51. UKW-Tagung Weinheim

Technik und Probleme bei telematischen Fahrzeugüberwachungssystemen

Dipl.-Ing. Erich H. Franke, DK6II

erich.franke@afusoft.com

Inspiriert durch die rasante Verbreitung von Satellitennavigations-Empfängern und der Zugriff zu billigen Kommunikationsmedien haben sich zahlreiche Unternehmen aufgemacht, Systeme zur Fahrzeugüberwachung anzubieten. Doch diese Anwendung ist nicht ohne Tücken. Fragen nach Akzeptanz, ethischer und rechtlicher Vertretbarkeit wie auch Datenschutz und Sicherheit müssen gleichberechtigt neben rein technische Anforderungen gestellt werden. Wir wollen uns in diesem Beitrag beide Bereiche näher anschauen.

Königsbach-Stein, im Juli 2006

Einführung und Abgrenzung

Der Begriff „*Telematik*“ hat sich umgangssprachlich als Synonym für Fahrzeugverfolgungssysteme eingebürgert. Nicht ganz korrekt wie ich meine, da dieses Wort ursprünglich nur die Verknüpfung von *Telekommunikation* und *Informatik* beschreibt und damit einen viel weiteren Definitionsbereich besitzt.

Zumindest ein wenig korrekter wäre der Begriff „*Verkehrstelematik*“ um den Einsatz von Kommunikation und Informatik im Verkehrswesen zu beschreiben. Hierunter fallen jedoch nicht nur der Landeinsatz sondern auch Schienen-, Luft- und Seeverkehr. Trotz dieser Einschränkungen werde ich in diesem Beitrag das Wort Telematik als Synonym für Verkehrstelematik mit dem Einsatzort Straße benutzen.

Im kommerziellen und universitären Umfeld entstehen zwar fast täglich neue Telematik-Dienste vor allem im „low-cost“-Bereich. Doch nur wenige Anwendungen schaffen es sich am Markt zu platzieren.

In der Tat steckt der Telematikeinsatz im Straßenverkehr in Deutschland trotz heroischer Anstrengungen von Industrie und Politik noch immer ein wenig in den Kinderschuhen.

Im Gegensatz dazu ist die Verbindung von Rechnern und Kommunikation in der Luftfahrt tägliche Praxis. Auch in der Seeschifffahrt und auf der Schiene ist Telematik weit verbreitet. Was ist auf der Straße anders?

Nun, bedingt durch den Individualverkehr sind die Einsatzfälle auf der Straße wesentlich weiter aufgefächert als beispielsweise in der Luft- oder Seefahrt. Die Anforderungen reichen von reiner Standortermittlung über die Fernabfrage von Messdaten oder Fernwirkaufgaben bis hin zur Text-, Daten- und Bildübertragung.

Doch nicht alles was technisch machbar ist und von Ingenieuren und Technikbegeisterten als interessant empfunden wird, ist für den Anwender im Alltag auch wirklich akzeptabel. Lassen Sie uns hierzu ein paar Beispiele beleuchten.

Anwendungen: Anspruch und Wirklichkeit

Als Hauptschwerpunkt der Telematikanwendungen wird immer wieder das Flottenmanagement genannt. Transportunternehmen erhoffen sich hiervon eine Optimierung des Fahrzeugeinsatzes, vor allem im internationalen Güterverkehr.

Flottenmanagement als Telematikanwendung ist auch entsprechend überlaufen. Hier spielen Großanbieter wie Fleetboard [FLB] genauso mit wie Kleinstanbieter, mit zum Teil ganz unterschiedlichen Preisansätzen.

Allerdings setzt dies eine im gesamten Einsatzgebiet vorhandene Kommunikationsmöglichkeit voraus. Und die ist durchaus nicht immer gegeben. Was nützt die beste Software und die hübschen schwarzen Kästchen – seien sie noch so billig - wenn ein Fahrzeug in Gegenden ohne Mobilfunkanbindung einfach nicht erreicht werden kann?

Oder was ist, wenn die veranschlagten Kommunikationskosten im Alltagseinsatz plötzlich über alle Grenzen ansteigen? In der Tat klafft die Schere zwischen dem Versprechen der Vertriebsseite und der rauen Kommunikations-Wirklichkeit manchmal deutlich auseinander.

Bleiben die physikalischen und ökonomischen Realitäten gar zu sehr hinter den Versprechen der Anbieterseite oder den Erwartungen der Kunden zurück, so führt das nicht selten zu Frustration bei den betroffenen Anwendern, die hernach verständlicherweise mit Skepsis und Zurückhaltung reagieren, was dann auch seriöse Anbieter zu spüren bekommen.

Auf der anderen Seite sind die Fahrer telematisch aufgerüsteter Fahrzeuge nicht immer darauf erpicht, dass sie nun praktisch jederzeit und überall überwacht werden können. Und das vielleicht ohne dass sie davon Kenntnis haben und hierauf Einfluss nehmen können.

Dieser nicht zu unterschätzende „*Big-Brother-Effekt*“ erfordert eine sehr offene und ehrliche Politik seitens der Firmenleitungen, ein Anspruch der im Alltag nicht immer gegeben ist.

Es gibt noch weitere Faktoren: Von Branchenkennern kritisch gesehen wird in diesem Zusammenhang „Toll-Collect“ das Mauterfassungssystem für den Güterverkehr auf Autobahnen [TOLL], bei dem eine Vermischung der Mauterhebung mit zusätzlichen Telematikfunktionen grundsätzlich technisch möglich wäre.

Da dies aber für die an Toll-Collect beteiligten Systemhäuser ein Quasi-Monopol schaffen und für viele Drittanbieter von Flottenmanagementsystemen letztendlich das Aus bedeuten würde, hat die Europäische Kommission bereits vor drei Jahren ihr Veto gegen eine Vermischung von Maut und Telematik eingelegt. Wie lange das dem Mittelstand wohl helfen wird?

Wir müssen uns natürlich auch mit der Frage auseinander setzen, was eigentlich mit den erhobenen Daten geschieht. Und wie wird dies erst später nach Einführung der PKW-Maut aussehen? Man denke dabei an die laufende Diskussion über die Nutzung der an den Mautbrücken erfassten Bewegungsdaten und daran, dass einmal getroffene Entscheidungen bei Bedarf revidiert werden können und dies vielleicht auch müssen.

In seinem Roman „*Die Physiker*“ schreibt Dürrenmatt treffend, dass jeder denkbare Gedanke einmal gedacht wird. [PHYS] Wir müssen daher sehr sorgfältig beobachten, wohin sich diese Angelegenheit in den nächsten Jahren politisch entwickeln wird.

Das zweite große Anwendungsgebiet der Telematik liegt in der *Absicherung* von Waren und Fahrzeugen gegen Diebstahl durch Außen- und Innentäter sowie gegen Beraubung. Im Ersteren Fall denken Sie bitte an die Kiste Whiskey, die dann und wann einmal „von der Laderampe fällt“.

Hier kann Telematik durch Kombination von Türkontakten, RFID und Standortbestimmung helfen, Licht ins Dunkle zu bringen und auch wirksam dazu beitragen ehrliche Mitarbeiter von einem hässlichen Verdacht entlasten! [UEBW]

Beim Schutz gegen *Beraubung* sind Fahrer gegenüber Telematik eher positiv motiviert, da telematische Systeme die Tatausführung erschwert und damit für den Täter das Risiko erhöht. Fahrer und Unternehmer versprechen sich dadurch eine gewisse Abschreckung und damit einen höheren Schutz des Personals und der Fracht.

In diese Kategorie gehören auch das „*Geofencing*“ und „*Corridoring*“ bei dem ganze Fahrzeuge gegen unbefugtes Bewegen oder gegen das Verlassen einer Route durch virtuelle vom Ortungssystem generierte „Zäune“ abgesichert wird. Dazu müssen im Fahrzeugrechner geeignete Gebietsbeschreibungen hinterlegt und permanent ausgewertet werden.

In diesem Einsatzfall muss sowohl die Kommunikation und Standortbestimmung zuverlässig funktionieren. Zusätzlich muss die bedingungslose Vertraulichkeit der übertragenen Informationen gewährleistet werden.

Die Übertragung muss wirksam gegen Unterbrechung („*denial of service*“, DoS), Ausspähen (*Abhören mit Inhaltsauswertung*) und Verfälschen (engl. „*spoofing*“) und „*recording*“ geschützt werden. Hierbei kommen bei seriösen Systemen geeignete anerkannte kryptologische Verfahren zum Einsatz.

Klassische Mobilfunk-Anwendungen sind allerdings gerade gegen DoS-Attacken eher anfällig. Suchen Sie als ersten Test einfach einmal im Internet mit einer beliebigen Suchmaschine nach den Begriffen „*jammer + GSM*“ („*jammer*“: engl. Störsender). Sie werden erstaunt sein, was dort im illegalen Bereich alles angeboten wird! Wir werden diesen Problemkreis später noch eingehender diskutieren.

Irgendwo zwischen den beiden oben genannten Ansprüchen liegen Anwendungen zur Maschinendatenerfassung, Verkehrszählung bis hin zur Fahrplanüberwachung im öffentlichen Personennahverkehr. Bei der Fernüberwachung von Arbeitsmaschinen oder der Datenerfassung steht wiederum die technische „Performance“ im Vordergrund. Datenschutzrechtliche Bedenken sind in diesem Gebiet weniger zu erwarten.

Das gilt insbesondere für das in Amateurkreisen angewandte „*Automatic Position Reporting System*“ [WB4APR], [APRS]. Über dieses System „veröffentlichen“ auf freiwilliger Basis Stationen ihren Standort und weitere Messdaten im Rundstrahlverfahren. Als Kommunikationsmedium wird Packet Radio verwendet. Die Daten werden verbindungslos ausgestrahlt und können von allen entsprechend ausgestatteten Stationen im Umfeld aufgenommen werden.

Bei APRS gibt es also kein Netz im eigentlichen Sinne. Alle Informationen werden zwischen den Teilnehmern ausgetauscht und von diesen weiter geleitet. Die Teilnehmer bilden so das Netz. Man spricht daher auch von „kooperativen“ Systemen.

APRS wurde 1992 von Bob Bruninga (WB4APR) definiert und erfreut sich auch in anderen Anwendungsgebieten recht ordentlicher Beliebtheit. Bob beschreibt APRS auf seiner Website bei der U.S. NAVY auch treffend als System zum schnellen Austausch lokaler taktischer Information [WB4APR].

APRS darf aus fernmelderechtlichen Gründen auf Amateurfrequenzen nicht kommerziell genutzt werden. Ich habe es in diesem Beitrag aufgenommen, da es eine für Amateure sowie berechtigte Behörden- und Privatanwender interessante Technologie darstellt. Außerdem wird dadurch die Diskussion über Überwachung und den „gläsernen Verkehrsteilnehmer“ um eine interessante Variante bereichert!

Segmentierung

Telematische Fahrzeugverfolgungssysteme werden in der Literatur und durch die Systemanbieter gerne in „*Segmente*“ aufgeteilt. dadurch werden die Komponenten in strukturierter Form beschrieben.

Das „*Fahrzeugsegment*“ umfasst alle Funktionen „vor Ort“. In Fahrzeugen spielt zumeist die Standortbestimmung die Hauptrolle, gepaart mit anderen „*Location based services*“ [LBS], wie Alarm bei Veränderung des Standorts. Anwendungen im Flottenmanagement erfordern zusätzliche Meldungsübertragung, beispielsweise Dispositionsdaten oder Fahraufträge.

Synonym für Fahrzeug könnte aber auch die Alarmanlage einer Jagdhütte, ein Wasserwerk im Schwarzwald, eine Gas-Pumpstation in Kasachstan oder ein Windkraftwerk sein. Bei diesen Anwendungen liegt der Schwerpunkt auf der Übertragung von Alarm-Meldungen, Maschinendaten, ggf. gekoppelt mit Fernwirktechnik, beispielsweise für Notabschaltungen.

Im „Kommunikationssegment“ sind die Funktionen der Meldungsübertragung zusammengefasst. Hierunter zählen Mobilfunk- und Satellitenübertragung, aber auch der klassische Amateur- oder der taktische Funk.

Das „Nutzersegment“ ist abhängig von der eigentlichen Aufgabe. Telematische Sicherheits- und Alarmsysteme wie auch Flottenmanagement-Systeme sind überwiegend „zentral“ orientiert. Die Meldungen laufen vom Fahrzeug zu einer Leitstelle bzw. wieder zurück. Den LKW-Fahrer in Tübingen interessiert nur in den allerwenigsten Fällen der genaue Standort seines Kollegen in Rostock.

In anderen Anwendungen, beispielsweise bei bestimmten polizeilichen Maßnahmen, bei Großschadenslagen oder in militärischen Informationssystemen müssen die mobilen Teilnehmer sehr wohl den Überblick über die Gesamtlage erhalten [C3I]. Dies wird unter dem Begriff „*Situation Awareness*“ beschrieben. In diesem Fall muss das System bestimmte notwendige Informationen zu ausgewählten Teilnehmern zurückspiegeln.

Methoden der Standortbestimmung

Das *Global Positioning System* (GPS) wurde bereits in den siebziger Jahren konzipiert und zwischen 1973 und 1995 bis zur Betriebsbereitschaft („*full operational capability*“) ausgebaut. Seit dem Jahr 2000 ist das System auch für den Breiteneinsatz tauglich, als Bill Clinton die künstliche Verschlechterung der Navigationssignale für zivile Nutzer (*selective availability*) abschalten ließ.

Das System erlaubt einem terrestrischen Empfänger durch Messung der Unterschiede der Signallaufzeiten zu einzelnen Satelliten seinen Standort mit einer Genauigkeit von ca. 20m. Die Genauigkeitsangabe ist statistisch zu sehen. Sie hängt ab von der Lage der umlaufenden Satelliten am Himmel, der sog. „Konstellation“, den Ausbreitungsbedingungen in der Atmosphäre und vor allem von der Umgebung des jeweiligen Empfängers.

Da die Ortung die jeweiligen relativen Entfernungen des Empfängers zu den verschiedenen Satelliten benutzt („*Pseudorange*“), ist das Verfahren besonders anfällig gegen Laufzeitsprünge durch Reflexionen beispielsweise an Hauswänden. Ist dann noch ein Teil des Himmels verdeckt und dadurch ein paar Satelliten nicht direkt sichtbar, verschlechtert sich die Ortung umso mehr.

Deshalb funktioniert die GPS-Ortung innerhalb von Gebäuden nicht betriebssicher, selbst wenn man dort die Satellitensignale empfangen kann.

Auch im Stadtverkehr kann dies zu Problemen führen. Zwanzig Meter Genauigkeit, die unter Umständen auch zu 100m werden kann ist hier nicht genug! Denken Sie beispielsweise an das exakte Auffinden von Straßenkreuzungen. Navigationssysteme können sich hier durch Techniken wie „*Map Matching*“. So nennt man das Verfahren, die Positionsgenauigkeit durch Vergleich mit gespeicherten Punkten („*point of interest*“) oder dem bekannten Straßenverlauf optisch aufzupeppen. Allerdings benötigen die Navigationssysteme dafür exakt georeferenzierte und vor allem verlässlich aktualisierte Straßendaten, sonst kommt dabei nichts als Unsinn heraus.

Da das Satellitensignal in Tunnels überhaupt nicht und bei Abschattungen oder Mehrwegeempfang nur gestört empfangen werden kann, muss man bei höheren Anforderungen die Navigationslösung mit Radsensoren, Kompanden bzw. Kreiseln stützen.

Die Fehler aus der Signalausbreitung in der Troposphäre werden normalerweise durch „differentiell korrigierten GPS“ verbessert [DGPS]. Hierzu stehen terrestrische Methoden wie beispielsweise [RASANT] zur Verfügung. Elegant ist die satellitengestützte Korrektur durch das „*European Ground Navigation Overlay System*“ [EGNOS]. Hierbei wird die Korrekturinformation für jedermann empfangbar im Rundstrahldienst über geostationäre Satelliten auf Frequenzen benachbart zum GPS-Signal ausgesandt. Ein geeigneter Empfänger benutzt dann die bestehende GPS-Antenne gleichzeitig zum Empfang von EGNOS.

EGNOS wird in Marketingaussagen auch gerne als „Stufe 1“ von GALILEO, dem zukünftigen Satellitenortungssystem der „*European Space Agency*“ [ESA] betrachtet. Galileo wird Satellitenortung in verschiedenen Genauigkeitsstufen anbieten. Verschiedene Dienste, wie zum Beispiel genaue Daten für Landesysteme werden dabei verschlüsselt sein. Die wichtigste Neuerung dabei ist, dass erstmalig Informationen über die Zuverlässigkeit („*Integrity*“) des Ortungsergebnisses ermittelt werden kann.

Bei GPS ist die Integrity hingegen nicht nachweisbar. Deshalb kann GPS nicht ohne weiteres für kritische Anwendung wie beispielsweise Flugzeug-Landesysteme genutzt werden.

Eine interessante Variante der Standortbestimmung über Satelliten stellt QUASPR dar. Dies ist ein Firmenstandard, der von QUALCOMM [QC] früher in Satcom-Systemen genutzt wur-

de. QUASPR nutzt zur Ortung den Uplink vom Fahrzeug zu den Satelliten aus. Daher steht das Ortungsergebnis nicht im Fahrzeug selbst, sondern nur in einer Zentrale zur Verfügung. Die Ortungsgenauigkeit beträgt dabei ca. 200m.

Im terrestrischen Bereich bieten Mobilfunkanbieter auch die so genannte Zellenortung an. Hierbei kann der Standort eines Mobilfunkgerätes im Funknetz mehr oder minder genau bestimmt werden. Man unterscheidet dabei „*infrastrukturabhängige Ortung*“ und „*feldstärkebezogene Ortung*“ bis hin zu geräteunterstützter Trilateration im Endgerät.

Zur Trilateration wird der so genannte „Time Advance“ Wert benutzt. Dieser dient im GSM-System eigentlich zur Laufzeitkorrektur des TDMA-Verfahren und wird zwischen dem Mobilteil und allen Basisstationen ausgehandelt. Der TA-Wert hat eine Granulität von ca. 3,66µs, was eine Stufung von ca. 1,1 km entspricht.

Dies erlaubt unter bestmöglichen Bedingungen eine Ortungsgenauigkeit von ca. 550 Metern. In der Praxis kann das durchaus ungenauer sein, vor allem bei geringer Dichte von Basisstationen. Im ländlichen Umfeld des Verfassers zeigte das Werkzeug einen namhaften deutschen Anbieters den Standort gar mit drei Kilometern Ablage an. Dies war der Standort der Basisstation.

Soweit also zum „Hollywood“-Ansatz einen mobil Telefonierenden über das bestehende Netz metergenau zu orten[1]. Um festzustellen, ob sich ein LKW-Fahrer momentan gerade in Hamburg oder München aufhält, mag das wohl genügen.

Das Zellenortungsverfahren ist aus zwei Gründen etwas problematisch. Erstens sind die Ortungen vielfach recht teuer. Ich habe am Markt schon Angebote gesehen, die bis zu 40ct pro Ortung von Kunden verlangten. Für Flottenmanagement-Anwendungen ist das vielfach zu teuer, für Sicherheitsaufgaben ist die Ortung häufig zu ungenau. Trotzdem halten sich diese Angebote zum Teil wegen aggressivem Marketing am Markt. Und es gibt einen weiteren nachvollziehbaren Grund:

Zellenortung kann praktisch mit jedem Mobiltelefon ohne Zusatzgeräte durchgeführt werden. Dabei ist es technisch ohne weiteres möglich eine Person ohne deren Wissen und Einverständnis zu orten. Dem Verfasser sind Fälle bekannt, in denen Mitarbeiter über ihre Firmentelefone an der „elektronischen Leine“ gehalten werden.

Genau hier stoßen wir an die Grenze zwischen dem technisch Machbaren und rechtlichen, ethischen und politischen Randbedingungen. Dies ist eine Grenze, die wir als Ingenieure aufmerksam beachten sollten.

Methoden der Nachrichtenübertragung

Nicht minder interessant sind die verschiedenen Methoden der Nachrichtenübertragung.

In der Vergangenheit wurden auf Mobilfunk basierende Systeme angeboten, die Kurznachrichten des „*Short Message Service*“ (SMS) des Mobilfunks benutzten. Diese Übertragung ist zwar äußerst einfach zu implementieren, jedoch aus Kosten- Zuverlässigkeits- und Sicherheitsgründen überholt und daher abzulehnen. SMS werden nach Anzahl abgerechnet. Die Kosten betragen zwischen 0,6ct und 20ct je nach Anbieter, Vertragsart und Meldungsaufkommen.

Alte SMS-basierende Systeme arbeiten im „*Punkt-zu-Punkt*“ Verfahren. Daher ist die Leitstelle mit einem eigenen Kommunikationsgerät ausgestattet, zu dem die Mobilteilnehmer ihre Nachrichten senden. SMS-Nachrichten sind in der Zustellung häufig nicht garantiert. Die Übermittlungszeit kann sehr stark schwanken, Nachrichten können vor allem im Verkehr über Landesgrenzen in Überleiteinrichtungen („*Gateways*“) „hängen bleiben“. Außerdem sind die Nachrichten in vielen Systemen extrem leicht zu verfälschen. Wirklich sichere Datenschutz-

[1] Hier wird die Möglichkeit der direkten Ortung bzw. Trilateration einzelner Mobilteilnehmer durch spezielle Maßnahmen nicht betrachtet.

verfahren können wegen der geringen Datenmenge von 160 Zeichen (nicht ASCII!) nicht angewandt werden.

Eine deutliche Verbesserung bietet der „*General Packet Radio Service*“ (GPRS) bzw. der Datendienst des „*Universal Mobile Telecommunications Service*“ (UMTS). Beide Datendienste besitzen eine höhere Kapazität. Daten können paketorientiert unter Nutzung von Internet-Protokollen (IP) übertragen werden. Nicht die Datenrate ist dabei das Problem sondern die Möglichkeit, die zu übertragenden Daten durch Authentisierungsinformation vertrauenswürdig zu machen und den Nachrichteninhalt nach einem anerkannten kryptologischen Verfahren gegen Inhaltsauswertung zu schützen. Diesem Anspruch genügt heute nur ein kleiner Teil der am Markt befindlichen Telematikgeräte.

Wegen der Nutzung der Internet-Protokolle ist für viele derartiger Systeme ein im Internet eingebundener Server erforderlich, der vom Nutzer entweder erworben oder vom Service-Provider angemietet werden muss. Dies ist jedoch üblicherweise kein unüberwindbares Problem.

Gemeinsames Merkmal aller terrestrischen Mobilfunkdienste sind mehr oder minder große Probleme an Landesgrenzen. Selbst große Mobilfunkanbieter haben nicht in allen Partnerländern Verträge für die Datenweiterleitung. So kann es sein, dass man beim Passieren einer Landesgrenze zwar noch im Sprachdienst telefonieren, aber keine Daten mehr übertragen kann.

Zweites gemeinsames Merkmal auf GSM/GPRS basierender telematischer Dienste ist die vergleichsweise leichte Störbarkeit. Auf dem grauen und schwarzen Markt werden zahlreiche – illegale - Störsender angeboten, die im Umkreis von 50 bis 1000m den Mobilfunkbetrieb lahm legen. Im Internet werden passende Geräte unter den Begriffen „*GSM*“ und „*Jammer*“ (engl. für Störsender) mit der üblichen Klausel „nur für den Export“ zwischen 200€ und 2.000€ angeboten. Zum Betrieb ist kein Know-How sondern nur genügend kriminelle Energie und ein Stromanschluss für Auto oder das Netz erforderlich. Erste Straftaten unter Einsatz derartiger Störer wurden bereits gemeldet (Quelle nicht offen legen).

Dieses Manko besitzen auf Satelliten basierende Telematikdienste üblicherweise nicht. Hier erfolgt die Kommunikation über eine Zwei-Wege-Verbindung zu umlaufenden oder geostationären Satelliten. Hierfür kommen Iridium einerseits, und Inmarsat oder Eutelsat andererseits in Frage. Eine handvoll seriöser und eine paar wenige unseriöse Anbieter sind mit derartigen Lösungen am Markt.

Wegen der Richtwirkung der Antennen und bei Nutzung geeigneter Modulationsverfahren sind Satellitenverbindungen trotz des ungünstigen Link-Budgets erstaunlich störresistent.

Wird der Satellitensender und die Antennen, zumeist sind dies flache Patch-Antennen, fachgerecht und „konspirativ“ verbaut, dann stellen diese in einem typischen Beraubungsszenario für den Täter ein unkalkulierbares Risiko dar, wenn sie nicht sofort gefunden werden können bzw. deren Position durch Verrat bekannt ist.

Auch ist der Energieverbrauch einiger Gerätearten bemerkenswert. Es gibt Geräte, die mit eingebauten Batterien bis zu fünf Jahre betriebsbereit sind. Damit sind sie für batterieautonome Aufgaben, wie die Containerverfolgung besonders gut geeignet. Allerdings schlafen dann die Geräte häufig und lange, so dass in derartigen Anwendungen ggf. nur eine bis vier Ortungen am Tag durchgeführt werden.

Auf der Kostenseite sind Satellitendienste gar nicht einmal so teuer. Je nach System, Meldungsaufkommen und Anwendung muss man mit 12€ bis 40€ pro Monat und Fahrzeug rechnen. Das ist ein Wert, der im internationalen Verkehr durchaus mit terrestrischem Mobilfunk konkurrieren kann.

Bei satellitenbasierenden Systemen muss noch unterschieden werden, ob die Übertragung über geostationäre oder umlaufende Satelliten erfolgt.

Geostationäre Satelliten sind in jedem Fall vorzuziehen, da diese eine verlässliche Übertragung ohne Abdeckungslücken gewährleisten. Bei umlaufenden Satelliten hängt die Übertra-

gungsfähigkeit des Systems natürlich davon ab ob zum Alarmzeitpunkt momentan überhaupt ein Satellit zur Verfügung steht.

Ist dies nicht der Fall, so muss die Alarmnachricht gespeichert werden. In speziellen Fällen kann es dann Minuten bis hin zu Stunden dauern, bis einmal wieder ein Satellit vorbeikommt, dem man das Datenpaket mitgeben kann. In sicherheitskritischen Anwendungen ist das selbstverständlich inakzeptabel.

In unserem Beispiel mit APRS hingegen kommen einfache Halbduplex-Funkgeräte zum Einsatz. Da die Informationsmenge gering ist, kann gut mit der mithin langsamen Bitrate von 1200 bit/sec gearbeitet werden. APRS ist ein dezentrales, kooperatives System, bei dem Fahrzeuge eine Art von „*ad-hoc-Netzwerk*“ bilden und untereinander Daten austauschen. Empfangene und durch den eigenen GPS-Empfänger gewonnene Information wird dann rundstrahlend als sog. „*unnumbered information*“ (UI) weitergeleitet. Da APRS Amateurfunkfrequenzen benutzt ist der Betrieb nur lizenzierten Funkamateuren gestattet. In Deutschland liegt das Aktivitätszentrum auf 144,800 MHz, in den U.S.A. auf 144,390 MHz.

Zumindest tritt bei APRS der „Big-Brother-Effekt“ nicht auf, denn der an APRS interessierte Amateur will ja gerade seine Position, Fahrgeschwindigkeit, Umgebungstemperatur und was man sich sonst noch so vorstellen kann jedermann bekannt machen (CQ).

Für Insider interessante Rechtsfragen befassen sich mit dem Problem, dass APRS von nicht-Amateuren unter Rufzeichenmissbrauch illegal benutzt wird. Solche Vorfälle durch „Schlauberger“ wie beispielsweise Pizzadienste können von Zeit zu Zeit in jeder größeren Stadt beobachtet werden.

Dass hingegen ein mit APRS ausgestattetes Fahrzeug auch einmal von einem nicht lizenzierten Fahrer mit dem Funkamateur auf dem Beifahrersitz gesteuert werden kann, sollte kein Problem darstellen.

Weit interessanter ist die Diskussion was geschieht, wenn die Ortungsdaten, die der Amateur über APRS so freizügig absondert und die auf verschiedenen Servern im Internet für jedermann zugänglich hinterlegt werden, von Außenstehenden nach unerwarteten Kriterien ausgewertet werden. Beispielsweise wie lange ein bestimmtes Fahrzeug für eine bestimmte Fahrstrecke gebraucht hat und welche Geschwindigkeit da wohl gefahren wurde. Oder ob sich das Fahrzeug längere Zeit in der Nähe bestimmter Liegenschaften, wie zum Beispiel Botschaften oder Treffpunkte bestimmter observierter Gruppen aufgehalten hat! Das Wort „Datenspur“ erhält da eine ganz neue Bedeutung.

Übrigens: dieses Messverfahren ist unter dem Begriff „Zonenmessverfahren“ bekannt… Untreue Ehefrauen und -männer wissen immerhin um diese Überwachung und können bei Bedarf „den Stecker ziehen“. Oder auch nicht, denn dann muss der Fahrer seinem Partner unter Umständen erst einmal die fehlenden Daten erklären…

APRS-Puristen mögen mir meine spöttisch-kritischen Worte verzeihen. APRS ist *definitiv* eine spannende Sache für jeden technikbegeisterten Amateur. Über mögliche Konsequenzen muss allerdings offen und ehrlich diskutiert werden können.

Das Nutzer-„Segment“

Bisher haben wir uns hauptsächlich mit dem „*Fahrzeug*“- und dem „*Kommunikationssegment*“ beschäftigt. Dies sind aber auch technisch die interessantesten Stellen. Das „Nutzersegment“ kann nun verschiedentlich aufgebaut sein.

In *zentralistisch* organisierten Systemen besteht das „Nutzersegment“ einfach aus der Leitstelle. Denken Sie als Beispiel an eine Rettungsleitstelle der Feuerwehr, Polizei oder von Rettungsdiensten oder einfach an die Dispositionszentrale einer Spedition. Die gesamte „taktische“ Information wird von den Fahrzeugen an diese Leitstelle übertragen und dort visualisiert.

Kooperative Systeme hingegen verteilen die Information auch zwischen den Teilnehmern und stehen damit auch „vort Ort“ zur Verfügung. Dadurch wird die Kenntnis über die Gesamtlage, beispielsweise bei einem Schadensereignis, entscheidend gefördert.

Lagedarstellung und Leitstellentechnik

In zentral orientierten wie auch in kooperativen Systemen müssen die gewonnenen und übertragenen Informationen ausgewertet und dargestellt werden.

Meist besteht die Forderung nach Visualisierung von Standort und Status der Fahrzeuge. Hier gibt es eine Reihe von Firmen am Markt, die Kartensysteme und benachbarte Dienstleistungen wie Georeferenzierung und Geocodierung anbieten. Hierzu zählen unter vielen anderen Map&Guide [MUG], Microsoft [MP] und neuerdings auch Google mit Google Maps [GM]. Welches System man nun wählt, hängt vom Leistungsanspruch und dem Geldbeutel ab. Hier ist genaues Anschauen besonders wichtig, damit man nicht „Äpfel mit Birnen" vergleicht.

Anbieter wie Map&Guide, Google oder Microsoft beispielsweise kombinieren Kartenwerke verschiedener Hersteller zu Gesamtkarten. Das Straßennetz und andere Objekte sind ist auf Geokoordinaten referenziert (georeferenziert) und erlauben, einen Punkt, beispielsweise den Standort eines Fahrzeuges an Hand seiner Koordinate exakt in die Karte einzuzeichnen.

Google besitzt das „Schmankerl" zwischen der Kartendarstellung auch auf Luftbildaufnahmen umzuschalten, was in Präsentationen einfach atemberaubend aussieht, für Rettungssysteme wertvolle Geländeinformation liefert, in einem Flottenmanagement-System hingegen keinen Nutzen bringt.

Systeme wie von Map&Guide erlauben auch das „*Reverse Geocoding*", d.h. Straßennamen aus Koordinaten zurück zu gewinnen, um damit Anfahrtswege zu markieren. Diese Funktion macht dieses Produkt besonders für Aufgaben im Sicherheits- und Flottenmanagement wertvoll.

Google Maps steht nach eigenen Aussagen derzeit für kommerzielle Anwendungen in Deutschland nicht zur Verfügung[2]. Lediglich Tests und „*Proof-of-Concept*" Installationen sind ausdrücklich gestattet, nicht jedoch Produktivsysteme.

Für den engagierten Privatanwender bietet sich jedoch eine sehr gut und einfach zu beherrschende und vor allem praktisch kostenlose Möglichkeit an gutes Kartenmaterial heranzukommen. Die Lizenzierungspolitik und das Geschäftsmodell von Google ist hier äußerst interessant und bei näherem Hinsehen gar nicht unfair.

Kommerzielle Telematik-Systeme unter Einbeziehung von Google Maps müssen allerdings mit gesundem Misstrauen betrachtet werden, denn sie sind nach heutigem Stand schlichtweg illegal.

Noch kritischer steht es mit Systemen die auf handgescannten Karten aufsetzen oder gar rechtswidrig mit unlizenziertem – mithin gestohlenem – Kartenmaterial aufsetzen. Da Kartenwerke dem Urheberschutz unterliegen müssen sich potentielle Anwender immer die Frage stellen, woher die vermeintlichen Schnäppchenpreise eines Anbieters denn wirklich kommen.

In der eigentlichen Leistellentechnik werden reine Softwarelösungen, so genannte „standalone" Systeme teilweise von Web-basierenden Lösungen ersetzt. Gut gemacht, sind Web-Lösungen äußerst hilfreich, da sie von verschiedenen Arbeitsplätzen ohne Softwareinstallation benutzt werden können.

Moderne Programmiertechniken wie [AJAX] erlauben in gewissen Grenzen auch dynamische Darstellungen in „beinahe-Echtzeit". Manche auf dem älteren [LAMP] basierenden Lösungen sind allerdings ausgereifter und haben in Security- und Flottenmanagement ihren festen Platz.

Web-Lösungen benötigen allerdings schnelle Internet-Kommunikation um akzeptable Antwortzeiten zu erreichen. Außerdem ist die Kompatibilität zwischen den Web-Browsern ein wohl bekanntes Problem. Da jeder Browser-Programmierer im Interesse seiner eigenen

---

[2] Stand Juni 2006. Wird laut Aussage des Vertriebs später neu geregelt.

Marktanteile jeweils sein eigenes Süppchen kocht und die Probleme der Anwender geflissentlich ignoriert, treten hier auch bei den besten Systemen immer wieder Darstellungsschwierigkeiten auf.

Stand-Alone-Lösungen haben überall dort einen Vorteil, wo es auf rasche Reaktion, „echte Echtzeit“ und auf geringe zu übertragende Datenvolumina ankommt. Dies macht sie zu Kandidaten für mobile Clients. Auf modernen PDA mit Kommunikationsanbindung GPRS/UMTS oder Smart Phones lassen sich heute erstaunlich gut funktionierende C3I-Systeme aufsetzen.

Ausblick

Wie jede Technologie beinhaltet die Verkehrstelematik Nutzen und Risiken gleichermaßen. Verantwortungsvoll und korrekt genutzt ergibt sich eine Vielzahl neuartiger Möglichkeiten, den Schutz, die Sicherheit und die Effizienz im Alltag sinnvoll zu steigern.

Wie immer muss dabei die Frage erlaubt sein, ob wirklich alles technisch Mögliche und Denkbare im praktischen Alltagseinsatz auch immer sinnvoll und – insbesondere bei der Telematik – auch ethisch und politisch vertretbar ist.

Überdies muss vor übereiltem Einsatz telematischer Systeme kritisch geprüft werden, ob der Einsatzzweck mit der angebotenen Technik überhaupt erfüllbar ist. Nicht alle der am Markt angebotenen Systeme eignen sich wirklich für jede Anwendung.

Allzu gerne versprechen Produktanbieter vor allem im niederpreisigen Sektor Leistungsmerkmale, die sich bei näherem Hinsehen als unsinnig bis unseriös herausstellen. Sorgfältige Beratung und Abwägung reduziert spätere Frustration.

Werden diese Punkte beachtet bringt Telematik auch den Nutzen, den man von ihr erwartet.

Für Amateure öffnen sich spannende Gebiete, in denen sie sich selbst einbringen können.

Abkürzungen und Begriffe

AJAX	Asynchronous Javascript and XML. Eine „Technologie“ aus dem Bereich Webseiten-Programmierung die unter Anwendung dieser Sprachen Webseiten nur an den notwendigen Stellen „asynchron“ aufdatiert.
APRS	Automated Position Reporting System. Von Funkamateuren betriebener kooperativer Dienst zur Positions- und Meldungsübertragung.
ASCII	American Standard Code for Intermation Interchange. Wohlbekannter 7-Bit-Code aus der Urzeit amerikanischen Fernschreibens. Nicht umzubringen!
C3I	Eigentlich C^3I: In zivilen Quellen: „Command, Control, Communication and Information“ oder im militärischen Umfeld „Command, Control, Communication and Intelligence“. (Systeme) zur Kombination von Kommandostrukturen, Kommunikation und Information- bzw. Aufklärungsinformation zur Verbesserung der Lagebeurteilung zur Erzieleung einer besseren „Situation Awareness“.
DGPS	Differentielles (genauigkeitsverbessertes) GPS
DoS	„Denial of Service“; (gezielte) Unterbrechung des Betriebs eines Systems, Sabotage.
EGNOS	European Ground Navigation Overlay System. Euriopäische Initiative zur Übertragung von GPS-Korrekturdaten über geostationäre Satelliten im Rundstrahldienst.
GPRS	General Packet Radio Service. Standard zur Datenübertragung im GSM-Netz
GPS	Global Positioning System. Amerikanisches Satelliten-Navigationssystem.
GSM	„Groupe seciale mobile“ oder „Global Standard for Mobile cummunication“. Mobilfunkstandard
HTML	Hypertext Markup Language. Sprache zur Beschreibung von Inhalten im Internet.
HTTP	Hypertext Transfer Protocol. Protokoll oderhalb von TCP. Meist genutzt zur Übertragung von HTML-Inhalten.
IP	Internet Protocol. Unterstes Übertragungsprotokoll für Daten im Internet. Höhere Protokolle wie TCP und UDP bauen darauf auf..
LAMP	Linux, Apache, MySQL, PHP. Eine „Technologie“ aus der LINUX-Welt, die Web-Seiten unter Anwendung eben dieser Programmpakete dynamisch macht.
PDA	Personal Digital Assistant; Vertriebsbezeichnung für einen Taschencomputer.

SMS	Short Message Service. Kurztelegramm im GSM-Netz. Kann bis zu 160 Zeichen, die NICHT dem ASCII-Code entsprechen, übertragen.
TCP	„Transmission Control Protocol“. Ist ein verbindungsorientiertes Protokoll des IP-Stacks. Kein Schutz gegen Datenverlust. Keine kryptologische Funktion. Großer Overhead..
UDP	„User Datagram Protocol“. Ist ein verbindungsloses Protokoll des IP-Stacks. Schutz gegen Datenverlust. Keine kryptologische Funktion. Geringer Overhead.
UI	„Unnumbered Information“; Datensätze, die innerhalb von Packet Radio verbindungslos ausgetausch werden. Vergleichbar mit UDP bei IP.
UMTS	„Universal Mobile Telecommunication service“ Mobilfunkstandard.
UTF-8	8-bit Unicode Transformation Format. Codierungsvorschrift für UNICODE-Zeichen, die neben den lateinischen auch kyrillische, hebräische, arabische, koreanische etc. Schriftzeichen enthält. UTF-8 codierte Zeichen können bis zu 4 Byte umfassen und kann durch das trickreiche Codeschema bis zu 1.114.112 Zeichen codieren.
XML	Extensible Markup Language. HTML-ähnliche Sprache zur Codierung strukturierter Daten.

Quellen

[APRS]	„APRS in Deutschland“; www.aprs.de. siehe auch [WB4APR]
[C3I]	Blair, Sir Ian; „Command, Control, Communication and Information“; www.met.police.uk/c3i/
[DGPS]	Franke, E.H.; „Genauigkeitssteigerung bei GPS-basierenden Navigationssystemen“, Skriptum der 44. UKW-Tagung Weinheim, 1999; Quelle wie [EGNOS]
[EGNOS]	Franke, E.H.; „Galileo, GNSS, EGNOS und WAAS – Neues aus der Welt der Satellitennavigation“, Skriptum der 47. UKW-Tagung Weinheim, 2002; www.afusoft.com/website/medien/hamradio/publications/veroffentlichungen.html
[ESA]	„European Space Agency“; www.esa.int
[FLB]	„Daimler-Chrysler Services Fleetboard GmbH“; www.fleetboard.de
[GM]	“Google Maps”; www.google.com/apis/maps
[LBS]	Prof. Dr. Wunderlich, Thomas; „Positionsbestimmung für Location based Services“; www.intergeo.de/deutsch/page/kongress/downloads/archiv/2004/Wunderlich.pdf
[MP]	Microsoft Mappoint; http://www.microsoft.com/mappoint/default.mspx
[MUG]	Map and Guide; http://www.mapandguide.de/
[RASANT]	Galitzki et. al. „Realisierung des Echtzeit-Positionierungssystems EPS“ www.lverma.nrw.de/produkte/raumbezug/sapos/dienste/images/rasant11.pdf
[PHYS]	Dürrenmatt, F. „Die Physiker“; Diogenes;
[QC]	www.qualcomm.com
[SECW]	„AFUSOFT Security.WEB“, www.afusoft.com
[TA]	„Time Advance“-Wert. Dient der Laufzeitkorrektur im TDMA-Verfahren des GSM-Netzes
[TDMA]	Time domain Multiplex Access; Mehrfache Kanalnutzung durch Zeitschlitzverfahren
[TOLL]	„Web-Seite der Toll Collect GmbH“; www.toll-collect.de
[UEBW]	Franke, Dr. Pistor, Dr. Schmiedel; „Überwachungseinrichtung zur ständigen kontaktlosen Erfassung von mehreren beweglichen Objekten oder Gütern in Räumen oder Fahrzeugen mit drahtloser Weitermeldung der Entnahme oder Hinzufügung (Pat. Anm. 10 2005 005 962.7)“
[WB4APR]	Bruninga, B.; WB4APR; U.S. Navy Engineering&Weapons; http://eng.usna.navy.mil/~bruninga/aprs.html