS HEUTE STANDARD IN ENERGIENETZEN

Der für die **Vernetzung von Unterstationen** in Energienetzen entwickelte **IEC 61850 Standard** ist ein Beispiel für ein Vernetzungskonzept, welches bereits die Ethernettechnik als Übertragungsstandard nutzt. Um den Anforderungen der Echtzeitfähigkeit gerecht zu werden, wurden **anwendungsspezifische Dienste** definiert, die direkt auf den Ethernetstandard aufsetzen und damit auf standardisierte Netzprotokolle über die Basisfunktionen des Ethernets hinaus verzichten [6]. Für weitere Dienste, die eine komplexere Vernetzung erfordern, wurde hingegen **TCP/IP** für eine gesicherte Übertragung über das Netz genutzt. Die Aspekte der Vernetzung zukünftiger, auf regenerativen Energiequellen aufbauenden Energienetzen wird in einem eigenen Kapitel detailliert beleuchtet.

Diese beispielhaften Entwicklungen unterstreichen, dass für die echtzeitfähige, drahtgebundene, lokale Vernetzung vor allem Techniken der **Ethernetfamilie** (IEEE 802.3 Standards und Erweiterungen zur Gewährleistung der Echtzeitfähigkeit, wie z.B. Time-Triggered Ethernet [3]) als wesentlicher Stand der Technik für CPS angenommen werden kann.

WEITERE ENTWICKLUNGSTRENDS IM BEREICH DRAHTGEBUNDENER VERNETZUNGS-TECHNIKEN

Für besondere Anforderungen sind weitere drahtgebundene Übertragungstechniken verfügbar:

- **Glasfasertechnik** ermöglicht sehr hohe Datenraten bei hoher Energieeffizienz und ist im Kernnetz des Festnetzes Standard.

Weiterhin können besondere Anforderungen hinsichtlich der elektromagnetischen Verträglichkeit oder bezüglich des Explosionsschutzes erfüllt werden.

- Zur Überbrückung der „letzten Meile“ ist im Zugangsnetzbereich die klassische **Kupfertechnik** mit verschiedenen **DSL**-Evolutionsstufen im Einsatz. Die Einführung der Vectoring-Technik eröffnet neue Wege, um die Kapazität dieser existierenden Infrastruktur nochmals deutlich zu steigern.
- Für an das Stromnetz angebundene, statische Systeme ist die drahtgeführte **Kommunikation über Stromkabel** (Power Line Communications) eine interessante Variante, hierbei ist neben proprietären Systemen speziell der HomePlug Industriestandard von Bedeutung. Aufgrund von Interferenzproblemen zwischen PLC-Systemen und des Störpotentials von Schaltvorgängen im Stromnetz bleibt die aktuelle Verbreitung von PLC-Systemen außerhalb der Vernetzung in Bestandsimmobilien im Vergleich zu Technologiealternativen zurück.
- **Bus- und Verkabelungstechniken** mit besonderen Formfaktoren (z. B. *Wiretape*) spielen z.B. in der Gebäudevernetzung eine Rolle.

Zusammenfassend ist eine weitere Konsolidierung unterschiedlichster drahtgebundener Vernetzungstechniken unter dem Schirm „Ethernet“ zu erwarten. In der Anpassung der Ethernettechnik an bisher nicht erschlossene Bereiche liegt daher ein besonderes Innovationspotential.

CPS-SPEZIFISCHER INNOVATIONSBEDARF **DRAHTGEBUNDENE VERNETZUNGSTECHNIK:**

- ↗ Ethernet-basierte Vernetzungstechnik mit extremen Formfaktoren
- ↗ Hoch Energie-effziente Ethernetvernetzung
- ↗ Ausfallsichere Vernetzung durch redundante Übertragungskanäle
- ↗ Gewährleistung von Echtzeitgarantien in Überlastsituationen

LOKALE FUNKTECHNIK DOMINIERT VON IEEE 802-FAMILIE

Gegenüber der zuvor angesprochenen Ethernettechnik bieten Funksysteme den entscheidenden Vorteil einer großen Flexibilität beim Netzaufbau und der Unterstützung von mobilen Systemen. Nachfolgend werden zunächst lokale Funktechniken betrachtet, während die Techniken der Weitverkehrsvernetzung in dem darauffolgenden Abschnitt beleuchtet werden.

VIELFÄLTIGE LÖSUNGEN ZUR ADRESSIERUNG UNTERSCHIEDLICHER ANFORDERUNGEN

Im **lokalen Bereich** dominieren Systeme der IEEE 802-Familie, wobei folgende Standards hervorgehoben werden können:

- Drahtlose lokale Netze gemäß dem **IEEE 802.11-Standard** (*Wireless Local Area Networks*), wie insbesondere:
  - 802.11e: Erweiterungen für Priorisierungsmechanismen und Echtzeitfähigkeit
  - 802.11n: aktuellster Standard für IT-Umgebungen mit ca. 300 Mbit/s
  - 802.11ac: 1 Gbit/s-WLAN im ISM-Band
  - 802.11ad: 7 Gbit/s-WLAN (bei 60 GHz)
  - 802.11p: direkte Kommunikation zwischen Fahrzeugen im Straßenverkehr (*Vehicle-to-Vehicle*)
- Drahtloser Nahbereichsfunk gemäß verschiedenen **IEEE 802.15-Ausprägungen** (Wireless Personal Area Networks), wie insbesondere:
  - 802.15.4: Basistechnik für zahlreiche, funkbasierte Steuernetze, wie *Zigbee, WirelessHART, WiSUN*
  - 802.14.5: Bluetooth, mit Erweiterung: *Low Energy Profile*
  - 802.14.3: Wireless USB (Ultra Wide Band)
  - 802.15.3c: 2 Gbit/s WPAN bei 60 GHz

In Tabelle 2 wird die Erfüllung von CPS-Anforderungskriterien von Ethernet, WLAN und WPAN im Überblick qualitativ bewertet. Dabei zeigen sich Gemeinsamkeiten, aber auch die spezifischen Eigenschaften, sodass jede Ausrichtung ihre Berechtigung innerhalb einer umfassenden Kommunikationsarchitektur für CPS erhält:

- Ethernet ist zuverlässig, robust und bietet hohe Datenraten, kommt aber nur für nicht mobile Szenarien in Frage, z.B. im Energiesektor.
- Die funkbasierten Techniken punkten bei der Flexibilität und Mehrwertdiensten (wie Lokalisierung), haben aber naturgemäß Schwächen bei der Zuverlässigkeit, wodurch bereits der Innovationsbedarf angezeigt wird.
- Extreme Formfaktoren und niedriger Energiebedarf bis hin zur autarken Energieversorgung mittels *Energy Harvesting* können besonders gut von WPAN-Techniken bedient werden.

Durch die Integration in Mobiltelefone ist Bluetooth heute eine besonders weit verbreitet WPAN-Technik (Stückzahl: 2 Mrd. pro Jahr). Mit der Erweiterung Bluetooth *Low Energy Profile* ist es gelungen, das Defizit hinsichtlich der Energieeffizienz gegenüber den *Zigbee*-Systemen weitgehend zu kompensieren. Durch die *WirelessHART*-Technik wird z.B. die Anforderung nach Echtzeitfähigkeit für IEEE 802.15.4 basierte Systeme adressiert.

Vergangene Versuche, die Dominanz der IEEE-Systemstandards im Bereich der lokalen Funksysteme durch alternative Ansätze zu brechen, sind im Bereich der lokalen Vernetzungstechniken wenig erfolgreich geblieben bzw. gescheitert (siehe z.B. HiperLAN). Insofern ist es für die zukünftige Entwicklung unerlässlich, die Entwicklung der IEEE 802-Standardfamilie eng zu verfolgen und frühzeitig zu prüfen, ob und in welcher Form Innovationen dort direkt verankert werden können (vgl. Bluetooth Low Energy Profile) oder über unabhängige Erweiterungen Mehrwert geschaffen werden kann (vgl. WirelessHART).

CPS Kriterium	Ethernet	WLAN	WPAN
Hohe Interoperabilität	●	●	●
Verteilte Kommunikation	◔ (Einschränkungen durch Kabelführung)	● (Mesh-Funktionen)	● (Mesh-Funktionen)
Hohe Zuverlässigkeit und Robustheit	●(◔) (abgeschirmte Kabel, ausgenommen Überlast)	◐ (unlizensiertes Band, stark abhängig von Umgebung)	◔ (teilweise Betrieb in spezialisierten Funkspektren)
Hohe Sicherheit	●	◔ (○) Problem Fehlkonfiguration	◔ (○) Problem Fehlkonfiguration
Echtzeitfähigkeit	◔ - ● (lastabhängig)	◔ - ● (lastabhängig)	◔ - ● (lastabhängig)
Große Anzahl der Knoten	◔	◐	◔
Lückenlose Abdeckung	○ (Einschränkungen durch Kabelführung)	◐ (Dämpfung in Gebäuden)	◐-◔ (Niedrige Frequenzen verfügbar)
Große räumliche Ausdehnung	◔ Km	◐ Einzeln bis ca. 200 m, bei Multihop km	◐ Einzeln bis ca. 200 m bei Multihop km
Priorisierung einzelner Nachrichten	◐ nur für Erweiterungen	◐ nur für Erweiterungen	◐ nur für Erweiterungen
Langer Lebenszyklus	◔	◐	◔
Extreme Formfaktoren	◔	◐	◔
Hohe Mobilität	○	●	◔
Sehr große Datenmengen	●	◔-●	◔-●
Niedriger Energiebedarf	◔	◔	●
Niedriger Spektrumsbedarf	●	◐	◔
Mehrwertdienste	○	◐ (Lokalisierung)	● (Lokalisierung)

Tabelle 2: Vergleich lokaler Vernetzungstechniken im Hinblick auf CPS-Anforderungen

Neben den IEEE 802 Systemen existieren eine Reihe von spezialisierten Funktechniken, die für **Mess- und Steuer-anwendungen** genutzt werden, z.B. Wireless M-Bus.

FUNKBASIERTE OBJEKTCHARAKTERISIERUNG

Besonders erwähnenswert und relevant für CPS sind weiterhin Nahbereichsfunktechniken, die im Rahmen der ISO für den Bereich der Logistik und des elektronischen Bezahlens zur drahtlos auslesbaren **Charakterisierung von Objekten** standardisiert wurden:

- **RFID** (Radio Frequency Identification): primär Kennzeichnung von Waren zur Automatisierung von Logistiksystemen (ISO 18000)
- **NFC** (Near Field Communication): Austausch von größeren Datenmengen über sehr kurze Entfernungen, z.B. für Bezahlsysteme (ISO 18092)

Durch die hier eingesetzte Transpondertechnik entfällt die Notwendigkeit einer Energieversorgung für die gekennzeichneten Objekte. Da die NFC-Technik vom Formfaktor und Energiebedarf her der RFID-Technik am nächsten kommt, gleichzeitig aber

deutlich größere Datenmengen übertragen werden können, kann die NFC-Technik auch zur komplexeren Charakterisierung von Objekten herangezogen werden.

NEUE FREQUENZBEREICHE ERMÖGLICHEN GBIT-ÜBERTRAGUNG

Während die bisher angesprochenen Systeme vor allem im 400/800 MHz bzw. 2,4/5 GHz-Bereich betrieben werden, ist die **Nutzung noch nicht belegter bzw. neu zugewiesener Frequenzbänder für CPS** von besonderem Interesse. Zu nennen sind hier zum einen Frequenzbänder im niedrigeren MHz-Bereich (169 MHz), da hier die Reichweite bei sehr niedrigen Sendeleistungen durch reduzierte Freiraumdämpfung und bessere Durchdringung von Wänden von Vorteil ist. Andererseits sind die Bandbreite (und damit die Datenrate) niedrig und die Interferenz bei dicht besetzten Netzen eine Herausforderung. Bei den für das **60 GHz-Band** konzipierten Systemen (z. B. 802.11ad, 802.15.3c) stehen hingegen sehr hohe Datenraten und die Möglichkeit der parallelen Nutzung des Spektrums in geringen räumlichen Abständen im Vordergrund. Diese Systeme befinden sich aktuell noch in der Entwicklung und bieten daher unmittelbares Innovationspotential.

MEHRWERTDIENST: FUNKBASIERTE LOKALISIERUNG

Für in ihrem physikalischen Aufbau fortlaufend dynamisch veränderliche CPS (Verkehr, Logistik, Produktion, Medizin, etc.) spielt die zuverlässige Lokalisierung der Komponenten eine sehr wichtige Rolle, um die Wechselwirkung der Komponenten steuern zu können. Hierfür kann eine Vielzahl von Technologieansätzen zum Einsatz kommen (z.B. Kamerasysteme). Aus Kostengründen und aufgrund der Robustheit in schmutzbehafteten Umgebungen ist die integrierte funkbasierte Kommunikation und Lokalisierung eine attraktive Lösung. WPAN-Systeme bieten entsprechende Erweiterungen zur Unterstützung von ToA-Verfahren an (z.B. IEEE 802.15.4a). Durch die Nachbearbeitung der Rohdaten können auch in „funkfeindlicher“ Umgebung mittlere Positionierungsfehler im Bereich weniger 10 cm erzielt werden [7]. Dennoch besteht erheblicher Forschungsbedarf, um die für eine automatisierte Steuerung von Komponenten eines CPS notwendige Genauigkeit zu erzielen.

CPS-SPEZIFISCHER INNOVATIONSBEDARF
DRAHTGEBUNDENE VERNETZUNGSTECHNIK:

Zusammenfassend lassen sich für die lokalen Funknetztechniken folgende Felder mit besonderem Innovationsbedarf identifizieren:

- Beiträge zur Entwicklung von 60 GHz-Systemen (802.11ad, 802.15.3c) und Erforschung deren Einsatzes für CPS für Kommunikation und Lokalisierung
- Identifikation von spezifischen Frequenzbändern für CPS und Untersuchung neuartiger Frequenznutzungskonzepte
- Konzepte für die Modifikation/Erweiterung der WLAN/WPAN-Techniken für eine hochrobuste Übertragung, z.B. mittels modifizierter Kodierung, Frequency Hopping, Meshing, Carrier Aggregation, etc.
- Neuartige Policy-Mechanismen zur Steuerung der Interferenzen zwischen konkurrierenden Diensten und Systemen in gemeinsam genutzten Frequenzbändern

LTE: UNIVERSALER MOBILFUNKSTANDARD AUCH FÜR SPEZIALISIERTE ANWENDUNGEN

Der Bereich des Mobilfunks hat in den letzten 20 Jahren eine außergewöhnliche Entwicklung genommen. Technologisch gesehen ist dabei die Entwicklung über mehrere Generationen der eingesetzten Systemtechnik von Relevanz:

- GSM: Systeme der zweiten Generation, heute weltweit über 5+ Mrd. Verträge
- UMTS: Systeme der dritten Generation, heute weltweit über 1+ Mrd. Verträge
- LTE: Systeme der vierten Generation, heute weltweit 100+ Mill. Verträge, aktuell im Aufbau [1]

[1] Quelle für Marktdaten: http://www.gsacom.com/news/statistics (zuletzt besucht am 2.11.2013)

Aus Sicht der CPS sind insbesondere die Datendienste für die Kommunikation zwischen intelligenten Systemkomponenten von besonderem Interesse (*Machine-to-Machine M2M Communications*, oder auch neuerdings *Machine-Type-Communications MTC*).

M2M-DIENSTE ÜBER GPRS UND UMTS

Basierend auf dem packet-orientierten Datendienst *General Packet Radio Service* (GPRS) des GSM-Systems sind vielfältige M2M-Anwendungen realisiert worden. Spezifische Hardware (wie sog. *Wireless Modules oder Form Factor SIMs*) erleichtern die Realisierung. Für viele weiträumige Mess- und Steueraufgaben sind die über GPRS zur Verfügung stehenden Datenraten vollkommen ausreichend. Einschränkungen bestehen bei der Echtzeitfähigkeit (die Verzögerung liegt im Sekundenbereich) sowie in Kapazitätsgrenzen des Mobilfunksystems. Hier bietet das direkte Nachfolgesystem UMTS keine entscheidenden Vorteile (bei höheren Hardwarekosten), sodass heute GPRS für viele Anwendungen (z. B. Smart Metering) der Stand der Technik ist. Da sich der Lebenszyklus des GSM-Systems mittelfristig zu Ende neigt, besteht auch

für die etablierten M2M-Anwendungen ein Bedarf, langfristig verfügbare, neue Lösungen zu finden. Hierbei steht die LTE-Technik im Fokus, da diese mit einem Zeithorizont von 20-25 Jahren verfügbar sein wird und sich zusätzlich aufgrund von deutlich kürzeren Antwortzeiten (im 100 ms-Bereich) auch für Anwendungen mit verstärktem Echtzeitanforderungen eignet (z.B. für Schutz- und Leitfunktionen in Energiesystemen [8]).

MACHINE-TYPE COMMUNICATION FÜR LTE AKTUELLES FUE-THEMA

Die Entwicklung der LTE-Netze wurde auf die Unterstützung sehr hoher Datenraten einzelner Benutzer optimiert. Dies wird insbesondere durch die schlanke Signalisierung ermöglicht. Es können z.B. „nur“ zehn Benutzer zur exakt gleichen Zeit [9] (man spricht hier von einem Subframe) Daten senden bzw. empfangen (Datenrate von einigen MBit/s). Befinden sich mehr Benutzer in einer Zelle, werden sie zeitlich nacheinander bedient.

Im Gegensatz dazu haben die CPS-typischen M2M-Anwendungen in vielen Fällen (auch im Smart Grid Kontext [10]) deutlich andere Anforderungen an das Kommunikationsnetz. Es sollen häufig nur geringe Datenmengen, welche eine geringe Datenrate erfordern, übertragen werden. Dies führt bei den aktuell eingeführten LTE-Systemen zu einem deutlich erhöhten Signalisierungsaufwand, sodass der Nutzdatenanteil nur noch bei ca. 37% liegt. Bis zu 63% der Funkressourcen werden für die Signalisierung verwendet.

Bei Szenarien mit sehr vielen M2M Endgeräten (einige Tausend Endgeräte, welche pro Sekunden aktiv werden wollen) kann auch die Anmeldeprozedur bei der Zelle (man spricht hier von Zufallszugriff bzw. Random Access) ein Engpass werden [11]. Deshalb wird im Moment intensiv an der Weiterentwicklung von LTE zur besseren Unterstützung von M2M Anwendungen gearbeitet (z. B. lokale Datenaggregation mehrere M2M-Endgeräte, vereinfachter Kanalzugriff nur zu bestimmten Zeitintervallen [12] oder Berücksichtigung der Funkkanaleigenschaften bei der Übertragung von zeitunkritischen Daten [13]). Dabei geht es insbesondere um die Unterstützung sehr vieler Teilnehmer in einer Zelle ohne signifikante Beeinträchtigung „klassischer“ Mobilfunkteilnehmer. Außerdem steht die Entwicklung kostengünstiger Endgeräte (sogenannte *Low Cost MTC User Equipment*) im Vordergrund der Forschung und Standardisierung [14].

M2M-Endgeräte könnten mit deutlich geringerem Funktionsumfang bezüglich des Funkmoduls ausgestattet werden: z. B. Verringerung der Sendeleistung oder Unterstützung einer geringen maximalen Bandbreite (z. B. nur 1,4 MHz im Gegensatz zu 20 MHz), was zu einer geringen maximalen Datenrate führt.

Neben einem Redesign der LTE-Funkschnittstelle für CPS-Anforderungen ist auch die Realisierung von Diensten für das LTE-CPS-Umfeld anzupassen. Das *LTE Core Network* und *IP-based Multimedia-Subsystem* (IMS) setzen durch hohe Komplexität hohe Einstiegshürden beim Aufbau von Netzinfrastrukturen und sind nicht ausgelegt auf die Steuerung einer großen Anzahl von Netzknoten. Hier ist die Entwicklung einer CPS-spezifischen Ausprägung der Signalisierung für LTE-Infrastrukturkomponenten notwendig [15].

GSM-RAIL ALS MUSTER FÜR CPS-SPEZIFISCHE LTE NETZE?

Als mögliche Referenz auch für die zukünftige Entwicklung von LTE-basierten Kommunikationsnetzen für CPS sei an dieser Stelle das ***GSM-Rail***-System hervorgehoben (siehe Abb. 5). Aufbauend auf den GSM-Standard ist seit 1997 ein europaweites, **exklusiv für die Steuerung des Bahnsystems reserviertes Mobilfunksystem** aufgebaut worden. Die funkgesteuerte Automatisierung des Bahnverkehrs wurde dabei bereits in den 1990er Jahren als so relevant erkannt, dass ein eigenes Frequenzband zugewiesen wurde. Weiterhin wurden nach den Vorgaben der Bahnbetreiber Dienste integriert, die z.B. die Überwachung und Steuerung des Bahnverkehrs ermöglichen. Durch die europaweit abgestimmte Vorgehensweise entstand ein ausreichend großer Markt für die Hersteller entsprechender Systeme. Inzwischen werden GSM-R-Systeme auch außerhalb von Europa installiert. Die Wiederverwendung einer in großen Stückzahlen eingesetzten Basistechnologie, ergänzt um Zusatzfunktionen und betrieben in geschützten Frequenzbereichen kann **als Muster für zukünftige LTE-basierte CPS Kommunikationsnetze** dienen.

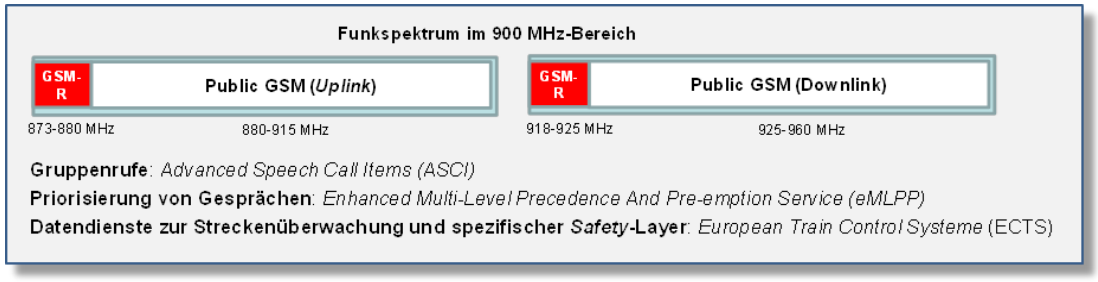

Abbildung 5: GSM-R: Kommunikationsnetz für die Bahnsteuerung

SYNERGIEN ZWISCHEN BEHÖRDENFUNK UND CPS

Ergänzend zu den öffentlichen Zellularfunksystemen sind Bündelfunksysteme nach dem **TETRA**-Standard verfügbar. Diese repräsentieren technologisch den Stand der zweiten Generation des Mobilfunks und sind im Betriebsfunk schon seit Jahren im Einsatz. Aktuell wird in Deutschland für den Behördenfunk ein bundesweites Netz auf der Basis des TETRA-Standards aufgebaut. Für zukünftige CPS sind diese Netze relevant als Rückfalloption bzw. zur Redundanzerhöhung, da sie in exklusiv zugewiesenen Frequenzbereichen operieren. Die Entwicklung zukünftiger Bündelfunksysteme wird die LTE-Technik nutzen. Hierzu sind insbesondere in den USA bereits konkrete Entwicklungen im Gange. So wurde in den USA bereits 20 MHz im 700 MHz-Band für ein LTE-basiertes Behördenfunknetz zugewiesen [16].

Eine möglicherweise gemeinsame Perspektive für Kommunikationsnetze für den Behördenfunk und CPS ergibt sich über die gemeinsame Anforderung an Gruppenkommunikationsdienste. Weiterhin erfordern sowohl der Behördenfunk wie auch das CPS-Umfeld höchste Verfügbarkeit. Eine mögliche Synergie auch in Bezug auf den Betrieb der Systeme wird in Kapitel 4 aufgezeigt.

ZELLULARFUNKALTERNATIVEN ZU LTE

Weiterhin sind **spezifische Weitbereichsfunksysteme** anzusprechen, wie z. B. die **WiMAX** oder **CDMA-450-Technik**. Diese haben einen geringeren Verbreitungsgrad als die zuvor genannten Systeme, sind jedoch aufgrund ihrer Nutzbarkeit in reservierten Frequenzbereichen von Interesse für die Realisierung von CPS. Da die LTE-Technik bereits heute für unterschiedlichste Frequenzbereiche verfügbar ist, kann davon ausgegangen werden, dass hiermit mittelfristig auch spezialisierte Frequenzbereiche bedient werden können, wenn ein ausreichender Marktbedarf vorhanden ist. Nicht-LTE-Zellularfunktechniken müssen sich daher langfristig durch z. B. besonders kostengünstigen Aufbau und Betrieb der Netze gegenüber LTE-Ansätzen behaupten.

MESH NETWORKS AUCH FÜR DAS EUROPÄISCHE UMFELD GEEIGNET?

Als Alternative zu Zellularfunknetze sind besonders in den USA, aber auch anderen Regionen vor allem außerhalb Kontinental-europas, sog. vermaschte Netze im Einsatz. Durch die direkte

Vernetzung der Kommunikationsknoten untereinander, wie z. B. *Smart Meter*, kann hierbei eine flächendeckende Versorgung schrittweise aufgebaut werden [17]. Eventuelle Lücken in der Funkversorgung werden durch Relay Knoten geschlossen. Der Übergang zu den infrastrukturseitigen Steuerungssystemen erfolgt über Gateway-Stationen. Für *Mesh Networks* werden typischerweise lizenzfreie und damit kostenfreie Funkspektren für die lokale Vernetzung eingesetzt (wie z.B. das 2,4 GHz-ISM-Band), oftmals kombiniert mit weiteren Funkbändern, die die Kommunikation über größere Entfernungen bzw. mit höheren Datenraten ermöglichen. Aufgrund des bedarfsgerechten Ausbaus der Netzabdeckung ohne den Anspruch einer vollständigen Abdeckung eines Gebiets eignet sich diese Vorgehensweise vor allem für Versorger und damit für die CPS-Ausprägung *Smart Grid* [17].

In Deutschland konnten sich Mesh Networks bisher nicht durchsetzen, da die baulichen Gegebenheiten (Stein-/Beton-Bauten, Heizung/Zähler im Keller, Versorgungsleitungen im öffentlichen Raum primär unterirdisch und nicht durch einfach zugängliche Masten) weniger geeignet sind als in anderen Bereichen. Weiterhin muss mit geringeren Sendeleistungen gearbeitet werden. Für bestimmte Lösungsansätze, die den Betrieb eines exklusiven Netzes anstreben, ist es von Interesse, diese alternativen Ansätze zu überprüfen.

SATELLITENFUNKNETZE: REDUNDANZ FÜR NOTFÄLLE

Angesichts der weitreichenden Verfügbarkeit von terrestrischen Mobilsystemen haben satellitengestützte Mobilfunksysteme heute vor allem eine Relevanz für Spezialeinsatzzwecke, wie z. B. in der Schifffahrt oder für Expeditionsvorhaben. Auch im Katastrophenschutz haben Satellitensysteme eine große Bedeutung, da sie als Rückfallposition im Falle des Ausfalls terrestrischer Systeme dienen können. Hier liegt auch der Ansatzpunkt für die Nutzung für CPS-Konzepte. Für die redundante Absicherung von Übertragungspfaden können satellitengestützte Verbindungen wertvoller Teil eines Gesamtkonzepts sein und müssen daher für die Identifikation des Innovationsbedarfs berücksichtigt werden.

CPS-SPEZIFISCHER INNOVATIONSBEDARF
MOBILFUNKTECHNIK

Zusammenfassend bietet der Bereich der Weitverkehrs-vernetzung großes Innovationspotential, insbesondere im Bereich der Weiterentwicklung der LTE-Technik

- Hoch-energieeffiziente Datenübertragung mittels LTE
- LTE-Skalierbarkeitsgrenzen ausloten und verschieben, z.B. in Bezug auf die Wechselwirkung zwischen Web/Video und CPS-Datenverkehr
- CPS-spezifische Dienste (CPS-Broadcast statt Multimedia Broadcast)
- Effiziente Gruppenkommunikation mittels *Network Coding*
- Vergleich von Mesh Network vs. Zellularfunk
- Erforschung der redundanten Absicherung von terrestrischen Mobilfunksystemen durch Satellitensysteme, hierbei z.B. notwendige Anpassungen der CPS-Steuerungsanwendungen an geringere Datenraten und höhere Verzögerungszeiten.

INTERNET GOES CPS
RESSOURCENEFFIZIENZ UND SICHERHEIT

Bei der Entwicklung der Internetprotokolle und -datenformate standen Robustheit und Erweiterbarkeit im Vordergrund, während die Dienstgütegarantien und Ressourceneffizienz weniger berücksichtigt wurden. So werden mit dem klassischen Internetprotokoll (IP) wie auch mit den Webdatenformaten (die Beschreibungssprache HTML bzw. die allgemeinere XML) die Schlagworte „*best effort*“ und „ressource hungry“ verbunden.

RESSOURCEN-EFFIZIENTE INTERNET-PROTOKOLLE UND WEB-BASIERTE DATENFORMATE

In den letzten Jahren sind aber speziell die besonderen Ressourcenbeschränkungen eingebetteter Systeme durch verschiedene Erweiterungen adressiert worden. Beispiele hierfür sind:

- IPv6 over Low power Wireless Personal Area Networks (6LOWPAN): Optimierung des IPV6-Protokolls, um die nahtlose Einbindung von Sensornetzen in IP-Infrastrukturen zu ermöglichen (RFC 4944).
- Routing Over Low Power and Lossy Networks (ROLL): Verfahren, die ein ressourceneffizientes und gleichzeitig zuverlässiges Routing über gestörte Übertragungswege unterstützen (RFC 6550).
- EXI Efficient XML Interchange (EXI): binär und damit hocheffizient kodierte Datenformate, die ein störungsfreies Zusammenspiel mit Web Services-basierten IT-Infrastrukturen ermöglicht. Anhand der Abbildung 6 wird beispielhaft der Gewinn der effizienten Kodierung für die zwischen Elektrofahrzeug und Ladeinfrastruktur übertragenen Nachrichten aufgezeigt [20].
- Device Profile for WebServices (DPWS): Adaption des im IT-Bereich weit verbreiteten Ansatzes des Service-Oriented Architecture (SOA) und der damit verbundenen Protokolle [18].

Im Bereich der Bussysteme für die industrielle Produktion sind hierbei auch die Integration der dort verbereiteten OPC (Object Linking and Embedding for Process Control) Ansätzen mit DPWS vorgestellt worden [19].

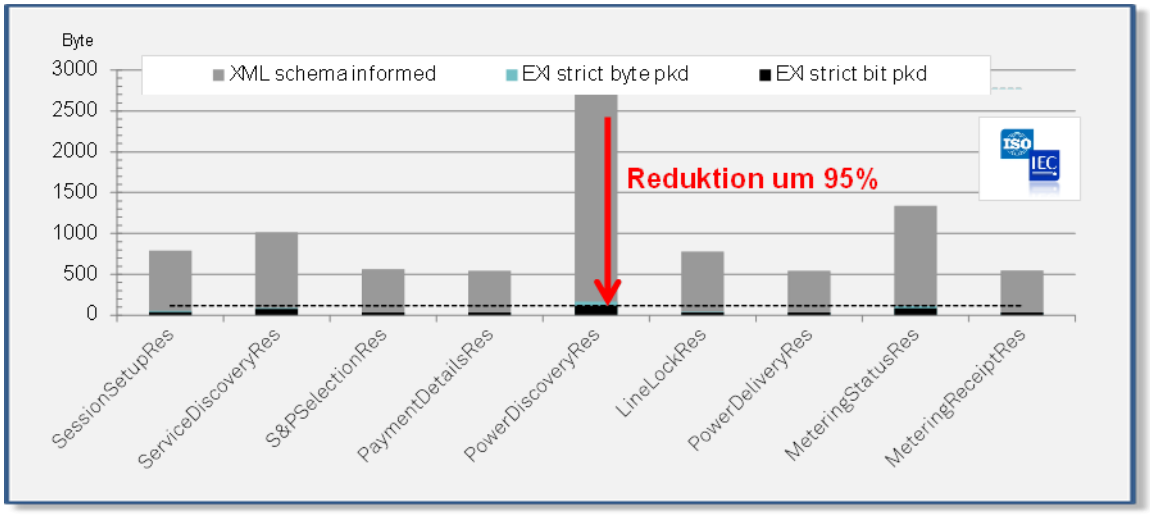

Abbildung 6: Vergleich lokaler Vernetzungstechniken im Hinblick auf CPS-Anforderungen [20]

SYSTEMÜBERGREIFENDE DATENSICHERHEITSKONZEPTE

Im Zusammenhang mit der Verwendung von Internettechniken stellt sich in besonderem Maße die Frage nach der Datensicherheit, an die durch CPS besonders hohe Anforderungen gestellt werden. Hierbei ist festzuhalten, dass im IT-Umfeld eine Reihe von erprobten Methoden und Werkzeugen, z. B. zur Authentifizierung und Verschlüsselung, zur Verfügung stehen, die eingebettet in ein konsequent umgesetztes Sicherheitskonzept und unter der Voraussetzung einer kontinuierlichen Wartung der Systeme einen weitgehenden Schutz gegenüber Angriffen gewährleisten können.

Die Forderungen nach einem sehr hohen Sicherheitsniveau können naheliegend auch durch physikalische Maßnahmen (Abschirmungen, Baumaßnahmen) befriedigt werden. Dies greift jedoch für viele CPS aufgrund der räumlichen Verteilung und hohen Mobilität zu kurz.

Für Cyber Physical Systems sind neuartige Sicherheitsmechanismen, die die physikalischen Eigenschaften miteinbeziehen, von besonderem Forschungsinteresse. So kann die gesicherte Kenntnis des Aufenthaltsorts der Systemkomponenten dazu dienen, externe Angriffe abzuwehren. Die Verknüpfung der Kommunikationswege mit weiteren CPS-Systemeigenschaften ist somit ein möglicher Ansatz, die Systeme abzusichern [30].

CPS-SPEZIFISCHER INNOVATIONSBEDARF
INTERNET DER DINGE UND DATENSICHERHEIT

Zusammenfassend ergibt sich insbesondere für systemübergreifende, die Hardware, Software und Kommunikation umfassenden Sicherheitskonzepte erhöhter Innovationsbedarf.

- Definition von CPS-spezifischer Beschreibungssprachen und deren effizienter Kodierung (z.B. CPS Mark-up Language).
- Entwicklung systemübergreifender Sicherheitskonzepte, die besondere physikalische Eigenschaften der CPS für Sicherheitsfunktionen nutzen.

REVOLUTION DES NETZBETRIEBS **SOFTWARE-DEFINED NETWORKING (SDN)**

Eine große Herausforderung für IP-basierte Netze ist die Gewährleistung von Dienstqualitätsparametern wie eine bestimmte Datenrate und/oder maximale Verzögerung. Über viele Jahre hinweg, wurden Qualitätsziele durch eine starke Überdimensionierung der Systeme adressiert, sodass die Systeme für klassische Webdienste „in der Regel akzeptable" Qualität lieferten. Dort wo für die Nutzer spürbare Engpässe erkennbar wurden, konnte durch Aufrüstung der Systeme Abhilfe geschaffen werden, oder die Nutzer mussten sich mit temporär verminderter Qualität arrangieren, so wie es in anderen Bereichen ja auch der Fall ist (siehe Straßenverkehr). Diese pragmatische Vorgehensweise stößt bei stetig steigendem Datenverkehr und immer anspruchsvolleren Diensten (z.B. IP-TV, aber auch Automatisierungsaufgaben) an Grenzen und ist auch aus technisch-wissenschaftlicher und ökonomischer Sicht nicht als dauerhafte Lösung überzeugend.

BEKANNTE LÖSUNGSANSÄTZE ZUR UMSETZUNG VON ANWENDUNGSSPEZIFISCHEN POLICIES

Daher sind in Forschung und Standardisierung verschiedene Ansätze vorgeschlagen worden, Qualitätsgarantien in den unterschiedlichen Schichten von IP-Netzen unter Einsatz verschiedener „Spielregeln", der sog. Policies, umzusetzen. Der tatsächliche Erfolg in der Umsetzung in heute für CPS verfügbare Netztechnik ist dabei sehr unterschiedlich.

- Explizite Reservierung von Ressourcen im Netz für eine spezifische Kommunikationsverbindung bzw. spezifische Netzknoten, z. B.:
  - Resource Reservation Protocol (RSVP) für IP-Router
  - Point Coordination Function (PCF) für WLAN-Systeme

  Obwohl diese Mechanismen grundsätzlich geeignet sind, Qualitätsziele zu erreichen, erfordern sie einen hohen

Organisationsaufwand und eine homogene Infrastruktur. Sie sind daher in der Breite nicht verfügbar.

- Beeinflussung der Abarbeitung von Datenpaketen in Netzknoten durch vom Sender vergebene **Prioritäten**, z. B.
  - *Differentiated Services* (IETF DiffServ) für IP-Router
  - *MAC Enhancements for Quality of Service* (IEEE 802.11e) für WLAN-Systeme

  Diese Ansätze sind mit geringerem Aufwand umsetzbar, jedoch bieten sie keine absoluten Garantien. Die erfolgreiche Umsetzung erfordert, dass ein Mix zwischen unterschiedlich priorisierten Paketen vorliegt und der Anteil der hoch priorisierten Pakete vergleichsweise gering ist im Verhältnis zur Gesamtkapazität einer Verbindung. In Kombination mit den nachfolgend beschriebenen virtuellen Netzen ist der Ansatz zunehmend in der Praxis vertreten.
- **Virtuelle Aufteilung von Netzressourcen** aus Gründen der Netzsicherheit , aber auch im Hinblick auf die Erfüllung von Qualitätsgarantien, z.B.:
- *Virtual Private Networks (VPN)* durch Nutzung VPN-spezifischer Ports von IP-Routern
- *Virtual Local Area Networks (VLAN)* für Netze auf Ethernetbasis (IEEE 802.1q)

  Die Einrichtung von VPNs ist die Standardvorgehensweise, um sichere Unternehmensnetze über öffentliche Unternehmensnetze zu betreiben. Die VLAN-Technik ist auch unter dem Aspekt der Erfüllung von Qualitätsgarantien, z.B. für die Realisierung von VoIP- oder IPTV-Diensten, heute bereits weit verbreitet. Die Nutzung und ggf. Erweiterung dieser Techniken für CPS-Systeme daher liegt nahe.

SOFTWARE-DEFINED NETWORKING MIT GAME-CHANGER-POTENTIAL?

Der entscheidende Impuls für die konkrete Realisierung einer neuen Generation von flexibel programmierbaren Netzen erfolgte über die *OpenFlow*-Initiative der Stanford University [20]. Durch die konsequente Trennung von Steuerung und Transport in den Netzknoten (*Switches*) ist es möglich, auch in komplexeren und weiträumigen Netzstrukturen Regeln für die Abarbeitung von bestimmten Datenströmen netzweit zu verankern. Standardisierte APIs für die Programmierung der Netzknoten sowie korrespondierende Informationsfelder in den *Headern* der zu

übertragenden Datenpakete sind die Grundlage hierfür. Die Begeisterung für die durch OpenFlow-Ansätze realisierbaren *Software-Defined Networks (SDN)* hat aktuell starken Hype-Charakter, sodass es sich im Hinblick auf CPS empfiehlt, die tatsächliche Leistungsfähigkeit im Verhältnis zu den Marketing-Aussagen wissenschaftlich fundiert zu überprüfen.

CPS-SPEZIFISCHER INNOVATIONSBEDARF
SOFTWARE-DEFINED NETWORKS

- Validierung der Einhaltung von QoS-Garantien mittels OpenFlow in CPS-Szenarien
- Ableitung CPS-spezifischer Policy-Konzepte für OpenFlow-basierte Netzarchitekturen
- Integration von OpenFlow-Konzepten in Mobilfunknetze

LANGFRISTIGE TECHNOLOGIEZYKLEN

Um die Kräfte zu fokussieren, besteht der größte Handlungsbedarf für Innovationen in den Bereichen, die am Anfang des Technologiezyklus stehen und daher aktuell noch beeinflussbar sind. Der Prozess bis zum tatsächlichen Durchbruch im Markt ist aber auch immer als Ausleseprozess zu verstehen, in dem sich nicht alle zunächst vielsprechenden Ansätze durchsetzen werden. Die frühzeitige, wissenschaftlich fundierte Auseinandersetzung mit sich abzeichnenden Innovationsfeldern dient dazu, von neuen Technologietrends zu profitieren bzw. bestenfalls deren Entwicklung mit zu beeinflussen.

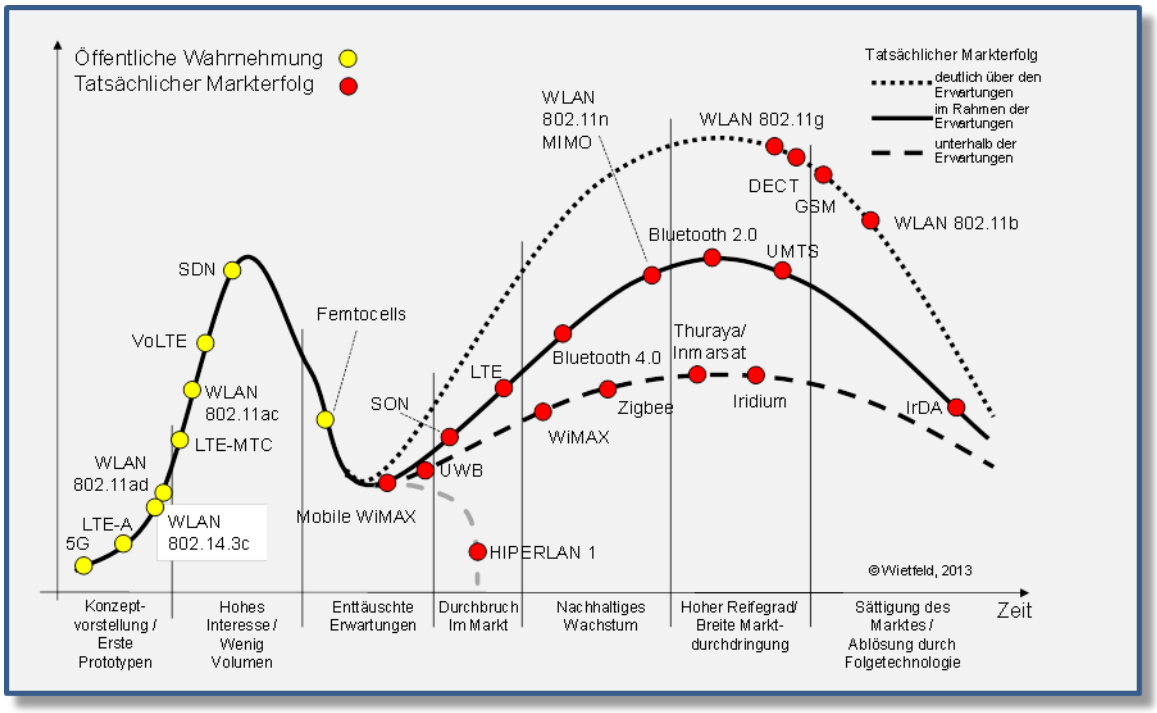

Abbildung 7: Technologiezyklus: Hype vs. Markterfolg

Abbildung 7 ordnet einen Teil der zuvor eingeführten Techniken qualitativ und bespielhaft in einen Technologiezyklus ein, der sich am Hype-Cycle (nach Gartner) orientiert und diesen erweitert:

- Das Durchlaufen der Hype-Phase wird gekennzeichnet durch eine hohe Aufmerksamkeit in der Fachwelt (gelbe Markierung), während die Darstellung danach den tatsächlichen Markterfolg qualitativ bewertet (rote Markierung).

- Hierbei wird differenziert, inwieweit sich die Technik entsprechend den Erwartungen durchsetzt, diese unter- oder übererfüllt.

LESSONS LEARNED
IKT-TECHNOLOGIEZYKLEN FÜR DAS CPS-UMFELD

- Es bietet sich an, ggf. Technologiegeneration zu überspringen, um Zyklen zu verlängern: auf GSM folgt LTE-MTC (ohne Zwischenschritt UMTS).
- Nicht jeder technisch geeigneter Ansatz setzt sich im Markt durch: LTE überholt *Mobile WiMAX* aufgrund der Skaleneffekte des etablierten Mobilfunkmarkts.

04
SINNVOLL UND NOTWENDIG?
EXKLUSIVE NETZINFRASTRUKTUREN FÜR CYBER PHYSICAL SYSTEMS

Aufgrund der hohen Anforderungen an Kommunikations-infrastrukturen für CPS liegt es nahe, die bestmögliche Erfüllung von Qualitätszielen dann zu erwarten, wenn auf eine spezifische Netzinfrastruktur aufgebaut werden kann, in der mögliche Wechselwirkungen mit konkurrierenden Anwendungen ausgeschlossen sind.

VERFÜGBARKEIT VS. WIRTSCHAFTLICHKEIT

So betreiben Energieversorger seit Jahren eigene Glasfasernetze, die in Hochspannungsleitungen integriert sind. Auch das bereits erwähnte GSM-*Rail* ebenso wie der Behördenfunk TETRA sind Beispiele dafür, dass oft dann, wenn die Qualitätsziele Verfügbarkeit, Zuverlässigkeit und Sicherheit im Verhältnis zur Wirtschaftlichkeit besonders hoch gewichtet werden, separate Infrastrukturen umgesetzt werden. Dies kann bedeuten, dass eine moderat angepasste Standardtechnik als separate Infrastruktur betrieben wird (wie z. B. *GSM-Rail* im exklusiven Funkspektrum) oder aber sogar eine eigene Systemtechnik zum Einsatz kommt (wie bei TETRA). Durch den Aufbau von separaten Netzinfrastrukturen kann auch die Wechselwirkung zwischen den Kommunikationsnetzen und den kritischen Infrastrukturen reduziert werden, z.B. durch eine autarke Stromversorgung, die z. B. Ausfälle des Stromnetzes zumindest für einen gewissen Zeitraum überbrücken kann.

Je mehr Wirtschaftlichkeitsüberlegungen mit ins Spiel kommen, das Anforderungsprofil keine Echtzeitfähigkeit erfordert und Abstriche bei der Verfügbarkeit gemacht werden können, umso mehr werden Standardinfrastrukturen genutzt. So werden Finanztransaktionen oder auch B2B-Web Services (z. B. für das Bestellwesen) heute über öffentliche IP-basierte Infrastrukturen durchgeführt. Auch bei der Realisierung von Smart Metering Infrastrukturen wird neben der von den Betreibern installierten *PLC*-Technik auch öffentlich verfügbare Mobilfunktechnik (*GPRS*) eingesetzt.

Die für Cyber Physical Systems sehr relevanten Anforderungskriterien „Echtzeitfähigkeit“ und „Sehr hohe Verfügbarkeit“ werden aktuell durch öffentliche IP-basierte Infrastrukturen nur mit teilweise deutlichen Einschränkungen erfüllt. Insofern müssen für zukünftige CPS im Vollausbau neue Netzinfrastrukturen aufgebaut werden bzw. bestehende Netze deutlich aufgerüstet werden. Die dafür notwendige Netztechnik ist teilweise bereits verfügbar oder in der Entwicklung. Speziell die zuvor skizzierten *OpenFlow*-Schnittstellen haben generell das Potential, CPS-spezifische Anforderungen in den Netzen umsetzen zu können. Doch für die spätere Umsetzung stellt sich die wichtige Frage, ob die anspruchsvollen Qualitätsziele für CPS durch die Technik der *Software-Defined Networks* tatsächlich zuverlässig in allgemein verfügbaren Netzinfrastrukturen umgesetzt werden kann, oder ob eine Abstützung auf physikalisch unabhängige Netzinfrastrukturen sinnvoll ist.

REALISIERUNGSMODELLE FÜR DEN AUFBAU UND BETRIEB VON CPS-NETZEN IM VERGLEICH

Zugespitzt sind folgende Varianten denkbar (siehe auch Abbildungen 8 und 9):

- Variante 1: Spezifische Netzinfrastruktur für bestimmte CPS Anwendung
- Variante 2: Generische CPS-Netzinfrastruktur
- Variante 3: Virtualisierte Netzbereiche in generischen Infrastrukturen

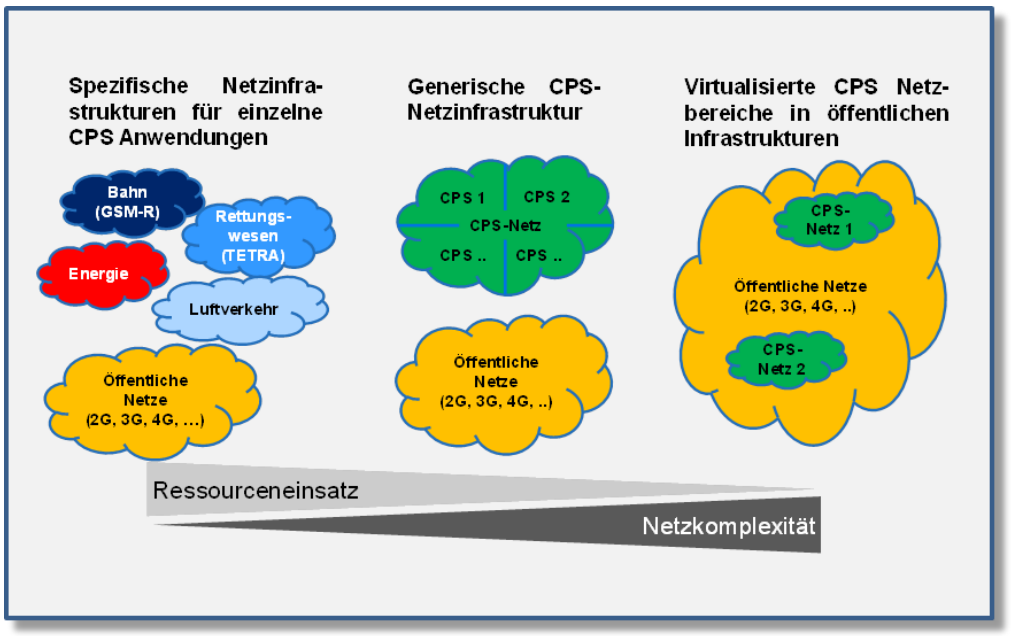

Abbildung 8: Realisierungsvarianten CPS-Netzinfrastruktur

Die Realisierung dieser drei Varianten betrifft die physikalische Netzinfrastruktur, die Steuerung der Prioritäten durch die Netztechnik und die schließlich die Dienste und Datenformate.

Der CPS-spezifische Datenaustausch unterliegt in allen drei Fällen keinen wesentlichen Einschränkungen, auch wenn die Definition von CPS-übergreifenden Diensten und Datenformaten ggf. aufwändiger und weniger flexibel sein kann.

Größere Unterschiede zeigen sich bezüglich der Auswahl der physikalischen Infrastruktur und der Steuerung von Prioritäten in der Netzebene. Die Integration von CPS-Datenübertragung in öffentlichen Netzinfrastrukturen reduziert den Ressourceneinsatz und erscheint als wirtschaftlichste Lösung. Die Komplexität der Steuerung der Netzinfrastruktur ist jedoch in diesem Fall erheblich, insbesondere muss vor dem Hintergrund unterschiedlichster Priorisierungsanforderungen sichergestellt werden, dass diese zuverlässig auch in Extremsituationen umgesetzt werden. Bei

spezifischen CPS-Netzinfrastrukturen reduzieren sich die möglichen Wechselwirkungen auf die Konkurrenz zwischen einzelnen CPS-Diensten eines CPS oder auch zwischen unterschiedlichen CPS. Eine generische CPS-Infrastruktur kann ein Kompromiss sein, der die Steuerungskomplexität reduziert, Synergien für eine wirtschaftliche Realisierung nutzt und gleichzeitig die Qualitätsziele erreicht. Es besteht erheblicher Forschungsbedarf, die verschiedenen Realisierungsvarianten hinsichtlich ihrer technischen aber auch kommerziellen Machbarkeit zu bewerten.

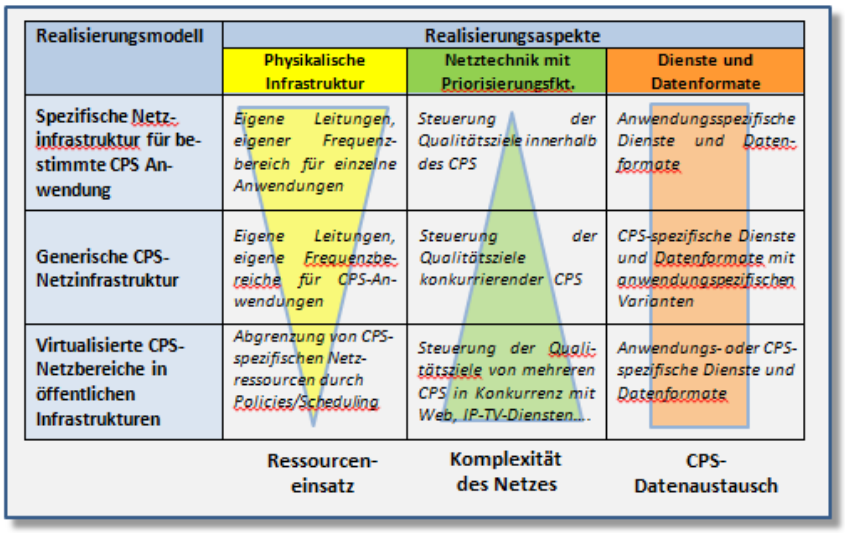

Abbildung 9: Realisierungsaspekte CPS-Netzinfrastruktur

BOS-CPS-NETZ: NUTZUNG VON SYNERGIEN ZWISCHEN CPS UND BEHÖRDENFUNK DENKBAR?

Parallel zur Erforschung CPS-spezifischer Netze besteht auch ein Innovationsbedarf in Bezug auf Kommunikationsinfrastrukturen für Behörden und Organisationen mit Sicherheitsaufgaben (BOS). Für diesen Zweck wird aktuell ein TETRA-Funknetz aufgebaut. Für die Zukunft wird eine LTE-basierte Infrastruktur konzipiert. In den USA wurde diese Entscheidung bereits getroffen und ein exklusives Funkband reserviert [16]. In Europa ist die Entwicklung noch nicht in gleichem Maße fortgeschritten. Angesichts der drängenden Fragestellung nach der Finanzierung einer BOS-spezifischen Breitbandinfrastruktur lohnt es sich darüber nachzudenken, ob Synergien zwischen CPS- und BOS-Netzen nutzbar sind. Die Anforderungen hinsichtlich der Zuverlässigkeit und Verfügbarkeit sind vergleichbar, jedoch ist im BOS-Bereich die Multimedia-Kommunikation zwischen Rettungskräften ein wichtiger Dienst, der im CPS nicht im Vordergrund steht. Ein LTE-basiertes BOS-CPS-

Netz in einem separaten Frequenzbereich könnte mehrere anstehende Probleme lösen:

- Bereitstellung eines Multi-Media-fähigen Systems für die Gefahrenabwehr und den Katastrophenschutz (TETRA Ergänzung/Nachfolge)
- Bereitstellung einer leistungsfähigen Kommunikations-infrastruktur für CPS-Szenarien in Verkehr, Energie, etc.

Auch hier besteht Forschungsbedarf hinsichtlich der Machbarkeit in technischer wie auch kommerzieller Sicht.

FORSCHUNGSBEDARF
CPS-NETZBETRIEBSMODELLE

- Aktuelle IP-Netzinfrastrukturen erfüllen die anspruchsvollen Anforderungen von CPS hinsichtlich Reaktionszeit, Verfügbarkeit und Sicherheit nicht vollständig.
- Entscheidend für den robusten Betrieb von CPS-Netzen ist auch die steuerbare Wechselwirkung zwischen den CPS-Netzen und den kritischen Infrastrukturen: z.B. Stromausfall darf nicht zu vollständigem CPS-Netzausfall führen.
- Der Aufbau eigener CPS-Netze sollte daher geprüft werden: insbesondere ein auf Standardtechnik aufbauendes CPS-übergreifendes Netz könnte eine technisch wie wirtschaftlich interessante Option sein.
- Mögliche Synergien zwischen dem notwendigen Ausbau einer multimediafähigen Funkunterstützung von Rettungskräften/Behörden und dem Aufbau von hochzuverlässigen CPS-Kommunikationsinfrastrukturen sollten untersucht werden.

05
CPS-KOMMUNIKATIONSNETZE AM KONKRETEN BEISPIEL **VERNETZTE ENERGIESYSTEME DER ZUKUNFT**

Die Umstellung des Energiesystems zum Smart Grid bedingt einen weit reichenden Umbau des elektrischen Energiesystems. Die zunehmende räumliche Verteilung der Energieproduktionssysteme und die hohe Volatilität der regenerativen Energiequellen führen zu einem komplexen, weiträumigen Cyber Physical System mit hohem Kommunikationsbedarf [21]. Nachfolgend wird anhand von zwei Beispielen aufgezeigt, welche Lösungsansätze in der aktuellen Forschung verfolgt werden, um den Herausforderungen zu begegnen.

DAS ELEKTROFAHRZEUG IMMER ZUM RICHTIGEN ZEITPUNKT VOLLGETANKT: KOMMUNIKATIONSSTANDARDS FÜR DIE ELEKTROMOBILITÄT

Die Steuerung der Ladevorgänge von Elektrofahrzeugen erlaubt es, Ladeprozesse dem Angebot regenerativer Energiequellen anzupassen und gleichzeitig dafür zu sorgen, dass die netzseitige Ladeinfrastruktur, insbesondere das Verteilnetz, nicht durch zu viele parallele Ladevorgänge überlastet wird. Gleichzeitig wird daran geforscht, die Batterien von Elektrofahrzeugen auch als einspeisende Energiespeicher zur Abfederung von Lastspitzen zu nutzen. Diese Ziele können nur erreicht werden, wenn die Lade- und Entlade-prozesse zuverlässig mittels entsprechender Kommunikations-netze gesteuert werden (siehe Abbildung 10).

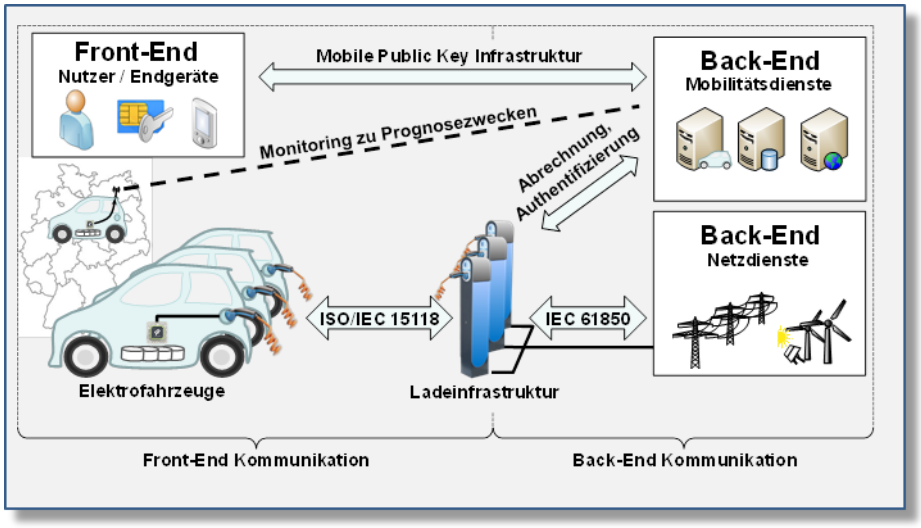

Abbildung 10: Kommunikations-schnittstellen im Umfeld der Steuerung des Elektromobilitäts-systems [24]

Hierzu wird an folgenden Lösungsansätzen in aktuellen Forschungs- und Standardisierungsprojekten gearbeitet (z. B. im NRW Kompetenzzentrum Elektromobilität Infrastruktur und -netze [22] oder im BMBF-Verbundprojekt Enterop) [23]:

Lokale Schnittstelle (Frontend) zwischen Fahrzeug und Ladesäule (IEC 15118, Vehicle2Grid Kommunikation):

- **Physikalische Übertragung mittels PLC (gemäß HomePlug Green Phy)**: Die PLC-Technik wurde aus verschiedenen Varianten ausgewählt, weil sie weder zusätzliche Leitungen im Ladekabel noch eine von den Fahrzeugherstellern unerwünschte Funkübertragung erfordert. Die Abstützung auf den Industriestandard HomePlug Green Phy erlaubt eine kostengünstige Realisierung.
- **Gesicherte Datenübertragung mittels TCP/IP**: Da keine extrem kurzen Reaktionszeiten gefordert sind, konnten Standardprotokolle verwendet werden.

- **Optimierte Web-basierte Datenformate**: Da die Steuerung des individuellen Ladeprozesses in weiträumige, Web Services-basierte IT-Systeme integriert werden muss (z. B. zur Durchführung von Bezahlvorgängen), sollte der Datenaustausch konform zu Web Services erfolgen. Gleichzeitig soll der Speicherverbrauch optimiert werden, sodass die **binäre XML-Kodierung** (EXI Efficient XML Interchange) eingesetzt wird. In Vergleichen der TU Dortmund konnte ein signifikanter Effizienzgewinn nachgewiesen werden. In ähnlicher Form wurden weitere, ressourceneffiziente Anpassungen der Web Services Standards vorgenommen [24].

Einbindung der Elektrofahrzeuge in das automatisierte Energienetz (Backend):

- Durch den IEC 61850 Standard für die Automatisierung von Unterstationen ist bereits die Komponente einer *Distributed Energy Resource* (DER) vorgegeben, die als Basis für die Modellierung eines Elektrofahrzeugs herangezogen werden kann.
- Um neben dem Automatisierungsaspekt (wann wird wieviel geladen?) die Einbindung in IT-Systeme (wer bezahlt wieviel?) möglichst nahtlos zu realisieren, wurde aktuell eine Web Services-basierte Realisierung der IEC 61850 Dienste und Datenformate vorgeschlagen und in der internationalen Standardisierung verfolgt [25].

LESSONS LEARNED
CPS-AUSPRÄGUNG ELEKTROMOBILITÄT

- ↗ Die aktuell international starke Position deutscher und insbesondere nordrhein-westfälischer Unternehmen und Universitäten im Bereich Elektromobilität (ISO/IEC 15118) und Distributed Energy Resources (IEC 61850) sollte ausgebaut werden, auch wenn sich der Markt für Elektro-mobilität langsamer als zunächst erwartet entwickelt.
- ↗ Der Einsatz von Web Services für eingebettete Devices kann weit über den Bereich der Elektromobilität hinaus Verwendung finden.

ZUVERLÄSSIGER SCHUTZ VOR BLACKOUTS DURCH ECHTZEITFÄHIGE KOMMUNIKATION IM SMART GRID

Für Energienetze existieren bereits umfangreiche Standards zur Überwachung der Stabilität des Energiesystems (*Wide Area Monitoring of Power Systems WAMPS*). Unter anderem im Rahmen der an der TU Dortmund angesiedelten DFG-Forschergruppe 1511 [26] wird aktuell unter anderem untersucht, ob diese und weiterführende Schutzdienste über Kommunikationsnetze realisiert werden können (auch *Wide Area Monitoring, Protection and Control WAMPAC*):

- Hierzu wird zum einen an neuartigen Methoden gearbeitet, um mit Hilfe einer neuartigen Hybridsimulation [27] die Wechselwirkung zwischen Energiesystem und Kommunikationsnetzen zu untersuchen (siehe Abb. 11) Die hierbei notwendige Verknüpfung und Synchronisation zwischen unterschiedlichen Simulatoren wird durch Einsatz der HLA-Technik (High Level Architecture) erreicht.
- Weiterhin wird anhand der im IEC 61850 Standard vorgeschlagenen Dienste erforscht, inwieweit Echtzeitschranken über unterschiedliche Netztopologien des Kommunikationssystems übertragen werden können. Hierbei kommen simulative Techniken wie auch analytische Techniken (Network Calculus) zum Einsatz.

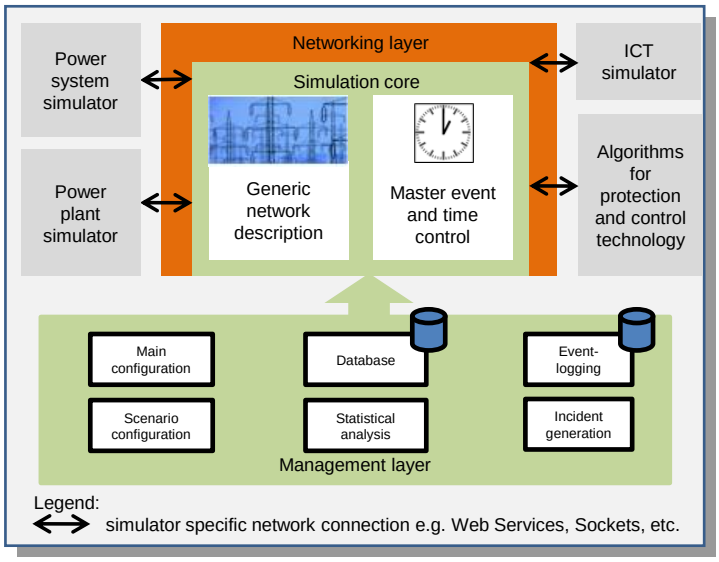

Abbildung 11: Hybridsimulation Energie/Kommunikation [27]

Im Rahmen des Forschungsprojekts SmartC2Net [28] wird die Wechselwirkung zwischen den Regelkreisen der energietechnischen Systeme und darunter liegenden Kommunikationsnetze erforscht. Dabei wird angestrebt, dass die

Kommunikationsnetze über einen „Inneren Regelkreis“ zunächst anstreben, die Qualitätskriterien der energietechnischen Steuerungsalgorithmen („Äußerer Regelkreis“) vollständig zu erfüllen (siehe Abbildung 12). In Extremsituationen, wie z. B. dem Ausfall von Teilen des Energienetzes, die wiederum Ausfälle der Kommunikationsinfrastruktur zur Folge haben können, ist eine Wechselwirkung zwischen den Regelkreisen erforderlich: Signalisiert der „Innere Regelkreis“ die Nichterfüllbarkeit von QoS-Kriterien des Kommunikationssystems, fällt der „Äußere Regelkreis“ auf reduzierte Steuerungsalgorithmen zurück, die auch mit begrenzten Kommunikationsmöglichkeiten Schäden vom Energienetz abwenden können.

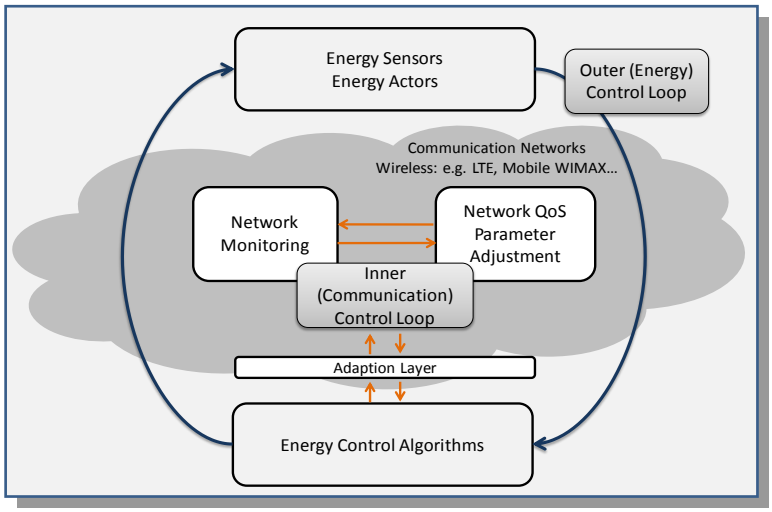

Abbildung 12: Wechselwirkung der Regelkreise von Energienetz und Kommunikationsnetz [28]

Weil über deutsche oder europäische Netze keine Referenzdaten vorliegen, stützen sich diese Forschungsarbeiten der Forschergruppe wie auch des EU-Projekts SmartC2Net auf ein amerikanisches Referenzmodell (New England Test System) ab. Hier besteht ein Bedarf für ein Referenzsystem, dass die Rahmenbedingungen Europas und speziell Deutschlands besser Rechnung trägt.

LESSENS LEARNED
CPS-AUSPRÄGUNG SMART GRID

Die im Bereich der Smart Grid Forschung eingesetzte Ansatz der Hybridsimulation zur Analyse der Wechselwirkung der verschiedenen Komponenten eines CPS sollte weiterentwickelt und auf andere CPS-Ausprägungen übertragen werden.

06
GRENZENLOSE MÖGLICHKEITEN
WIE DER KOMMUNIKATIONS-BEDARF FÜR WEITERE CPS GESTILLT WERDEN MUSS

Nachfolgend werden über die im vorhergehenden Kapitel ausführlich beleuchteten Energiesysteme hinaus weitere konkrete Beispiele für spezifische Forschungs- bzw. Innovationsprojekte zur Vernetzung von Cyber Physical Systems angesprochen.

VERNETZTE LOGISTIKPROZESSE

Unter dem Stichwort ***Internet der Dinge*** in Kombination mit ***Zellularen Transportsystemen*** werden im Logistikspitzencluster in verschiedenen Forschungsprojekten neuartige Logistikprozesse entwickelt. Als Beispiel sei hier der **inBin** [29] benannt, ein vom Fraunhofer IML entwickelter, intelligenter Logistikbehälter, der seinen Inhalt kennt und energieautark mit der Umwelt kommuniziert. So wird die Voraussetzung für eine verteilte, selbstorganisierende Logistik der Zukunft geschaffen. Die Herausforderung hinsichtlich der Vernetzung liegen in der extrem hohen Dichte der Kommunikationsknoten, den dynamisch veränderlichen Funkfeldbedingungen und der sehr hohen Anforderungen an die Energieeffizienz.

VERNETZTE SERVICEROBOTIK

Serviceroboter können in der Produktion wie auch in anderen Bereichen, wie der Landwirtschaft, dem Gesundheitswesen oder der Telekommunikation zum Einsatz kommen. Durch das koordinierte Agieren in Gruppen oder einem Schwarm kann die Effizienz des Einsatzes gesteigert werden. Zwingende Voraussetzung ist eine hochzuverlässige, drahtlose Kommunikation in einem hochdynamischen Umfeld. Ein Beispiel aktueller Forschung in diesem Bereich ist die flexible Bereitstellung von fliegenden Funkstationen im NRW-Hightech-Projekt **AVIGLE** [30], die in Katastropheneinsätzen, wie z.B. Hochwasser, selbst-organisierend eine Funkversorgung für die Helfer und unterstützende Sensoren aufbaut.

VERNETZTE VERKEHRSSYSTEME

Im Projekt **SIM-TD** [31] wurde auf breiter Basis die Kommunikation zwischen Fahrzeugen (*Car-to-Car*) und zwischen Fahrzeugen und der Infrastruktur (*Car-to-Infrastructure*) auf der Basis verfügbarer Technik demonstriert. Im von der DFG geförderten **SFB 876** [32] wird speziell die effiziente Übertragung von *extended-Floating-Car-Data* (eFCD) über LTE-Netze erforscht, wobei die Minimierung der Wechselwirkung zwischen dem „normalen“ Telekommunikationsverkehr (*Human-to-Human/Web*) und dem *Machine-Type-Communication-Verkehr* im Vordergrund steht. Im Projekt „**FFWS** (Falschfahrerwarnsystem)“ [33] wird hingegen auf das Konzept der „intelligenten Straße“ gesetzt, in dem ein funkbasiertes System mit Hilfe der Radiotomografie die Durchfahrtsrichtung mittels energieautarker Funksensorik erkennt.

VERNETZTE MEDIZINSYSTEME

Im Forschungsprojekt **smartOR** [34] wird beispielsweise eine Kommunikationsarchitektur erforscht, die einen roboter-unterstützten Operationssaal mit der Möglichkeit der Telemanipulation unterstützt. Hierbei sind leistungsfähige Kommunikationssysteme im lokalen wie auch im Weitbereich erforderlich.

10 THESEN
ZUSAMMENFASSUNG UND AUSBLICK

01

Die Erforschung von effektiven Methoden zur **Umsetzung von netzweiten *Policies* zur Realisierung echtzeitfähiger und zuverlässiger IP-Netze** bietet großes Innovationspotential. Zur Umsetzung von skalierbaren Qualitätsgarantien in CPS-Netzen ist z.B. die Technik des *Software-Defined Networking* (SDN) basierend auf *OpenFlow*-Standards sehr vielversprechend.

02

Die Entwicklung **ressourceneffizienter Anpassungen von Internetprotokollen und -datenformaten** ist in einigen Bereichen schon fortgeschritten. Die aktuell auch international sichtbare Stärke NRWs in Teilsegmenten (z. B. eingebettete *Web Services* in für Energienetze) sollte ausgebaut und für andere CPS-Bereiche genutzt werden.

03

Die LTE-Technik entwickelt sich zum Standard der Weitbereichsmobilkommunikation auch für spezialisierte Anwendungen. In der Erforschung von CPS-spezifischen Anpassungen und Erweiterungen sowohl aus Netzbetriebs- wie auch Endgerätesicht liegt ein großes Potential für deutlich **ressourceneffizientere und flexiblere LTE-basierte Lösungsansätze**, die z. B. auch die direkte Kommunikation zwischen LTE-Endgeräten unterstützen.

04

Analog zum Eisenbahnsystem (GSM-Rail) und dem Behördenfunk (TETRA) können für CPS reservierte, auf Standardtechniken wie IP und LTE Netzressourcen ein Lösungsansatz sein, um die **Wechselwirkung zwischen unterschiedlichen Nutzern** öffentlicher Netze geeignet zu steuern bzw. zu minimieren. Hierfür ist es notwendig, **technische Lösungsansätze für einen auch in**

Extremsituationen zuverlässig steuerbaren Netzbetrieb zu erforschen, miteinander zu vergleichen und gleichzeitig eine ökonomischen Bewertung durchzuführen.

05

Um **ausreichende Bandbreite** für die unterschiedlichen Hierarchieebenen der CPS-Systeme bereitstellen zu können, werden **neuartige Mehrfachnutzungskonzepte** für das knappe Funkspektrum benötigt (z. B. unter Nutzung der sog. *TV White Spaces*, d. h. lokal begrenzt verfügbare Fernsehbänder). Gleichzeitig sollte die exklusive **Reservierung spezifischer Funkbänder** für konvergente Netze für sicherheitskritische Anwendungen geprüft werden

06

Neuartige **Funksysteme im 60 GHz-Bereich** können die für CPS notwendige zuverlässige, lokale Kommunikation mit hochgenauer Lokalisierung integrieren. Hierzu müssen robuste und gleichzeitig kostengünstige Kommunikationslösungen erforscht werden, die in effizienter Form Hardware und Software-basierte Komponenten kombinieren (z. B. innovative Antennentechnik mit verteilten Datenanalyseverfahren).

07

Durch den rasanten Fortschritt im LTE-Bereich liegt das Potential von alternativen funkbasierten Ansätzen in der Adressierung spezialisierter Anforderungsprofile. Speziell im Bereich der keine Mobilitätunterstützung erfordernden Versorgungsnetz-automatisierung sollte das Potential von alternativen Ansätzen (insb. ***Mesh Networks***) ausgelotet werden.

08

Die Absicherung von CPS-Infrastrukturen gegenüber Angriffen ist essentiell. Im Bereich der Netztechnik müssen hierfür **geeignete Skalierungen existierender Sicherheitsmethoden** bzw. neuartige Lösungsansätze erforscht werden, die den Ressourcen-beschränkungen gerecht werden.

09

Ethernettechniken durchdringen alle CPS-relevanten Bereiche und verdrängen spezialisierte, drahtgebundene Vernetzungslösungen. Es besteht ein Bedarf für die Erforschung von **CPSoverEthernet-Lösungen**, die z. B. extreme Formfaktoren, autarke Energieversorgung und garantierte Echtzeitfähigkeit unterstützen.

10

Die Leistungsbewertung der Kommunikationstechniken von CPS erfordert die Berücksichtigung der Wechselwirkung zwischen Kommunikationsnetz und den weiteren Komponenten des CPS. Die **Technik der Hybridsimulation**, wie sie bereits für IKT-gestützte Energiesysteme erforscht wird, sollte auch auf andere CPS-Bereiche übertragen werden.

ABKÜRZUNGSVERZEICHNIS

CPS	Cyber Physical System
CAN	Controller Area Network
CDMA	Code Division Multiple Access
DER	Distributed Energy Resource
DSL	Digital Subscriber Line
EXI	Efficient XML Interchange
GSM	Global System of Mobile Communications
HLA	High Level Architecture
HTML	HyperText Mark-up Language
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IKT	Informations- und Kommunikationstechnik
IP	Internet Protocol
IP-TV	IP-Television
ISO	International Standards Organisation
LIN	Local Interconnect Network
LTE	Long-Term Evolution
M2M	Machine-to-Machine (Communications)
MIMO	Multiple-Input-Multiple-Output
MTC	Machine-Type Communications
MOST	Media Oriented Systems Transport
OPC	Object Linking and Embedding (OLE) for Process Control
PLC	Power Line Communications
ROLL	Routing Over Low Power and Lossy Networks
SDN	Software-Defined Networking
TCP	Transport Control Protocol
TETRA	Terrestrial Trunked Radio
UMTS	Universal Mobile Telecommunication Systems

USB	Universal System Bus
V2G	Vehicle to Grid
VLAN	Virtual Local Area Networks
VoLTE	Voice over LTE
VPN	Virtual Private Networks
WAMPAC	Wide-Area Monitoring, Protection and Control
WAMPS	Wide –Area Monitoring of Power Systems
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Networks
WPAN	Wireless Personal Area Networks
XML	eXtended Markup Language

LITERATURVERZEICHNIS

[1] E. A. Lee and S. A. Seshia, “Introduction to Embedded Systems - A Cyber-Physical Systems Approach”, LeeSeshia.org, 2011.

[2] Bundesnetzagentur/Bundeskartellamt, Monitoringbericht 2012, S.13, Feb 2013.

[3] J. Sommer, S. Gunreben, A. Mifdaoui, F. Feller, M. Köhn, D. Sass, J. Scharf: “Ethernet - A Survey on its Fields of Application”. IEEE Communications Surveys and Tutorials, Vol. 12, No. 2, 2010, pp. 263-284.

[4] Camek, A.; Buckl, C.; Correia, P.S.; Knoll, A., "An Automotive Side-View System Based on Ethernet and IP," 2012 26th International Conference on Advanced Information Networking and Applications Workshops (WAINA), pp.238,243, 26-29 March 2012.

[5] Lim, H.-T.; Volker, L.; Herrscher, D., "Challenges in a future IP/Ethernet-based in-car network for real-time applications," 48th ACM/EDAC/IEEE Design Automation Conference (DAC), pp.7,12, 5-9 June 2011.

[6] H. Georg, N. Dorsch, M. Putzke and C. Wietfeld. Performance Evaluation of Time-critical Communication Networks for Smart Grids based on IEC 61850. In 2013 IEEE INFOCOM Workshop on Communications and Control for Smart EnergySystems (INFOCOM'2013 CCSES). April 2013.

[7] A. Lewandowski, C. Wietfeld, "A comprehensive approach for optimizing ToA- localization in harsh industrial environments", ION/IEEE Position, Location and Navigation Symposium (PLANS), Indian Wells, CA, USA, May 2010.

[8] C. Wietfeld, H. Georg, S. Gröning, C. Lewandowski, C. Müller and J. Schmutzler, "Wireless M2M Communication Networks for Smart Grid Applications", European Wireless 2011 (EW2011), Vienna, Austria, Apr 2011, pp. 275-281.

[9] S.-Y. Lien, K.-C. Chen and Y. Lin “Toward Ubiquitous Massive Accesses in 3GPP Machine-to-Machine Communications”, IEEE Communications Magazine, Volume 49, Issue 4, April 2011.

[10] C. Müller, M. Putzke and C. Wietfeld, "Traffic Engineering Analysis of Smart Grid Services in Cellular Networks”. IEEE International Conference on Smart Grid Communications (SmartGridComm 2012), Tainan City, Taiwan, Nov 2012.

[11] R.-G. Cheng et al., “RACH Collision Probability for Machine-Type Communications”, IEEE 75th Vehicular Technology Conference (VTC-Spring), Yokohama, Japan, May 2012.

[12] 3GPP TS 22.368 V12.2.0, “Service Requirements for Machine-Type Communications”, Mar. 2013.

[13] C. Ide, B. Dusza, M. Putzke, C. Wietfeld, “Channel Sensitive Transmission Scheme for V2I-based Floating Car Data Collection via LTE”, IEEE International Conference on Communications (ICC), Ottawa, Canada, Jun. 2012.

[14] T. Taleb, A. Kunz, "Machine type communications in 3GPP networks: potential, challenges, and solutions," IEEE Communications Magazine, vol.50, no.3, pp.178-184, März 2012.

[15] 3GPP TR 36.888 V11.0.0, “Study on provision of low-cost Machine-Type Communications (MTC) User Equipments (UEs) based on LTE”, Jun. 2013.

[16] L. K. Moore „The First Responder Network and Next-Generation Communications for Public Safety: Issues for Congress“, Congressional Research Service, May 2013.

[17] B. Lichtensteiger, B. Bjelajac, C. Müller and C. Wietfeld, "RF Mesh Systems for Smart Metering: System Architecture and Performance", 1st IEEE International Conference on Smart Grid Communications (SmartGridComm), Gaithersburg, Maryland, USA, Oct 2010, pp. 379-384.

[18] A. Wolff, S. Michaelis, J. Schmutzler, C. Wietfeld, “Network-centric middleware for service oriented architectures across heterogeneous embedded systems”, Eleventh International IEEE EDOC Conference Workshop EDOC'07, pp. 105-108. 2007

[19] M.J.A.G. Izaguirre, A. Lobov, A.; J.L.M. Lastra, "OPC-UA and DPWS interoperability for factory floor monitoring using complex event processing," 9th IEEE International Conference on Industrial Informatics (INDIN), pp.205,211, July 2011.

[20] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner. 2008. “OpenFlow: enabling innovation in campus networks”. SIGCOMM Comput. Commun. Rev. 38, 2 (March 2008), pp. 69-74.

[21] C. Rehtanz and C. Wietfeld, "Das Internet der Energie", at - Automatisierungstechnik 10/2009, 10 2009, pp. 514-524.

[22] TIE-IN (NRW-Kompetenzzentrum Infrastruktur & Netze), Projektseite: www.elektromobilitaet.nrw.de/kompetenzzentren/infrastruktur-und-netze.html, zuletzt besucht am 2.11.2013

[23] Enterop Projektseite, www.enterop.net zuletzt besucht am 2.11.2013

[24] C. Wietfeld, J. Schmutzler and S. Gröning, "Kommunikationstechnische Aspekte zur Netzintegration von Elektrofahrzeugen", in Berliner Handbuch zur Elektromobilität, K. Boesche, C. Fest, O. Franz and A. Gaul (Herausgeber), C.H. BECK, 2013, pp. 491-516.

[25] J. Schmutzler, S. Gröning and C. Wietfeld, "Management of Distributed Energy Resources in IEC 61850 using Web Services on Devices", 2nd IEEE International Conference on Smart Grid Communications (SmartGridComm) 2011, Brussels, Belgium, Oct 2011, pp. 1-6.

[26] DFG Forschergruppe „Schutz- und leitsysteme zur zuverlässigen und sicheren elektrischen Energieübertragung“, www.for1511.tu-dortmund.de, zuletzt besucht am 1.8.2013

[27] H. Georg, S. C. Müller, C. Rehtanz and C. Wietfeld, "A HLA Based Simulator Architecture for Co-simulating ICT Based Power System Control and Protection Systems", 3rd IEEE International Conference on Smart Grid Communications (SmartGridComm 2012), Tainan City, Taiwan, Nov 2012.

[28] SmartC2Net Projektseite: www.smartC2net.eu., zuletzt besucht am 2.11.2013

[29] InBIN (Intelligent Bin), www.iml.fraunhofer.de/de/themengebiete/automation_eingebettete_systeme/Produkte/Intelligenter Behaelter.html ,zuletzt besucht am 2.11.2013

[30] AVIGLE (Avionic Service Platform) Projektseite, www.avigle.de , zuletzt besucht am 2.11.2013

[31] SIM-TD Projektseite, www.simtd.de , zuletzt besucht am 2.11.2013

[32] SFB 876 Projektseite Teilprojekt B4 Analyse und Kommunikation für die dynamische Verkehrsprognose, www.sfb876.tu-dortmund.de/SPP/sfb876-b4.html, zuletzt besucht am 2.11.2013

[33] Bericht zu Falschfahrerwarnsystem: www.derwesten.de/region/westfalen/wie-schlaue-pfosten-gegen-geisterfahrer-helfen-sollen-id7339482.html zuletzt besucht am 2.11.2013

[34] SmartOR Projektseite: www.smartor.de, zuletzt besucht am 2.11.2013

ÜBER IKT.NRW

IKT.NRW vernetzt die Akteure der nordrhein-westfälischen IKT-Branche:

Wirtschaft, Wissenschaft und Politik treiben gemeinsam die Weiterentwicklung des IKT-Marktes in Nordrhein-Westfalen voran. Ziel von IKT.NRW ist es, die Stärken der Branche, Synergiepotenziale und zukunftsträchtige Entwicklungen frühzeitig zu identifizieren und Innovationsprozesse aktiv zu fördern. Darüber hinaus wird die öffentliche Wahrnehmung für den IKT-Standort NRW geschärft.

Das Clustermanagement IKT.NRW führt beispielsweise Kooperations- und Netzwerk-Veranstaltungen durch, unterstützt Unternehmen bei Messe-Teilnahmen und Unternehmerreisen und veröffentlicht regelmäßig Branchen- und Trendreports. Offene Innovationsprozesse sind ein wichtiger Bestandteil im Selbstverständnis von IKT.NRW. Ideen und Kooperationsanfragen sind deshalb immer willkommen.

EUROPÄISCHE UNION
Investition in unsere Zukunft
Europäischer Fonds
für regionale Entwicklung

Ziel2.NRW
Regionale Wettbewerbsfähigkeit und Beschäftigung