Marco Bettelini, Amberg Engineering AG, Nikolaus Seifert, ASIT AG,
François Bry, Ludwig-Maximilians-Universität München

Innovatives Sicherheitssystem für U-Bahn-Stationen

Große kritische Infrastrukturanlagen in verschiedenen Bereichen unserer Gesellschaft sind zunehmend anfällig auf Störungen, bei Notfällen oder gar bei Angriffen. Die wachsende Automatisierung und die Verfügbarkeit von neuen Technologien eröffnen gleichzeitig neue Möglichkeiten. Im EU-Forschungsprojekt EMILI werden zurzeit die Grundlagen erarbeitet, mit denen die neue Generation von Steuerungssysteme schneller und zuverlässiger gemacht werden kann.

Keywords
Critical infrastructure – Metro – Control system - EMILI
Stichworte
Kritische Infrastruktur – Metro – Steuerung – EMILI

1. Einleitung

Zeitungsmeldung: Neues Notfall-Managementsystem verhindert Katastrophe in U-Bahnhof:
Im Jahr 2010 hatte die lokale U-Bahn Verkehrsgesellschaft ein Notfall-Managementsystem der neuesten Generation eingeführt. Am Montag, dem 27. Juni 2011 um 16:47 Uhr, kurz vor Beginn der Berufsverkehrszeit, legte ein Mann auf einem Bahnsteig der U-Bahnstation Stadtmitte mit Hilfe von einigen Litern brennbarerer Flüssigkeit ein Feuer, das schnell auf einen am Bahnsteig stehenden Zug übergriff. Innerhalb von wenigen Sekunden entdeckten die Sensoren des Überwachungssystems den Rauch und das Notfall-Managementsystem hatte die Situation analysiert. Nur eine halbe Minute nach Detektion des Feuers war eine Strategie zur Ereignisbewältigung identifiziert und der Stationsverantwortliche in der Leitstelle konnte die umgehende Evakuierung der vierstöckigen Station einleiten. Mit Hilfe des Notfall-Managementsystems wurden die in Richtung der brennenden Station fahrenden Züge an sicheren, rauchfreien Orten gestoppt und durch Aktivierung von Leitsignalen sowie spezifischer Lautsprecherdurchsagen die Räumung des Bahnhofs unterstützt. Nach der Ermittlung der wirksamsten Lüftungs- und Rauchführungsstrategie durch das Managementsystem wurden entsprechende Ventilatoren und Rauchschutzsysteme aktiviert. Die Feuerwehr konnte auf rauchfreien Wegen rasch zum Brandherd vorrücken und das Feuer bekämpfen. Obwohl beträchtliche Schäden entstanden, waren keine Opfer zu beklagen. Die Hitzeeinwirkung mit Temperaturen von ca. 1100°C führte 37 Minuten nach Feuerausbruch zu schweren Beschädigungen an der Deckenstruktur am Bahnsteig über dem Brandherd sowie an einigen Wagen.
Die Auswertung der Logbuch-Einträge im Notfall-Managementsystem zeigte, dass zwischen 950 und 1.250 Personen innerhalb von 19 Minuten von allen 6 Bahnsteigen der Station evakuiert worden waren. Der Sicherheitsverantwortliche der Verkehrsgesellschaft erklärte: „Das Notfall-Managementsystem mit der innovativen Logik zur Evaluierung von komplexen Ereignissen (Complex Event Processing) zeichnet sich durch eine schnelle und automatische Ausführung komplexer Abläufe aus und ermöglicht, dank der hochentwickelten Fähigkeit zur aerodynamischen Modellierung von Brandszenarien in U-Bahn-Stationen, rasche und präzise Vorhersagen hinsichtlich der Entwicklung des Szenarios (z.B. Rauchausbreitung) im Hinblick auf eine sichere Evakuierung".

2. Wachsende Anforderungen an das Notfall-Management

Große kritische Infrastrukturanlagen in verschiedenen Bereichen unserer Gesellschaft sind sehr anfällig auf Störungen, bei Notfällen oder gar bei Angriffen. Denken wir zum Beispiel an die verheerenden Folgen beim Ausfall eines großen Stromverteilnetzes oder an größere Störungen / Notfälle bei öffentlichen Transportsystemen oder Flughäfen. Die politische Integration und die wirtschaftliche Globalisierung führen zu wachsenden internationalen Vernetzungen und Abhängigkeiten. Die zunehmende Auslastung der vorhandenen Infrastrukturen, gekoppelt mit dem wachsenden

Kostendruck und dem Einsatz von neuen Technologien, erhöht die Anfälligkeit weiter dramatisch. So nimmt die Transportkapazität in Bahn- und Metrosystemen ständig zu und der Fahrplan wird verdichtet. Auch geringfügige technische Störungen können so zu weit reichenden Verkehrsbehinderungen führen. Diese Entwicklung ist auch sicherheitstechnisch von Bedeutung. Das mögliche Schadenspotential im Ereignisfall kann aufgrund der wachsenden Anzahl der Benutzer und der Abhängigkeiten der Systeme drastisch ansteigen.

Die zunehmende Automatisierung bei kritischen Infrastrukturen und die Verfügbarkeit von neuen Technologien eröffnen gleichzeitig neue Möglichkeiten. Dies betrifft unter anderem die Bereiche Detektion (Sensorik), Datenübermittlung und Rechenleistung. Die neuen Technologien und Systeme sind schneller, zuverlässiger und leistungsfähiger. Aber solche Möglichkeiten werden heute nur unzureichend genutzt. Kritische Infrastrukturen werden immer noch in hohem Masse von verhältnismäßig einfachen Überwachungs- und Kontrollsystemen gesteuert und sind vom Leitstellenpersonal abhängig, dessen Aufgaben immer komplexer und anspruchsvoller werden. Im Ereignisfall liefern moderne Tunnelausrüstungen und Steuerungssysteme eine Fülle von verschiedenen Signalen, welche das Personal im Kontrollraum rasch überfordern kann. Ein adäquates Filtern der umfangreichen Datenmengen ist heute kaum möglich und viele sicherheitsrelevante Entscheidungen werden aufgrund von vereinfachten und unvollständigen Informationen sowie Handlungsanweisungen getroffen. Kritische Infrastrukturen sind deswegen häufig suboptimal gesteuert.

Innovative Konzepte sind in die neue Generation von Notfall-Managementsystemen zur Steuerung und Überwachung von kritischen Infrastrukturen eingeflossen, welche in der Lage sind, die Informationen aus der umfangreichen Sensorik umfassend zu analysieren, komplexe Muster zu erkennen, die sicherheitstechnisch optimale Lösung zu finden und diese automatisch umzusetzen. Zum Teil widersprüchliche Einzelsignale werden im Ereignisfall rasch zu einer konsistenten Abbildung der Situation verarbeitet. Handlungsoptionen werden, basierend auf fortschrittlichen Simulationstechnologien, vollautomatisch in kürzester Zeit untersucht und verglichen, um die optimale Ereignisbewältigungsstrategie zu identifizieren. Die so ermittelte optimale Betriebsweise der technischen Ausstattungselemente sowie der Evakuierungs- und Interventionsstrategie werden weitgehend automatisch umgesetzt. Der Vorgang der Entscheidungsfindung und – ausführung ist somit schneller, zuverlässiger, umfassender und bleibt von Stressfaktoren weitgehend unbeeinträchtigt.

3. Aus der Vergangenheit lernen

Aus katastrophalen Ereignissen der Vergangenheit können Lehren für die Anwendung in den modernen Notfall-Managementsystemen gezogen werden. Eurotunnel (1996), Montblanc-Straßentunnel (1999), Gotthard-Straßentunnel (2001), Seilbahn Kaprun (2000), Flughafen Düsseldorf (1996), Metrostation Daegu (2003), Bahnhof Viareggio (2009) sind zum Teil gewöhnliche, zum Teil große Infrastrukturanlagen, welche bei Sicherheitsexperten vor allem Erinnerungen an verheerende Brandereignisse wecken. Sehr unterschiedliche Verkehrsinfrastrukturen, sehr unterschiedliche Nutzungen, teils modern teils veraltet: Egal bei welcher Infrastruktur, nach dem Ereignis konnten die Experten viele vermeidbare Ursachen entdecken, obwohl in der Sicherheitsplanung vor dem Ereignis davon kaum die Rede war. Brandereignisse in Verkehrsinfrastrukturen sind glücklicherweise extrem selten, doch man ist nicht immer gut darauf vorbereitet. Welche Lehren kann man aus der Vergangenheit ziehen, um nicht immer wieder von katastrophalen Brandereignissen „überrascht" zu werden?

Die eigentlichen Initialereignisse können sehr unterschiedlicher Art sein: Technische Defekte (z.B. Eurotunnel, Montblanc, Kaprun, Viareggio), Verkehrsunfall (z.B. Gotthard), menschliches Versagen bei Unterhaltsarbeiten (z.B. Düsseldorf), Brandstiftung (Daegu). Die Eskalation zum Großereignis hängt aber immer von einer ungünstigen Verkettung von Folgeereignissen ab. Dies soll anhand von zwei Beispielen illustriert werden:

Beim schwersten Brandunglück in einer U-Bahn im Jahre 2003 in der koreanischen Stadt Daegu starben 197 Fahrgäste, an die 150 wurden verletzt. Ein geistig verwirrter Mann hatte während der Fahrt in einem Zug mit Hilfe einer brennbaren Flüssigkeit Feuer gelegt, offensichtlich um sich selbst zu verbrennen und dabei möglichst viele Fahrgäste ebenfalls zu töten. Innerhalb weniger Minuten hatte das Feuer alle sechs Wagen erfasst. In den Wagen waren brennbare Materialien verbaut, die beim Verbrennen einen dicken, giftigen Rauch erzeugten. Der Zugführer informierte die Leitstelle nicht direkt nach Ausbruch des Feuers. Nach dem Halt des brennenden Zuges in der Station fuhr 4 Minuten später der Gegenzug auf dem Nachbargleis ein. Erst teilte der Zugführer dieses zweiten Zuges den Fahrgästen mit, sie sollen noch im Zug bleiben, da sie sofort weiterfahren könnten. Kurz darauf wurde die Stromversorgung unterbrochen, sodass dieser Zug die Station nicht wieder verlassen konnte. Schließlich bekam der Zugführer von der Leitstelle die Aufforderung, den Zug schnellstens zu verlassen. Dabei entfernte er den Hauptschlüssel der Komposition, wodurch die Stromversorgung der Türen über die Bordbatterien unterbrochen wurde und dadurch die Fahrgäste im Zug eingeschlossen waren.

Die meisten Todesopfer waren im zweiten Zug zu beklagen, dessen Einfahrt in den Bahnhof und dessen Halt durch eine rasche Reaktion wohl problemlos hätte verhindert werden können. Zweifellos eine unglückliche Verkettung, bei welcher aber tragisches Fehlverhalten der Zugführer und anderer Entscheidungsträger eine maßgebende Rolle spielte. Zudem waren auch die unzureichende Ausrüstung des Rollmaterials sowie strukturelle Mängel bei Sicherheitsmassnahmen in der Station (fehlende Sprinkleranlagen, fehlende Rauchschutzsysteme und Rauchkontrolleinrichtungen, etc.) verantwortlich für das katastrophale Ausmass.

Am 11. April 1996 brach im Flughafen Düsseldorf ein Brand in der besetzten Ankunftshalle im Terminal A aus. Der Grund war Unachtsamkeit bei Schweißarbeiten an der Zwischendecke des Gebäudes. Die Brandentwicklung blieb zunächst recht lange unentdeckt. Nach der Durchzündung in die Halle entwickelte sich die Brandausbreitung sehr schnell. Zahlreiche strukturelle und tech-

nische Mängel (z.B. die Verwendung brennbarer Materialien, fehlende Löschsysteme, unzureichende Löschwasserversorgung, unzureichende Fluchtwege) waren für die tragische Bilanz mitverantwortlich: 17 Menschen kamen ums Leben und weitere 62 Personen erlitten Verletzungen. Besonders tragisch war das Schicksal von insgesamt 7 Menschen, welche in zwei Aufzügen ums Leben kamen. Sie hatten versucht, von der Zuschauerzone auf dem Dach des Flughafengebäudes bzw. vom Parkdeck im Untergeschoss mit dem Aufzug in die Ankunftshalle zu gelangen. Die Aufzüge fuhren in die verrauchte Halle und die Türen öffneten sich. Die Menschen starben durch die dichten giftigen Rauchgase in den Aufzügen. Andere Todesopfer waren in Lounge-Bereichen zu beklagen, nachdem die auf Umluft geschaltete Lüftungsanlage im Gebäude Rauch und giftige Brandgase dorthin eingeblasen hatte. Nur durch grobe Fehler in den Überwachungs- und Kontrolleinrichtungen sowie beim Notfallmanagement war eine solche Eskalation überhaupt möglich. Neben den zu beklagenden Todesopfern und den vielen Verletzten waren auch extreme Gebäudeschäden von mehreren Hundert Millionen DM entstanden.

Veraltete oder unzureichende technische Systeme, falsche oder zu langsame Systemreaktionen, menschliches Fehlverhalten: Jede Brandkatastrophe der Vergangenheit wurde von einer Kombination solcher Elemente verursacht und/oder begünstigt. Was sind die Lehren, welche der Planer, der Manager und die Behörden daraus ziehen sollten? Vier Elemente stehen zweifellos im Vordergrund:

1. Die technische Infrastruktur muss von kompetentem Fachpersonal geplant werden, welches die komplexen Zusammenhänge im Ereignisfall kennt und meistern kann, und sie soll möglichst auf dem Stand der Technik gehalten werden. Das komplexe Zusammenwirken von Infrastruktur und sicherheitstechnischen Systemen ist wichtiger als der Einsatz einer Fülle von hochtechnologischen Anlagen.
2. Die zu evakuierenden Personen müssen im Ereignisfall rasch und präzise informiert und geführt werden.
3. Menschliches Versagen in Stresssituationen kommt immer wieder vor und muss durch konsequente Schulung und technische Unterstützung möglichst unterbunden werden.
4. Die Organisation der Einsatzkräfte muss optimal an die lokalen Verhältnisse, an die Infrastruktur aber vor allem an die im Ereignisfall vorgesehenen steuerungstechnischen Abläufe angepasst werden. Den Interventionskräften sind möglichst umfassende und aktuelle Informationen zur Verfügung zu stellen.

Steuerungssysteme der nächsten Generation müssen bei all diesen Aspekten einen entscheidenden Beitrag liefern können: Ereignisse rasch und zuverlässig erkennen, optimale Strategien identifizieren und implementieren, technische Systeme selbstständig steuern, die Verantwortlichen im Kontrollraum und die Einsatzkräfte umfassend unterstützen.

4. Feuer, Rauch und weitere Notfälle

Metrosysteme haben gesamthaft ein sehr hohes Sicherheitsniveau erreicht. Trotzdem sind Risiken immer noch vorhanden. Die Unfallwahrscheinlichkeit konnte zum Teil deutlich gesenkt werden, wie zum Beispiel im Fall der „klassischen" Bahn-Unfallszenarien Entgleisung und Kollision. Dabei spielen moderne Zugsicherungssysteme eine wichtige Rolle, welche eine wirksame und zuverlässige Kontrolle des Sicherheitsabstandes zwischen den Zügen garantieren und einen Frontalzusammenstoß praktisch unmöglich machen.

Der Brand, sowohl in Zügen als auch in Stationen, stellt nach wie vor die größte Gefährdung im Bahn- und Metrobereich dar. Die Erfahrungen zeigen, dass auch nach den neuesten Brandschutzrichtlinien gebaute Fahrzeuge und Strukturen, welche extrem schwer brennbar sind, unter ungünstigen Bedingungen durchaus entzündet werden können. Dieser Effekt wird durch ein großes Zündinitial begünstigt. Es ist bemerkenswert, dass „klassische" Brandursachen (elektrische Defekte, blockierte Bremsen usw.) an Bedeutung verlieren, weil sie grundsätzlich rascher detektiert und eliminiert werden. Absichtliche oder auf Unachtsamkeit zurückzuführende Brandstiftungen gewinnen hingegen an Bedeutung. Der Vollbrand eines Reise- oder Metrozuges kann verheerende Effekte haben: Die Brandleistung steigt meistens während den ersten 10 Minuten nach Brandbeginn verhältnismässig langsam an, kann aber in den nachfolgenden 10 Minuten bis auf rund 25 MW zunehmen. Die zugehörige Rauchmenge beträgt bis zu 70 m3/s und die Temperaturen erreichen um die 1'000°C. Die Rauchausbreitung ist häufig extrem rasch, bis 5–10 m/s, also wesentlich schneller als die typische Fluchtgeschwindigkeit von Personen im Tunnel oder auf Wegen im Bahnhof. Diese liegt je nach Sichtverhältnissen im Bereich von 1.0 bis 0.3 m/s.

Es ist wichtig, zwischen Ausnahmesituationen („exceptional situations") und echten Notfallsituationen („emergency situations") zu unterscheiden. Bei Ausnahmesituationen steht zwar die Sicherheit im Vordergrund, aber betriebliche Aspekte spielen noch eine wichtige Rolle. Typische Ausnahmesituationen im Metrobereich sind: Überfüllung von Zügen oder Stationen, wie sie z.B. während der Hauptverkehrszeit oder im Zuge von Großveranstaltungen vorkommen, Stillstand eines Fahrzeugs im Tunnel, Drohungen von Terrorakten in Zügen oder in Stationen. Steuerungssysteme müssen in solchen Situationen die Betriebsverantwortlichen unterstützen, damit diese mit der drastisch ansteigenden Belastung fertig werden. Dabei steht die Vorbeugung gegen ein Eskalieren der Situation im Vordergrund: Besteht Brandgefahr? Ist die Verkehrssicherheit garantiert? Können die Personenflüsse jederzeit sicher geführt werden?

Bei Notsituationen, wie z.B. Brand (im Zug, in einer Station oder in technischen Räumen), Zugentgleisungen oder akute Naturgefahren, muss alles getan werden, um die Sicherheit der Fahrgäste und des Personals zu gewährleisten. Die zeitlichen Abläufe spielen eine wesentliche Rolle und sehr schwierige Entscheidungen müssen sehr rasch und unter Stress getroffen werden. Typische, schwierige Fragen sind: Was passiert in diesem Tunnel oder im Zug? Welche Dienste müssen alarmiert werden (eigener technischer Dienst, Polizei, Feuerwehr usw.)? Welche Züge müssen umgeleitet werden? Welche Stationen müssen evakuiert werden und wie (durch die normalen Zugänge, durch die Züge, durch Notaus-

gänge usw.)? Wie sollen die technischen Systeme reagieren, um die gewählte Strategie optimal zu unterstützen (Steuerung des Lüftungssystems, Beleuchtung, Leitsystem usw.). Eine „intelligente" Steuerung unterstützt hier nicht nur bei der Umsetzung der gewählten Strategie, sondern vielmehr bei der Ermittlung und der Auswahl der optimalen Notfallstrategie.

5. Zunehmende Komplexität

U-Bahn Systeme sind im Vergleich zu anderen kritischen Infrastrukturen aus technologischer Sicht verhältnismäßig einfach. Sie weisen aber eine Fülle von elektromechanischen Ausstattungselementen auf, welche überwacht und gesteuert werden müssen. Die typische sicherheitstechnische Ausstattung eines modernen Metrosystems kann, trotz sehr großer individueller Unterschiede, folgendermaßen charakterisiert werden:

- Rollmaterial: Zugkontrollsystem, CCTV (Videoüberwachung), SOS-Anlagen, Notbremsen, Handfeuerlöscher, fest installierte Löschsysteme, Brandsensoren, Lüftung- und Klimaanlage, Funk, Lautsprecheranlage, Bildschirme des Fahrgastinformationssystems (Informationen und Mitteilungen), usw.
- Bahnhöfe und Haltestellen: Aufzüge, Fahrtreppen, Rauchschutzsysteme (Rauchschürzen, -vorhänge), Videoüberwachung, SOS-Anlagen, Notbremsen, Handfeuerlöscher, fest installierte Löschsysteme, Hydranten, Brandsensoren, Lüftungsanlagen und -komponenten, Lautsprecheranlagen, dynamische Fluchtleitsysteme, Anzeigen für Informationen und Mitteilungen, Funk, GSM usw.
- Tunnel: Zugleitsysteme und Zugsignalisierung, Feuerlöscher, Hydranten, Anemometer (Luftströmungsmessung), Lüftungsanlagen, Funk, GSM, dynamische oder feste Fluchtleitsysteme, SOS-Anlagen usw.

Hinzu kommt noch die allgemeine Infrastruktur zur Stromversorgung für den Betrieb des Gesamtsystems. Hierzu zählen z.B. die Mittelspannungsanlage (Leitungen, Transformatoren, Schutzeinrichtungen, Zähler usw.), Niederspannungsversorgung und – verteilung, unterbruchsfreie Stromversorgung, ev. Notfallgeneratoren und Beleuchtung. Weiter werden sehr viele Sensoren verwendet, um die Überwachung z.B. von technischen Anlagen oder von Sicherheitskomponenten (Betätigung von Fluchttüren, Entnahme von Feuerlöscher, usw.) zu ermöglichen.

Moderne SCADA-Systeme (SCADA: „Supervisory Control and Data Acquisition") erfassen die Signale aller Anlagen und sind in der Lage, sämtliche Ausrüstungskomponenten (z.B. Fahrtreppen, Aufzüge, Beleuchtung, Anzeigetafeln für Informationen und Mitteilungen) zu steuern. Die Anzahl Datenpunkte wird aber schon bei verhältnismäßig einfachen Metrosystemen rasch recht groß.

Die Anforderungen sind bei normalen Betriebsbedingungen oder bei verhältnismäßig leichten Störungen mit herkömmlichen Steuerungssystemen relativ einfach zu bewältigen. Im Ereignisfall ist das Personal in der Leitstelle aber schnell durch eine enorme Flut von teils widersprüchlichen Signalen aus unterschiedlichen Sensoren überlastet. Die Anforderungen an das Überwachungspersonal steigen dabei durch zunehmende Integration von Überwachungselementen (z.B. Videokameras) und durch den Trend hin zu automatisierten Systemen noch weiter an. Letztere benötigen auf Grund von fehlendem Personal zusätzliche Sicherheitssysteme und Sensoren.

6. Anforderungen

Steuerungssysteme der nächsten Generation für den Einsatz in kritischen Infrastrukturen erfordern Entwicklungen in verschiedenen Bereichen. Die Schlüsselfunktionen, welche den angestrebten Fortschritt garantieren werden, sind:

1. Fähigkeit, mit unterschiedlichen Betriebsbedingungen und Betriebszuständen umzugehen.

Die Anforderungen und Prioritäten im Normalbetrieb, im gestörten Betrieb (ein Teil der technischen Systeme ist aufgrund von technischen Defekten oder Unterhaltsarbeiten nicht verfügbar oder die aktuellen Bedingungen könnten zu potentiell gefährlichen Situationen führen) und im Ereignis- bzw. Notfallbetrieb (unmittelbare Gefährdung von Personen und Infrastruktur durch ein Ereignis) sind sehr unterschiedlich. Die Differenzen wirken sich praktisch auf allen Stufen, von der Behandlungsweise der technischen Signale bis hin zur administrativen Zuständigkeit und Verantwortlichkeit aus. Die Betriebsbedingungen können zeitlich und örtlich sehr variabel sein.

2. Fähigkeit, mit komplexen Ereignissen umzugehen.

Ein typisches extrem wichtiges Beispiel eines komplexen Ereignisses ist die Branddetektion. Diese erfolgt durch ein Fülle von direkten (thermische Brandmelder, Rauchmelder usw.) oder indirekten Brandsignalen (Öffnen einer Fluchttür, Entnahme eines Feuerlöschers aus seiner Halterung, usw.) und weitere, mehr oder weniger zuverlässige Informationen (Anrufe über das metroeigene SOS-Telefonnetz, Funkmeldungen des Personals, Mobiltelefonanrufe usw.). Die Informationsfülle ist extrem heterogen, unterschiedlich genau und zuverlässig, sowie in der Regel zu einem gewissen Grad widersprüchlich. Eine zuverlässige Branddetektion verwendet alle verfügbaren Informationen automatisch, erkennt die verfügbaren Charakteristika des spezifischen Ereignisses und startet die bestmögliche Reaktion.

3. Fähigkeit, einfache Daten zu analysieren und zu komplexen Informationen zu verknüpfen.

Eine Krisensituation generiert eine enorme Anzahl von unsicheren und zum Teil widersprüchlichen Signalen und Informationen. Sie sind für den Menschen nicht mehr überschaubar. Aber wichtige Entscheidungen, z.B. im Bezug auf die Führung der Intervention, hängen sehr stark von der Gesamtsituation ab. Unterschiedliche Typen von Informationen sind für die verschiedenen Akteure von Bedeutung. Die Informationen (Rauchausbreitung, Position der Züge, Position der Reisenden und eventuell des Personals, Zustand der technischen Anlagen, usw.) müssen genau und zuverlässig in benutzergerechten Ansichten zusammengefasst werden. Das im übergeordneten Management-Niveau für betriebliche Abläufe hinterlegte Datenmodell konstruiert aufgrund aller verfügbaren Informationen eine umfassende Gesamtbeschreibung des Zustan-

des des Systems oder Teilsystems. Diese wird jedem Akteur in anwendergerechten Spezialansichten zur Verfügung gestellt.

4. Fähigkeit, komplexe Handlungen durchzuführen.

Beispiele von komplexen Handlungen sind z.B. die Evakuierung einer Station, die Steuerung von komplexen Systemen oder die großräumige Umfahrung des Ereignisortes. Im verhältnismässig einfachen Fall der Evakuierung geht es z.B. darum, die richtigen Nachrichten durch die Lautsprecheranlagen in den Zügen und in den Stationen auszugeben, mit den vorhandenen Anzeigetafeln die Sprachnachrichten optimal zu ergänzen, Fluchtleiteinrichtungen korrekt zu schalten, Fahrtreppen in Fluchtrichtung zu bewegen usw. Falls einzelne Handlungen nicht erfolgreich sind, müssen eventuell kompensatorische Maßnahmen ergriffen werden. All diese Aktivitäten sind, alleine genommen, einfach und problemlos. Aber sie stellen eine unnötige Belastung für die Verantwortlichen in der Leitzentrale dar, deren Aufmerksamkeit von wichtigeren Aufgaben beansprucht wird. Die unvermeidliche Konsequenz davon sind Zeitverzögerungen und Fehler bei Entscheidungen.

5. "Intelligente" Entscheidungen und Entscheidungsunterstützung durch Simulation.

Die Kernaufgabe und die größte technologische Herausforderung der neuen Generation von Management- und Steuerungssystemen bestehen zweifellos darin, für jede Situation in kürzester Zeit die optimale Handlungsstrategie zu ermitteln. Es geht nicht nur darum, die zu erwartende Entwicklung des Systemzustandes zu ermitteln, um z.B. den optimalen Fluchtweg zu bestimmen. Die Steuerung muss vielmehr in der Lage sein, bei einem Ereignis diese Entwicklung über die Zeit möglichst günstig zu beeinflussen. Viele Einzelelemente sind voneinander abhängig: Jede Evakuierungsstrategie erfordert z.B. eine angemessene Lüftung. Gleichzeitig ist die Interventionsstrategie stark von der Evakuierungsstrategie abhängig. Die Zielsetzung besteht deswegen darin, basierend auf die vorhandenen Daten, welche Anfangs- und Randbedingungen des dynamischen Systems darstellen, verschiedene mögliche Szenarien zu simulieren, um die optimale Reaktion zu ermitteln. Die Anforderungen an die Simulationstechnologien, vor allem im Bezug auf Rauchausbreitung, Zugbewegung und Personenbewegung, sind daher relativ hoch.

6. Umfassende Simulationsfähigkeiten zu Schulungs- und Trainingszwecken.

Die Bedienung der Steuerung eines komplexen Systems kann nicht nur theoretisch erlernt werden. Wie auch für andere technische Systeme notwendig, brauchen wir umfassende Simulatoren, welche das Systemverhalten möglichst realitätsnah reproduzieren können. Solche Simulatoren verwenden grundsätzlich die „echte" Benutzeroberfläche der Steuerung der kritischen Infrastrukturanlage, aber die Systemantwort wird durch auf angemessene Modelle basierende dynamische Simulation nachgebildet. Solche Systeme werden extrem realitätsnah auf Vorgaben und Befehle reagieren und das Bedienpersonal wird aufgrund von reellen Szenarien optimal auf den Ernstfall vorbereitet.

7. Fortschrittliche graphische Benutzeroberfläche.

Die Anforderungen in diesem Bereich sind hoch, weil die Menge der Informationen, welche dem Steuerungssystem zur Verfügung stehen, bei einem Ereignis drastisch ansteigt. Wichtig ist deshalb die Fokussierung auf die Darstellung der wichtigen Aufgaben und damit auch das Zurverfügungstellen der notwendigen Software-Werkzeuge.

7. IT-Infrastruktur: SCADA und CEP, physische und semantische Modelle

7.1 SCADA

Komplexe Infrastrukturanlagen werden von SCADA-Systemen gesteuert. Diese werden für die gesamte Überwachung und Steuerung von großen, oft komplexen Anlagen wie z.B. einer U-Bahn-Station (etwa Brand- und Rauchmelder, Belüftungsanlagen, Fahrttreppen und Aufzüge) eingesetzt. SCADA-Systeme sind immer häufiger verteilte Systeme: Teilsysteme, die miteinander kommunizieren, sind für die Überwachung und Steuerung eines Teils der Anlage zuständig. In einer U-Bahn-Station kann ein Teilsystem Fahrttreppen oder Aufzüge steuern, ein anderes die Brand- und Rauchmelder überwachen. Die Steuerung erfolgt meist halbautomatisch, das heißt, dem Operator wird durch eine Mensch-Maschine-Schnittstelle das Eingreifen in die Anlagensteuerung ermöglicht.

SCADA-Systeme sind in zwei Schichten aufgeteilt: Eine niedere oder erste Schicht ist für die Datenerfassung aus Systemkomponenten (etwa Messanlagen, einzelne oder mehrere Sensoren, einzelne oder mehrere Geräte) zuständig. Fernbedienungsterminals (englisch: "Remote Terminal Unit" oder "RTU"), die mit Sensoren, Motoren, oder Geräten verbunden sind, liefern Messdaten. Die RTUs werden mittels speicherprogrammierbaren Steuerungen (SPS oder englisch: "Programmable Logic Controller" oder "PLC") realisiert, die programmierbar und folglich anpassbar sind. Eine höhere oder zweite Schicht, oft eine zentrale Komponente, ist für die Analyse der von der ersten Schicht gelieferten Messdaten zuständig. Die Kommunikation der RTUs untereinander und mit der höheren Schicht erfolgt heute immer häufiger auf der Basis von Internet-Techniken, insbesondere auf dem Datenübertragungsprotokoll TCP, dem Internet-Protokoll IP und XML-Anwendungen. Die Verwendung der verbreiteten, generischen Internet-Protokollen und -Datenformaten erleichtert die Konzeption, Portierung und Aktualisierung der SCADA-Systeme. Ein weiterer Trend ist die Entwicklung von nicht proprietären Datenformaten wie FCML (Facility Control Markup Language) [2].

7.2 CEP

Ereignisgesteuerte Informationssysteme benötigen eine systematische und automatische Verarbeitung von Ereignissen. "Complex Event Processing" oder "CEP" bezeichnet Methoden und Techniken zur Verarbeitung von Ereignissen während sie passieren, also kontinuierlich und zeitnah. CEP leitet aus Ereignissen ein höheres, wertvolles Wissen in Form von sogenannten komplexen Ereignissen ab, d.h. Situationen, die sich nur als Kombination von mehreren Ereignissen erkennen lassen. Ein Anwendungsgebiet für CEP sind die SCADA-Systeme.

Um Mess- und andere Fehler zu minimieren, sollten Daten von mehreren RTUs kombiniert werden. Ferner muss oft aus einfachen numerischen Messungen (z.B. Temperatur, Rauch) eine höhere symbolische Situation (z.B. Brand) erschlossen werden. CEP fügt die von RTUs gelieferten einzelnen Ereignisse zusammen und erkennt daraus komplexe Zusammenhänge, so genannte komplexe Ereignisse.

Der Begriff "Complex Event Processing" wurde in [3] geprägt. CEP hat in der Informatik-Forschung aber auch viele voneinander unabhängige Ursprünge, über aktive Datenbanken und Netzwerkmanagement bis hin zu sogenanntem „temporalem Schließen", das heißt, Formalismen zur Wissensrepräsentation, die Berechnung von Schlussfolgerungen aus zeitabhängigen Daten ermöglichen, im Bereich der künstlichen Intelligenz. Erst in den letzten Jahren tritt CEP als eigenständiger Bereich sowie als wichtiger Trend in der Industrie auf.

Bei CEP ist zu unterscheiden, ob komplexe Ereignisse als à priori bekannte Muster über Abfolgen von Einzelereignissen spezifiziert werden oder bisher unbekannte Muster in den Abfolgen als komplexe Ereignisse erkannt werden sollen. Beim ersten Fall bieten spezielle Ereignisanfragesprachen eine komfortable Möglichkeit, komplexe Ereignisse zu bestimmen und effizient zu erkennen. Beim zweiten Fall werden bei Ereignissen maschinelles Lernen und "Data Mining" angewendet. Für die Branderkennung in Gebäudekomplexen (wie z.B. U-Bahn-Stationen und Flughafengebäuden) werden zurzeit vor allem bekannte Datenmuster verwendet: Aus einer Vielfalt einzelner Ereignisse sollen gefährliche Situationen erkannt werden, deren Merkmale / Messdatenabläufe im Voraus bekannt sind. Die systematische Analyse von Messdaten unter bestimmten Bedingungen (etwa normaler Betrieb, hohe Fahrgastaufkommen, und Notfälle) bietet sich auch an. Sowohl die Anwendung der Erkennung bekannter Muster wie auch die Suche nach noch unbekannten Mustern ist also bei der Branderkennung in U-Bahn-Anlagen möglich und sinnvoll. CEP stellt also eine wirksame Ergänzung zur SCADA-Technologie dar.

Nicht nur komplexe Ereignisse sollen erkannt werden, sondern auch komplexe Aktionen oder Abläufe wie etwa eine Evakuierung sollen von CEP-Systemen spezifiziert und gesteuert werden. Unter einer komplexen Aktion versteht man eine Reihe von einfachen Aktionen, die zusammen zu einem Ziel führen. Bei der Evakuierung der untersten Ebene einer 3-stöckigen U-Bahn-Station werden eine Reihe von einfacheren Aktionen ablaufen, z.B.:

- Die unterste Ebene wird über mehrere Fluchtwege evakuiert.
- Die Bedingungen für eine solche Evakuierung werden geschaffen (z.B. die Fahrtrichtung der Fahrtreppen wechseln und die Belüftung anpassen).
- Die Fluchtwege in den zu evakuierenden Ebenen werden frei gehalten.

Komplexe Aktionen verlangen nach Vorhersagen zum Ablauf und benötigen möglicherweise Anpassungen während ihrer Durchführung. Die Spezifikation der komplexen Aktionen ist daher genauso anspruchsvoll wie die Erkennung von (im Voraus bekannten oder unbekannten) komplexen Ereignissen.

7.3 Physikalische Modelle

Zwecks Spezifikation komplexer Ereignisse, die erkannt werden sollen, und Aktionen, die unter bestimmten Bedingungen durchzuführen sind, werden physikalische Modelle benötigt. Diese Modelle werden unter anderem für die Verifizierung der Messdaten benutzt. Ein Modell der Feuer- und Rauchausbreitung ermöglicht zum Beispiel:

- Erkennung und Filterung von gesendeten „Datenausreißern" der Sensoren oder Geräte,
- Ermittlung eines Gesamtbildes aus verschiedenen Messdaten (etwa zu unterscheiden, ob es sich um eine kleinen lokalen oder großen ausgedehnten Brand handelt),
- Berechnung von Vorhersagen (zum Beispiel wie viel Rauch wird es in den nächsten 5 Minuten in einem bestimmten Durchgang geben)?

Physikalische Modelle der Rauchausbreitung sind Anwendungen der Fluiddynamik (englisch: "Computational Fluid Dynamics" oder "CFD" [4]). Die Herausforderung liegt nun darin, durch gezielte Vereinfachungen, schnelle Berechnungen für den Echtzeiteinsatz zu ermöglichen und dabei ausreichend präzise Werte zu liefern. Bezüglich der Evakuierung sind sogenannte Räumungsmodelle (englisch: „egress models") nötig, welche die Räumungszeit bis zum Erreichen des sicheren Bereichs durch die flüchtenden Personengruppen einschätzen. Auch hierbei liegt die Herausforderung darin, die geeigneten Vereinfachungen zu finden, die einen Echtzeiteinsatz ermöglichen.

7.4 Semantische Modelle

Die physikalischen Modelle stellen keine günstige Modellierungsebene dar, um komplexe Handlungen wie z.B. die Einleitung und Steuerung der Evakuierung zu spezifizieren. Ausgehend von den Werten des physikalischen Modells (z.B. Vorhersage über die Entwicklung der Brandleistung), müssen semantische Größen abgeleitet werden, die zum Beispiel darüber Auskunft geben, ob eine Treppe während der nächsten 5 Minuten rauchfrei bleiben wird. Das Ziel von semantischen Modellen ist es, solche semantischen Größen einerseits für die Ermittlung der Brand- und Rauchausbreitung und andererseits für die Evakuierungsplanung zu liefern. Semantische Modelle ermöglichen neben der Spezifizierung der möglichen komplexen Aktionen unter Berücksichtigung der dafür nötigen Konzepte auch die Anpassung oder sogar den Wechsel des physikalischen Modells. Die semantischen Modelle spielen also die Rolle einer konzeptuellen Schnittstelle zu den physikalischen Modellen.

Diese Schnittstelle erleichtert die Übertragung des Systems auf eine andere U-Bahn-Station. Während die physikalischen Modelle sehr von den spezifischen Gegebenheiten einer U-Bahn-Station abhängen, sind die semantischen Modelle dank ihrer höheren Abstraktion weniger von spezifischen Gegebenheiten betroffen und folglich einfacher auf eine andere Station übertragbar.

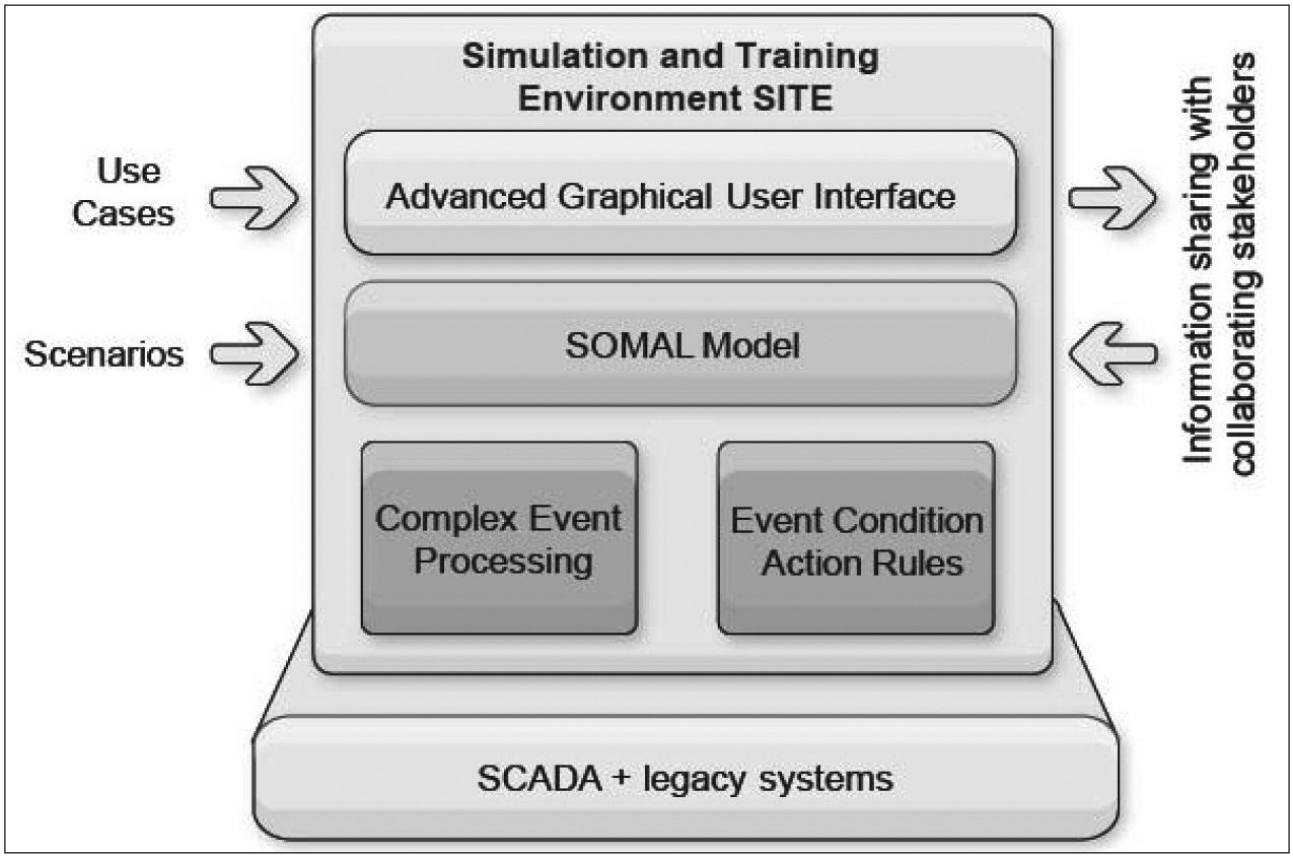


Abbildung 1: Mögliche künftige Struktur der Steuerung einer kritischen Infrastruktur (Quelle: EMILI).

Für jede U-Bahn-Station sind jedoch spezifische physikalische und semantische Modelle nötig, weil die Brand- und Rauchausbreitung sowie die Fluchtbedingungen je nach Infrastruktur stark variieren können.

8. Das Projekt EMILI, "Emergency Management In Large Infrastructures"

Das Projekt EMILI ("Emergency Management in Large Infrastructures") ist ein "capability project" im 7. Rahmenprogramm der EU ("FP7") zielt darauf ab, eine neue Generation von Datenmanagement und -überwachungssystem inklusive angepasster Simulations- und Trainingsfähigkeiten zu entwickeln. Solche neuartigen Systeme verbessern die betriebliche Sicherheit und das Notfall-Management in grossen kritischen Infrastrukturanlagen wie Flughafengebäuden, Stromverteilnetzen, U-Bahn- und Eisenbahnsystemen, Telekommunikationsanlagen, u.a. Abbildung 1 stellt eine mögliche Struktur der Steuerung einer kritischen Infrastruktur dar.

Das Notfall-Management bei großen Infrastrukturanlagen ist hinsichtlich der optimalen Zusammenarbeit der verschiedenen Akteure besonders kritisch, da diese zum einen Informationen austauschen sowie ihre Planungen und Aktivitäten koordinieren müssen und zum anderen auch auf sich verändernde Gegebenheiten im Verlauf des Ereignisses adäquat reagieren müssen. Zudem können die Anzahl und die Art der Akteure in Abhängigkeit von der spezifischen Situation variieren.

Das Datenmanagement, die Kommunikation und die Entscheidungsunterstützung müssen jeweils an die konkrete Situation in der zu betreibenden und zu überwachenden Infrastrukturanlage angepasst werden. Deshalb wird die technologische Entwicklung auch innerhalb des EMILI-Projekts auf der Basis von drei Fallbeispielen vorangetrieben:

- Anwendungsfall I: Überwachung und Kontrolle in Flughafen-Gebäuden
- Anwendungsfall II: Überwachung und Kontrolle von Infrastrukturanlagen des öffentlichen Personennahverkehrs (U-Bahn-System)
- Anwendungsfall III: Überwachung und Kontrolle moderner Energieversorgungsnetzwerke mit Abhängigkeiten von anderen kritischen Infrastrukturanlagen

Die Partner im EMILI Projekt sind:

- Fraunhofer IAIS, Institut für Intelligente Analyse und Informationssysteme, St. Augustin (D) – Koordinator; Fachkompetenz im Bereich Sicherheit und Betriebsschutz, militärische Simulationsanwendungen, Forschung hinsichtlich kritischer Infrastrukturen, deren Management sowie Simulation.

- SKYTEC AG, Oberhaching (D) - Fachkompetenz im Bereich hochentwickelter Komponenten von Datenmanagement- und Kontrollsystemen, insbesondere SCADA
- ASIT AG, Bern (CH) - Fachkompetenz im Bereich Risikoanalysen und Entwicklung von Sicherheits- und Einsatzkonzepten für den sicheren Betrieb von öffentlichen Infrastrukturanlagen
- Stichting Centrum voor Wiskunde en Informatica CWI, Amsterdam (NL) - Fachkompetenz in der Entwicklung von Daten-Managementsystemen sowie in der experimentellen Forschung
- Aplicaciones en Informática Avanzada AIA, Barcelona (E) - Fachkompetenz im Bereich Intelligenter Überwachungssysteme für Stromversorgungsnetzwerke
- Ludwig-Maximilians-Universität München, Institut für Informatik, Lehr- und Forschungseinheit für Programmier- und Modellierungssprachen, München (D) - Fachkompetenz im Bereich Modellierung, Semantic Web technologies und Complex Event Processing
- Institute Mihailo Pupin PUPIN, Belgrad (RS) - Fachkompetenz im Bereich hochentwickelter Komponenten von Datenmanagement- und Kontrollsystemen

Das Projekt EMILI hat am 1. Januar 2010 begonnen und läuft über total 36 Monate bis 31. Dezember 2012 (http://www.emili-project.eu).

Literatur und Quellen

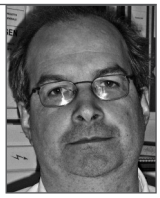
[1] Emergency Management In Large Infrastructures (EMILI), http://emili-project.eu

[2] François Bry, Bernhard Lorenz, Hans Jürgen Ohlbach, Martin Roeder, Marc Weinberger: The Facility Control Markup Language FCML. Proceedings of the Second International Conference on the Digital Society (ICDS 2008), IEEE Computer Society, pp. 177–122, 2008)

[3] D. C. Luckham. The Power of Events: An Introduction to Complex Event Processing in Distributed Enterprise Systems. Addison-Wesley, 2002

[4] M. Bettelini. CFD for Tunnel Safety". FLUENT User's Meeting, Bingen, 17-18.9.2001

Autoren



Dr. Marco Bettelini
Amberg Engineering AG
Fachbereichsleiter
Trockenloostraße 21
Postfach 27
CH-8105 Regensdorf-Watt (Schweiz)
Tel: +41 (0)79 404 14 45
Fax: +41 (0)44 870 06 20
E-Mail: mbettelini@amberg.ch
Internet: www.amberg.ch

Dr. Nikolaus Seifert
ASIT AG
Geschäftsführer
Bitziusstraße 40
CH-3006 Bern
Tel: +41 (0)79 229 02 80
Fax: +41 (0)31 359 24 84,
E-Mail: nikolaus.seifert@asit.ch
Internet: www.asit.ch

Prof. Dr. François Bry
Institut für Informatik
Ludwig-Maximilians-Universität München
Oettingenstr. 67
80538 München
Tel: 089/2180-9310
Fax: 089/2180-9311
E-Mail: bry@lmu.de
Internet: www.lmu.de

Innovative Safety System for Metro Stations

Large critical infrastructures in different sectors of our society are increasingly susceptible to disturbances in case of emergency or attack. But the increasing automation and availability of net technologies create new opportunities. The basic principles, which will allow for faster and more reliable next generation's control systems, are currently developed within the EU-research project EMILI.