Ein Konzept zur organisationsübergreifenden Integration von IT-Systemen für die zivile Sicherheit

Wolf Engelbach, Heiko Roßnagel, Sandra Frings

Competence Team Informationsmanagement
Fraunhofer IAO, Universität Stuttgart IAT
Nobelstr. 12,
70569 Stuttgart
[vorname.nachname]@iao.fraunhofer.de

Abstract: IT-Systeme zur Verbesserung der Reaktionsfähigkeit bei ungeplanten Ereignissen im Umfeld von Großveranstaltungen und öffentlichen Verkehrsinfrastrukturen müssen mehrere Bedingungen erfüllen: 1) die Zusammenarbeit zahlreicher, teilweise wechselnder Organisationen unterstützen, 2) auch im Normalbetrieb konkrete Vorteile bringen und 3) untereinander verbindbar sein, um komplexere Fragestellungen behandeln zu können. Die dafür vorgestellte Konzeption verfolgt einen offenen Ansatz für fachliche und informationstechnische Schnittstellen, der im Kontext konkreter Veranstaltungs- und Ereignisszenarien für Köln zusammen mit einem Rollenmodell hergeleitet wurde und erprobt wird.

1 Einleitung

Der öffentliche Personennahverkehr (ÖPNV) in deutschen Großstädten und Ballungsräumen bietet eine Infrastruktur, die sich sehr individuell und flexibel von Bewohnern, Beschäftigten und Besuchern dieser Regionen verwenden lässt. Dementsprechend hoch sind die Anforderungen an die Abwicklung des normalen Verkehrsgeschehens und zugleich die Herausforderungen, wenn vermehrte Anstrengungen zur Gewährleistung eines höheren Sicherheitsniveaus gefordert werden [BM09]. In vielen Metropolregionen finden zudem immer häufiger Großveranstaltungen statt, bei denen enorme Besucherströme bewältigt werden müssen. Dabei treten Belastungsspitzen im öffentlichen Personennahverkehr (ÖPNV) auf, was zu zahlreichen verkehrs- und sicherheitstechnischen Herausforderungen führen kann. Durch die steigende Anzahl an Großveranstaltungen und immer kürzere Vorlaufzeiten werden die Organisation und die Durchführung immer komplexer und zeitkritischer. Schwierigkeiten entstehen beispielsweise durch unzureichenden Informationsaustausch zwischen den Verantwortlichen, fehlende Informationsweitergabe an Teilnehmer und Fahrgäste, mangelhafte Schulungen des angeworbenen Sicherheitspersonals, knappe Finanzmittel der beteiligten Institutionen, uneinheitliches Datenmanagement der einzelnen Einsatzzentralen, eingeschränkten Informationsaustausch im Krisenfall sowie einer späten Erkennung von Krisenfällen [RE08]. Etablierte und neuartige IT-Instrumente bieten in dieser Situation die Chance, mehr Transparenz zu erlangen, virtuell Optionen und ihre Auswirkungen durchzuspielen sowie die Kommunikation zwischen Akteuren zu verbessern [TC04] [YD05].

Ziel des durch das BMBF im Rahmen des Programms "Forschung für die zivile Sicherheit" [BM09] als Teil der High-Tech-Strategie geförderten Forschungsprojekts VeRSiert [PV08] ist es daher, eine bessere organisatorische und informationstechnische Vernetzung von Nahverkehrsgesellschaften, Einsatzkräften, Veranstaltern und Fahrgästen zu erreichen, um die Sicherheit im ÖPNV bei Großveranstaltungen zu erhöhen. Eine wesentliche Vorraussetzung dafür ist es ein Konzept zur organisationsübergreifenden Integration von IT-Systemen. Dieser Beitrag stellt ein solches Konzept vor. Dafür werden in Abschnitt 2 verwandte Arbeiten betrachtet. In Abschnitt 3 werden der Untersuchungskontext dieser Arbeit präsentiert und die besonderen Herausforderungen in Bezug auf zivile Sicherheit im ÖPNV abgeleitet. Für diesen Untersuchungskontext wurde ein Rollenmodell erarbeitet, das in Abschnitt 4 vorgestellt wird. Dieses Rollenmodell dient als Grundlage für die IT-Gesamtkonzeption, die in Abschnitt 5 präsentiert wird, bevor die wesentlichen Ergebnisse des Beitrags in Abschnitt 6 zusammengefasst werden.

2 Verwandte Arbeiten

Mit den Herausforderungen zur Gestaltung von IT-Systemen für Sicherheitsfragen im Zusammenhang mit ÖPNV haben sich teilweise auch schon andere Projekte, insbesondere mit Förderung der EU, auseinander gesetzt [DS09]; derzeit laufen zudem zahlreiche Projekte zum Schutz kritischer Infrastrukturen innerhalb des Programms "Forschung für die zivile Sicherheit". Sie haben dabei allerdings immer bestimmte Schwerpunkte gelegt, die aufgegriffen werden können, aber den Kern des hier vorgestellten Ansatzes nicht berühren. Wichtige Anregungen enthalten:

MODURBAN, das bis 2008 lief, zielte auf die Definition von Systemarchitekturen und IT-Schnittstellen, um die Betriebskosten von Nahverkehrssystemen zu reduzieren. Hierbei ging es insbesondere um die Schnittstellen innerhalb von und zwischen Verkehrsunternehmen sowie innerhalb einer Gattung von IT-Systemen wie Fahrgastinformationen oder Videoüberwachung [MOD09]. Der Ansatz dieses Artikels hat einen Schwerpunkt auf der Kooperation verschiedener Akteursgruppen und heterogener IT-Systeme.

Das laufende Projekt **MODSAFE** adressiert die Definition von Sicherheitsanforderungen, beispielsweise Sicherheit vor kriminellen Aktivitäten, und der dafür sinnvollen Rollenmodelle und Zertifizierungsprozesse im ÖPNV [MB09]. Der in diesem Artikel vorgestellte Ansatz geht hinsichtlich der Umsetzung in IT-Systemen weiter, kann aber die inhaltlichen Vorstellungen aufgreifen.

Das 2009 beendete Projekt **COUNTERACT** bereitete Grundlagen zur Verbesserung der Sicherheit gegen terroristische Anschläge auf, u.a. für Akteure im ÖPNV [CO09]. Die Problemanalysen und Handlungsanregungen sind stark organisatorisch ausgerichtet und können in die hier vorgestellte IT-Architektur eingebracht werden.

Das 2010 endende Projekt **DEMASST** erarbeitet eine Vision für System-of-System-Lösungen bezogen auf Sicherheitsanforderungen im öffentlichen Personenverkehr [AN09]. Die vorliegenden Zwischenergebnisse werden für den hier vorgestellten Ansatz aufgegriffen und erweitert.

3 Erprobungskontext Großveranstaltungen in Köln

Das Forschungsprojekt VeRSiert zielt für das Beispiel Köln darauf ab, bei Großveranstaltungen durch eine optimierte Vernetzung von Verkehrsgesellschaften, Einsatzkräften, Veranstaltern und Fahrgästen die Sicherheit insbesondere im öffentlichen Personennahverkehr zu erhöhen. Die Kölner Verkehrsbetriebe (KVB), die Stadt Köln, der Nahverkehr Rheinland als Projektkoordinator sowie anderer Anwender in Köln bringen dazu ihre vielfältigen Erfahrungen bezüglich des Managements von Großveranstaltungen, der Zusammenarbeit und des Umgangs mit ungeplanten Ereignissen ein. Zur Gewährleistung größtmöglicher Sicherheit bei Großveranstaltungen werden dabei die Phasen der Vorbereitung, Durchführung (inkl. An- und Abreise) und Nachbereitung betrachtet [HE04]. Im Projekt werden organisatorische Maßnahmen und die differenzierte Nutzung von Informations- und Kommunikationstechniken sowie Schulungskonzepte analysiert, konzipiert, umgesetzt, modellhaft erprobt und empirisch evaluiert. Die folgenden organisatorischen und informationstechnischen Bausteine von VeRSiert sind für sich selbständig konzipiert, können aber auch fachlich und informationstechnisch miteinander vernetzt eingesetzt werden: Informations- und Kooperationsportal, Simulations-, Videoanalyse-, Mobile-Dienste- und Sicherheitsbefragungs-Plattformen sowie Bausteine zur Mitarbeiterschulung und zum Verkehrsmanagement [PV08].

Leitfadengestützte Befragungen und veranstaltungsorientierte Prozess- sowie Aufgabenanalysen bei Kölner Akteuren haben einen Überblick zur Planung, Durchführung und Nachbereitung von Großveranstaltungen verschafft, insbesondere bezogen auf organisationsübergreifende Zusammenarbeit. Dabei bestehen seitens der Veranstalter, der Genehmigungsbehörde, der Fachbehörden, der Verkehrseinrichtungen sowie der Sicherheitskräfte unterschiedliche Interessen und Anforderungen hinsichtlich einer informationstechnischen Unterstützung der eigenen Aufgaben sowie der Zusammenarbeit. Damit die IT-Potenziale konstruktiv genutzt werden können, lassen sich aus den Analysen mehrere Anforderungen ableiten und durch frühere Untersuchungen bestätigen:

1) Es ist die Zusammenarbeit zahlreicher, teilweise wechselnder Organisationen zu unterstützen, die für den Verkehrsablauf oder für Sicherheitsfragen in einer Region oder für eine bestimmte Zeit verantwortlich sind [MJ07]. Innerhalb komplexer Zusammenhänge von Verkehrsnetzen und Stadtsystemen haben Entscheidungen einzelner Akteure gravierende Auswirkungen auf andere Verantwortungsbereiche und sollten entsprechend zwischen ihnen abgestimmt oder zumindest untereinander transparent sein.

2) Die dafür einzusetzenden IT-Systeme sollen nicht nur in Krisensituation zum Einsatz kommen, sondern gerade auch im Normalbetrieb konkrete Vorteile bringen [MH07]. Nur dann ist zu erwarten, dass in sie investiert wird und dass Benutzer mit diesen Systemen umgehen können. Für Verkehrsunternehmen sind dabei Vandalismus und Schlägereien als alltägliche Sicherheitsherausforderungen eher eine Motivation zum Handeln als ungewiss erscheinende Ereignisse wie terroristische Attentate. Generell sind daher eher für viele Risiken einsetzbare IT-Systeme als sehr spezialisierte zu bevorzugen.

3) IT-Systeme sollen untereinander flexible verbindbar sein, um auch komplexere Fragestellungen behandeln zu können. Dabei ist die heterogene Ausgangslage hinsichtlich der

vorhandenen IT-Infrastruktur bei den beteiligten Akteuren zu berücksichtigen. Zugleich können so die vielen möglichen zukünftigen Sicherheitslösungen einfacher integriert werden, egal ob sie sich auf Arbeitsabläufe, organisatorische Zuständigkeiten oder auf neue IT-Systeme beziehen.

Um das Zusammenwirken aller Konzepte im Blick zu behalten und die exemplarische Demonstration des Zusammenspiels zu fördern, wurden zwei wesentliche verbindende Grundlagen abgestimmt, auf denen alle konzeptionellen Aktivitäten aufbauen und durch die miteinander kompatible Ergebnisse gesichert werden. Durch diesen Ansatz können durchgängige Arbeitsprozesse einfacher informationstechnisch demonstriert werden:

- **Arbeitsszenarien:**
  Alle Projektbausteine orientieren sich an den drei Veranstaltungsszenarien „Fußball-Bundesligaspiel“, „Kölner Lichter“ und „Deutscher Evangelischer Kirchentag“ sowie an sieben Szenarien ungeplanter Ereignisse: Terroristischer Anschlag, Unwetter, Personenschaden mit Todesfolge, Defekt einer U-Bahn, Amoklauf in Straßenbahn, Bombendrohung, Sperrung des Hauptbahnhofes aufgrund Fehleinschätzung [RO08].
- **Untersuchungsräume:**
  Empirische Erhebungen und Demonstrationselemente, die sich nicht auf ganz Köln beziehen, werden exemplarisch für die gemeinsamen Untersuchungsräume „Kölner Hauptbahnhof“ sowie „Haltestellenbereich Rhein-Energie-Stadion“ konkretisiert.

4 Gemeinsames Rollenmodell

Für die stringente Verwendung der verschiedenen Bausteine ist darüber hinaus ein gemeinsames Rollenmodell entwickelt worden. Dies dient der begrifflichen Klarheit der Kommunikation und schärft das gemeinsame Verständnis über Zielgruppen und Anwendungsfälle. Zugleich stellt es sicher, dass zentrale Akteursarten und Gesichtspunkte für alle Bausteine und Plattformen beachtet werden. Ergänzend lassen sich so Überlegungen zu einer teilweise gemeinsamen Benutzerverwaltung und abgestimmter Berechtigungsstufen anstellen. Die Diskussion von Rollen für die Bausteine und Plattformen umfasst drei klar unterscheidbare Abstraktionsebenen:

- **Veranstaltungswelt (Objektebene):** Personen, die bei einer Veranstaltung unterwegs sind, d.h. sich währenddessen in den relevanten Gebieten bewegen.
- **Organisationswelt (Managementebene):** Personen, die für die Planung, Durchführung und Nachbereitung einer Veranstaltung zuständig sind und sich währenddessen teilweise in diversen Leitstellen und Organisationszentralen befinden.
- **Systemwelt (Metaebene):** Personen, die inhaltlich oder informationstechnisch mit den Plattformen arbeiten, teilweise jedoch nicht während einer Veranstaltung.

Für diese drei Abstraktionsebenen wurde spezifisch für die Bausteine und Plattformen diskutiert, welche Rollen relevant sein können. Für alle diese Bausteine wurde das folgende gemeinsame Rollenmodell abgeleitet und jeweils instanziiert (siehe Abb. 1).

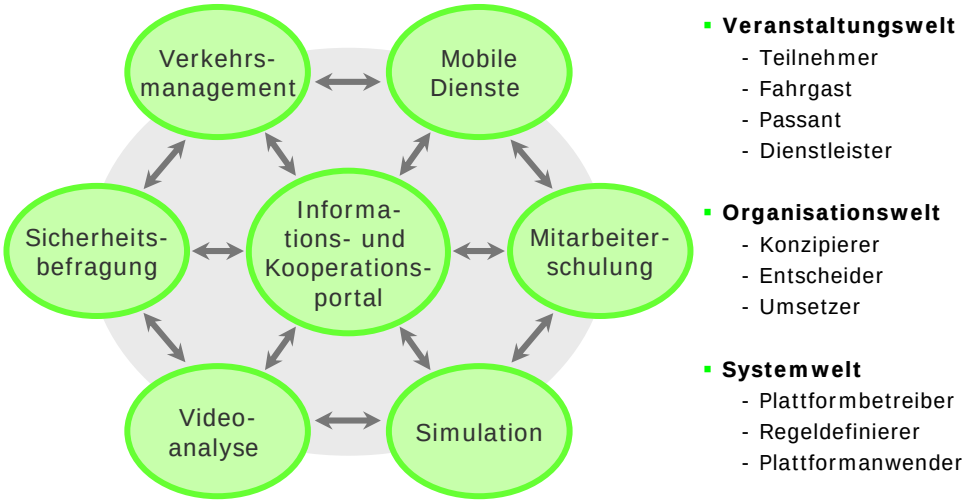

Abb. 1: Gemeinsames Rollenmodell der Bausteine von VeRSiert

5 IT-Gesamtkonzeption

IT-Systeme müssen modular aufgebaut und einfach kombinierbar sein, um den oben genannten Bedingungen zu genügen. Der Ansatz eines solchen „Systems-of-Systems“ erlaubt dabei die Interoperabilität von unabhängig voneinander gestalteten IT-Systemen. So können auch IT-Systeme für das alltägliche Verkehrsmanagement mit solchen interagieren, die für spezielle Sicherheitsherausforderungen ausgelegt sind. Alle Systeme behalten dabei ihre operative Eigenständigkeit und bleiben in der Verantwortung unterschiedlicher Akteure, können aber zugleich Informationen austauschen, um bessere Grundlagen für Entscheidungen in gerade in kritischen Situationen bereit zu stellen. Zugleich sind auf Grundlage solcher modularer IT-Systeme die Realisierung unterschiedlicher organisatorischer Konzepte (Zuständigkeiten und Arbeitsabläufe) sowie die Unterstützung konkreter Betriebsaufgaben und Sicherheitsanliegen möglich. Dies wurde für den geschilderten Untersuchungskontext ausgearbeitet und wird derzeit erprobt, die folgenden Ansätze erscheinen aber über den Einzelfall hinaus übertragbar zu sein.

Die technische (syntaktische) Interoperabilität bildet so die Basis für die inhaltliche (semantische) Interoperabilität, auch über Organisationsgrenzen hinweg. Um eine solche Modularität von IT-Systemen sicherzustellen, muss eine Gesamtarchitektur die notwendigen Schnittstellen und einige gemeinsam zu verwendende Standards und Begriffskonventionen abstimmen [BA2007]. Darüber hinaus sind die Zugriffsrechte zwischen Institutionen ein zentrales Anliegen, das der Klärung bedarf. Letztendlich sind zur Erschließung der Synergiepotenziale abgestimmte Arbeitsabläufe für spezifische Sicherheitsanliegen notwendig, die auf gemeinsamen konzeptionellen Modellen beruhen sollten. Aus diesen vielschichtigen Anforderungen wird deutlich, dass ein solcher Abstimmungsprozess langwierig und komplex werden kann.

5.1 Fachliche Schnittstellen

Je klarer gemeinsame fachliche Sicherheitsanliegen formuliert sind, desto einfacher können die erforderlichen IT-Anforderungen definiert werden. Ein abstrakter Klärungsprozess kann hingegen schnell an politischen und organisationalen Grundsätzen oder Partikularinteressen scheitern. Im Projekt VeRSiert wurden daher ausgehend von den definierten Szenarien, Untersuchungsräumen und Rollenmodellen fachliche Schnittstellen zwischen den Bausteinen zur Unterstützung von Einsatzfällen definiert. Anschließend erfolgte die erforderlichen Festlegungen auf IT-Standards und IT-Schnittstellen.

Abbildung 2 benennt zentrale inhaltliche Schnittstellen; beispielsweise werden Zählergebnisse der Videoanalyse an die Simulation übergeben (unterste Zeile der Abbildung). Hierbei erfolgt auf Seiten der Videoanalyse eine Aggregation und Auswertung, z.B. auf 5-Minuten-Intervalle. Die Übertragung kann im einfachsten Falle täglich durch Ablage einer strukturierten Datei an einem definierten Ort erfolgen, oder aktiv für jedes Zählergebnis übermittelt werden. Darüber hinaus wurden zwischen fast allen Bausteinen in beide Richtungen interessante fachliche Berührungspunkte identifiziert werden. Ob ein IT-unterstützter Austausch dabei über zentrale Schnittstellen der Gesamtarchitektur, durch bilaterale Lösungen oder überhaupt nicht erfolgt, ist in einigen Fällen noch offen.

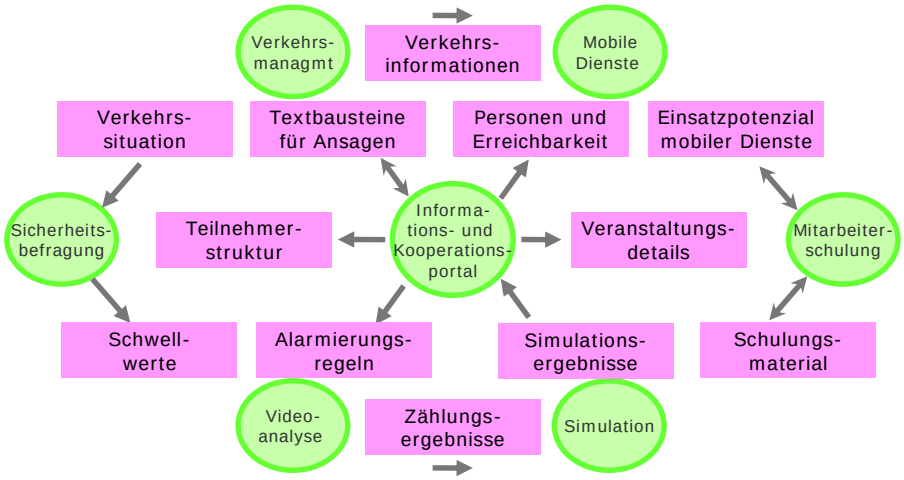

Abb. 2: Fachliche Schnittstellen im Gesamtsystem von VeRSiert

5.2 Informationstechnische Standards

Insgesamt ist zu erkennen, dass jeder Baustein fachliche Module anderer Bausteine zur Steigerung seines Wertes verwenden kann. Die Ansätze können teilweise auch rein organisatorisch unterstützt werden. Weitergehend können Inhalte, Funktionalitäten oder Regeln einzelner Plattformen auch informationstechnisch über andere Plattformen zur Verfügung gestellt und so eine durchgängige Unterstützung von Rolleninhabern bei Veranstaltungs- und Ereignisszenarien realisiert werden. Das Gesamtsystem bietet so mehr Funktionalitäten und Komfort als die Summe der einzelnen Plattformen.

Die inhaltlichen Berührungspunkte müssen dafür informationstechnisch realisierbar sein. Die jeweiligen Entwicklungsumgebungen der Plattformen standen jedoch überwiegend schon vor Projektbeginn fest und können durch das Projekt nicht vereinheitlicht werden. Entsprechend wurden für den Austausch im Projekt klare Richtlinien und etablierte Formate definiert, wie Daten oder Informationen von einer Plattform auf eine andere übergeben (materielle Integration) bzw. plattformübergreifend verwendet (virtuelle Integration) werden können. Die Semantik (inhaltlichen Anforderungen) ist zwischen den kommunizierenden Plattformen jeweils bilateral abzustimmen (z.B. Zeitstempel, Ort, Anzahl, …). Dabei ist neben der gleichen Datenstruktur insbesondere die fachliche Kongruenz zu beachten, also dass gleich benannte Inhalte auch die gleiche Bedeutung haben. Als einheitliche Syntax (Datenstruktur) wird XML angestrebt, da es wegen der Baumstruktur flexibler als einfacher zu erzeugende Datenformate wie csv ist. Der Informationsaustausch soll über offene Protokolle realisiert werden (http, ftp, SOAP).

Als aufruforientierte Übergabeform („pull“) werden XML-RPC (Remote Procedure Calls) oder WebServices angestrebt, als einfache aktive Übergabeform („push“) von Inhalten können RSS-Feeds verwendet werden; dieser hybride Ansatz wird den bestehenden fachlichen Anforderungen am besten gerecht. Für Video-Sequenzen werden Standardformate wie MPEG eingesetzt, für Audio-Aufnahmen MP3. Bilder werden als JPEG, als Referenz gedachte Pläne und Dokumente als PDF abgelegt. Sofern jeweils bilateral geeignet, können auch die lokalen Interfaces der einzelnen Plattformen verwendet werden. Es können zudem systemweite Software-Agenten eingesetzt werden, die den Datenfluss automatisch überwachen und dann nach vordefinierten Regeln Ereignisse in bestimmten IT-Systemen auslösen. Auch gemeinsame Modellbibliotheken, beispielsweise zur Ablage von Regeln und Funktionen, sind möglich.

Bei der konkreten Klärung von Austauschwegen für die fachlichen Anforderungen ist beispielsweise zu prüfen, ob ein Datenaustausch „in Echtzeit“ oder „zeitversetzt“ erfolgen soll. Für eine weitere Verfolgung der Integrationsoptionen kann auch auf Erfahrungen und Lösungen anderer Kölner Integrationsprojekte zurückgegriffen werden, insbesondere für den Ansatz von „Mobil im Rheinland“ [MR09]. Je nach weiterer Konkretisierung von Geschäfts- und Betreibermodellen ist eine interne Verrechnung von gegenseitig zur Verfügung gestellten Informationen oder Funktionalitäten denkbar, für die dann entsprechende Monitoring- und Auswertungsstandards definiert werden müssten.

6 Zusammenfassung und Ausblick

Dieser Artikel leitet die Anforderungen an eine IT-Architektur her, die für Sicherheitsszenarien bei Großveranstaltungen eine pragmatische Unterstützung der vielfältigen beteiligten Akteure bieten. Diese Konzeption wird derzeit im Rahmen des Projektes VeRSiert mit verschiedenen zusammenspielenden IT-Bausteinen erprobt. Wenn ein solcher Ansatz den Status von Demonstratoren verlässt und in den operativen Einsatz übergeht, sind weitere Hürden zu nehmen, angefangen von der Konfiguration von Firewalls bis hin zu möglichen haftungsrechtlichen Fragen bei zunehmender Informationstransparenz. Auch jede einzelne Organisation kann ihre Arbeitsprozesse ggf. mit Hilfe solcher interoperablen IT-Systeme optimieren.

Der Ansatz ist insbesondere dann erfolgreich, wenn er die alltäglichen Aufgaben ebenso unterstützt wie eher hypothetische Krisenszenarien. Zudem könnte sich die Frage nach Kostenaufteilungen zwischen Informationsanbietern und Informationsnutzern stellen. Ggf. haben die Informationsanbieter aber auch ein Interesse an der Nutzung ihres Wissens durch andere Akteure, weil so gemeinsam bessere Handlungsweisen möglich werden. Wenn die Anbieter von IT-Systemen für Verkehrsmanagementaufgaben wie für Sicherheitsfragestellung die notwendigen Schnittstellen unterstützen, ist es für zukünftige Einsatzszenarien einfacher, sie entsprechend der geschilderten Vision von Kooperationen zu realisieren.

7 Literatur

[AN09] Eriksson, E.A.: Briefing for EC/DE workshop: System-of-Systems Demonstration & Experimentation for Mass Transport Security, Sept. 2009 (DEMASST Deliverable 6.1)

[BA07] Botterell, A. and Addams-Moring, R. (2007) Public Warning in the Networked Age: Open Standards to the rescue?, Communications of the ACM, 50, 3, 59-60.

[BM09] Bundesministerium für Bildung und Forschung (BMBF, Hrsg.): Forschung für die zivile Sicherheit. Schutz von Verkehrsinfrastrukturen, 2009

[CA09] Cluster Of User Networks in Transport and Energy Relating to Anti-terrorist ACTivities, http://www.counteract.eu/

[DS09] Delle Site, P.; Salucci, M.V.: Urban Transport. Thematic Research Summary. Transport Research Knowledge Center, 2009

[HE04] Heinze, G. W. (2004) Klassifikation von Events, in H. Dienel and J. Schmithals (Eds.), Handbuch Eventverkehr - Planung, Gestaltung, Arbeitshilfen, Erich Schmidt Verlag, Berlin, 25-35.

[MB09] Model-Based Safety Evaluation of Automation Systems, http://www.modsafe.eu/

[MH07] Manoj, B. S. and Hubenko Baker, A. (2007) Communication Challenges in Emergency Response, Communications of the ACM, 50, 3, 51-53.

[MJ07] Mendonca, D., Jefferson, T. and Harrald, J. (2007) Collaborative Adhocracies and Mix-and-Match Technologies in Emergency Management: Using the emergent interoperability approach to address unanticipated contingencies during emergency response, Communications of the ACM, 50, 3, 45-49.

[MR09] Mobil im Rheinland, http://www.mobil-im-rheinland.de/

[MU09] Modular Urban Guided Rail System, http://www.modurban.org/

[PV08] Projekt VeRSiert (2008) Homepage, http://www.versiert.info/, accessed 2009-08-01.

[RE08] Roßnagel, H., Engelbach, W., Frings, S. and Weisbecker, A. (2008) Mobile Dienste zur Erhöhung der Sicherheit bei Großveranstaltungen, in D. Spath, O. Höß and A. Weisbecker (Eds.), Stuttgarter Softwaretechnik Forum 2008: Science meets Business, 2008-11-28, Fraunhofer IRB Verlag, Stuttgart, 91-102.

[RO08] Rossnagel, H., Engelbach, W., Frings, S.: Ortsbezogene mobile Dienste zur Verbesserung der Sicherheit bei Großveranstaltungen, in J. Roth (Eds.), Tagungsband 5. Fachgespräch Ortsbezogene Anwendungen und Dienste, Nürnberg, 2008, S. 35–40

[TC04] Turoff, M., Chumer, M., Van de Walle, B. and Yao, X. (2004) The Design of a Dynamic Emergency Response Management Information Systems (DERMIS), Journal of Information Technology Theory and Application (JITTA), 5, 4, 1-36.

[YD05] Yuan, Y. and Detlor, B. (2005) Intelligent Mobile Crisis Response Systems: Systems to help coordinate responder communication and response efforts in order to minimize the threat to human life and damage to property, Communications of the ACM, 48, 2, 95-98.