

# Mensch-Maschine-Systeme im resilienten Krisenmanagement

Tilo Mentler, Michael Herczeg

Institut für Multimediale und Interaktive Systeme, Universität zu Lübeck

## **Zusammenfassung**

Bei der Bewältigung von Krisen und Katastrophen werden zunehmend computerbasierte Werkzeuge eingesetzt. Sie werden dabei Teil komplexer, mit der Gefahrenabwehr und Daseinsvorsorge beauftragter soziotechnischer Gesamtsysteme. Ihre Sicherheit und Zuverlässigkeit zu erhöhen, Funktionsstörungen oder Leistungsdegradationen unter möglichst vielen Umständen zu verhindern und sie flexibel unter neuen Randbedingungen nutzbar zu halten oder zu machen, muss ein zentrales Ziel der Entwicklung sein. Idee des Resilience-Engineering ist, sicherheitskritische Systeme auf allen Ebenen robuster, adaptiver und flexibler zu gestalten, insbesondere indem der Faktor Sicherheit nicht mehr nur aus dem konventionellen Blickwinkel des Risikomanagements betrachtet wird. In diesem Beitrag werden zunächst die Prinzipien des Resilience-Engineering vorgestellt. Sie werden anschließend auf die Gestaltung von Mensch-Maschine-Systemen im Krisenmanagement übertragen.

## 1 Einleitung

Die Abwehr von Gefahren, die Daseinsvorsorge und die Gewährleistung innerer Sicherheit, insbesondere in Ausnahmesituationen bei Großschadenslagen, Katastrophen und Krisen, stellen vielseitige und dynamische Herausforderungen für die zuständigen Behörden und Organisationen mit Sicherheitsaufgaben (BOS) dar. Um ihnen begegnen zu können, müssen die technischen und sozialen Teilsysteme dieser komplexen soziotechnischen Systeme möglichst gut zusammenwirken (Ulich 2001; Vicente 1999). Zunehmend werden in diesen zeit- und sicherheitskritischen Kontexten computerbasierte Werkzeuge eingesetzt. Dabei können folgende grundlegenden Nutzungsszenarien unterschieden werden:

1. innerhalb einer Behörde bzw. Organisation, z. B. zur Koordination der eigenen Arbeiten (Mentler & Herczeg 2013);
2. organisationsübergreifend zum Austausch von Daten und Information, z. B. in Form gemeinsamer Lagebilder (z. B. Reuter & Ritzkatis 2013);
3. zwischen den Behörden bzw. Organisationen und der Öffentlichkeit, z. B. über soziale Netzwerke (z. B. Beneito-Montagut et al. 2013).

Mit der wachsenden Verbreitung interaktiver und vernetzter Anwendungssysteme auf all diesen Ebenen steigt ihre Bedeutung für die Effektivität und Effizienz des Einsatzverlaufes. Funktionsstörungen bzw. Leistungsminderungen müssen möglichst auch bei stärkeren Abweichungen von vordefinierten Betriebsbedingungen vermieden werden, auch wenn diese gerade bei außergewöhnlichen Ereignissen kaum vorhersehbar sind und sich dynamisch verändern können (siehe z. B. Kendra & Wachtendorf 2003). Nachfolgend werden unter Bezugnahme auf Resilience-Engineering Prinzipien und Methoden zur Gestaltung robuster, adaptiver und flexibler Systeme vorgestellt und auf die Gestaltung von Mensch-Maschine-Systemen für das Krisenmanagement angewendet.

## 2 Resilience Engineering

Nicht nur in Disziplinen wie der Pädagogik (Zander 2011), Physik (Campbell 2008) oder Ökologie (Holling 1973), sondern auch im Zusammenhang mit sicherheitskritischen Systemen wird vermehrt von *Resilienz* gesprochen. Hollnagel et al. (2013) beschreiben das für diesen Kontext Wesentliche des Begriffes als „*intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions*“.

Resilience-Engineering steht dabei zunächst einmal für eine veränderte Denkweise über Sicherheit. Sie wird hier als Fähigkeit eines Systems aufgefasst, unter veränderlichen Bedingungen zu funktionieren und kann somit im Sinne der Widerstands- bzw. Anpassungsfähigkeit verbessert werden (Resilience Engineering Association 2014). Andere Ansätze beruhen vorrangig auf Ereignisanalysen und probabilistischen Risikobewertungen. Sie zielen somit auf die Beseitigung von Schwächen ab (Hollnagel, Woods & Levenson 2006). Im Resilience-Engineering wird i.allg. von folgenden Voraussetzungen und Grundsätzen ausgegangen (Leonhardt et al. 2009):

1. Einsatzbedingungen lassen sich nicht vollständig im Voraus spezifizieren. Anpassungen an aktuelle Umstände erfolgen unter Zeitdruck und können daher nur Annäherungen an optimale Lösungen sein.
2. Unerwünschte Ereignisse können als unerwartete Kombination von Leistungsschwankungen verstanden werden und lassen sich nicht immer einem Element zuordnen.
3. Effektives Sicherheitsmanagement muss sowohl proaktiv als auch reaktiv sein.
4. Sicherheit und Produktivität lassen sich nicht isoliert voneinander betrachten. Sicherheit muss durch Verbesserungen, nicht durch Beschränkungen erzielt werden.

Resiliente Organisationen bzw. Systeme müssen daher auf all ihren Ebenen in der Lage sein

- aus früheren positiven wie negativen Ereignissen zu lernen,
- auf aktuelle Zustände flexibel zu reagieren,
- kurzfristige, kritische Entwicklungen bzw. Elemente zu überwachen,
- langfristige Bedrohungen und Möglichkeiten zu antizipieren.

Es ist prüfen, wie Mensch-Maschine-Systeme hinsichtlich ihrer Benutzungsschnittstelle und Funktionalität sowie der Arbeitsteilung zwischen Mensch und Maschine zu gestalten sind, um Individuen und Organisationen bei der Bewältigung dieser komplexen Aufgaben zu unterstützen.

### 3 Gestaltungsgrundsätze

Nachfolgend werden grundsätzliche Anforderungen an die Funktionalität und Gestaltung interaktiver Systeme zur Nutzung im Krisenmanagement beschrieben. Dabei wird zwischen den einleitend beschriebenen Nutzungsszenarien unterschieden.

#### 3.1 Lernen aus Ereignissen

Um sowohl aus erfolgreich bewältigten Krisen als auch aus problematischen Einsätzen Rückschlüsse für die Verbesserung von Strukturen und Abläufen innerhalb einzelner BOS ziehen zu können, sollten computerbasierte Werkzeuge einerseits die Nachvollziehbarkeit von Entscheidungen erleichtern und andererseits unproblematische Rückmeldungen der Einsatzkräfte ermöglichen (z. B. hinsichtlich der Gebrauchstauglichkeit oder durch Gewährleistung von Anonymität).

Relevante Daten (z. B. Mitteilungen, Statusmeldungen, Protokolle, Fotos) müssen dabei automatisch gesichert und semantisch verknüpft werden (z. B. Zeitstempel, Positionsdaten, Chronologie). Dies betrifft nicht nur die intern anfallende Daten, sondern auch die aus sozialen Netzwerken, bei denen nicht davon ausgegangen werden darf, dass Daten auch noch zu einem späteren Zeitpunkt auf Bedarf abrufbar sein werden.

Berichtssysteme über kritische Ereignisse (Critical Incident Reporting Systems, CIRS) sind bereits in vielen Anwendungsdomänen (z. B. Flugwesen, Gesundheitswesen) etabliert und sollten auch im Bereich der BOS flächendeckend eingeführt werden. Der Zugriff sollte bedarfsweise auch anderen an entsprechenden Einsätzen beteiligten Einrichtungen zur Verfügung stellen. Organisationsübergreifendes Lernen sollte weiterhin durch die Konsolidierung von Datenmodellen verschiedener Mensch-Maschine-Systeme und durch die Standardisierung von Reporting-Mechanismen unterstützt werden.

Zwischen den BOS und der Öffentlichkeit darf der Austausch nicht nur auf den Zeitraum der Krise bzw. Katastrophe beschränkt bleiben, sondern muss auch und gerade im Anschluss aktiv über soziale Netzwerke betrieben werden. Rückmeldungen von Zeugen oder Betroffenen sind zu motivieren, einzuholen und zu bewerten. Hierzu müssen geeignete Kanäle und Methoden zur Verfügung gestellt und bekannt gemacht werden (z. B. definierte Gruppen innerhalb von sozialen Netzwerken, etablierte Kennzeichnungsmöglichkeiten für ereignisbezogene Nachrichten).

## 3.2 Reagieren auf aktuelle Zustände

Um auf ein aktuelles Ereignis effizient reagieren zu können, müssen die Einsatzkräfte wissen bzw. schnellstmöglich ermitteln, was zu tun ist und in der Lage sein, die jeweiligen Schritte umzusetzen. Im Zusammenhang mit Mensch-Maschine-Systemen stellt sich hierbei insbesondere die Frage nach dem Übergang zwischen Routine- und Ausnahmebetrieb. Können die im Alltag genutzten Anwendungen und ihre Bedienkonzepte, ggf. in anderem Modus, beibehalten werden oder ist ein Wechsel auf speziell für Ausnahmefälle entwickelte Systeme notwendig? Gebrauchstaugliche und flexible Benutzungsschnittstellen sollten eine durchgängige Benutzung (z. B. durch eine konsistente Gestaltung) und die Skalierung von Funktionalität (z. B. durch geeignete Funktionsteilung Mensch-Maschine) ermöglichen, ohne die stark geforderten Benutzer in Lern- und Eingewöhnungsphasen zusätzlich zu belasten.

Der Wechsel zum Routine- zum Ausnahmebetrieb ist auch in organisationsübergreifender Nutzung interaktiver Systeme von entscheidender Bedeutung für den Einsatzverlauf. Wichtig ist dabei die Kennzeichnung interner und externer Daten mit ihren jeweiligen Verfassern. Entscheidungsunterstützungssysteme (Decision Support Systems) können Führungskräfte bei der Bewertung von Situationen unterstützen und ggf. auch widersprüchliche Zielsetzungen verschiedener BOS bewerten, z. B. in Modellrechnungen.

Zwischen den BOS und der Öffentlichkeit sollten die bereits vor einem konkreten außergewöhnlichen Ereignis explizite Kommunikationskanäle in sozialen Netzwerken bestehen, so dass das Melden von Ereignissen und Entwicklungen durch die Öffentlichkeit zeitnah erfolgen kann und sich nicht ausschließlich spontan gestaltet. Die Bewertung der Meldungen und Maßnahmen durch die Einsatzkräfte muss unter der Maßgabe erfolgen, dass freiwillige Helfer und Betroffene in bester Absicht handeln, aber keine Domänenexperten sind. Sie verwenden beispielsweise umgangssprachliches Vokabular oder informieren über für sie relevante, aber für die Einsatzbewältigung nachrangige Vorfälle (siehe z. B. Merrick & Duffy 2013). Es muss auch mit absichtlichen Fehlinformationen gerechnet werden. Darüber hinaus dürfen die ggf. zahlreichen Mitteilungen aus den sozialen Netzwerken nicht zu einer falschen Lagebeurteilung führen, da z. B. durch gestörte Informations- und Kommunikationsinfrastrukturen der Zugang nur für einen Teil der Betroffenen möglich sein könnte. Dies ist bei der Darstellung von Informationen zu beachten.

## 3.3 Überwachen kritischer Elemente

Um in Katastrophen und Krisen potentielle Gefahrenquellen und Fehlentwicklungen überwachen zu können, ist aufgrund der Dynamik und räumlichen Verteilung der Ereignisse die direkte Wahrnehmung und Bewertung durch einzelne Einsatzkräfte kaum möglich bzw. ausreichend. Mensch-Maschine-Systeme müssen Daten aus verschiedenen Quelle einholen, aggregieren, aufbereiten und verschiedene Visualisierungsmöglichkeiten bieten, um den Benutzern im Sinne der Prozessführung das Erkennen von Trends, Schwerpunkten oder Sprüngen in Einsatzverläufen zu erleichtern. Die unzureichende Beurteilung durch einzelne Einsatzkräfte gilt im übertragenden Sinne auch für einzelne BOS. Vernetzte Systemlösungen müssen den Zugriff auf relevante Daten anderer Einrichtungen ermöglichen.

Zwischen BOS und Öffentlichkeit besteht hinsichtlich dieses Aspektes ein Spannungsverhältnis. Es betrifft einerseits das Auftreten meldepflichtiger Ereignisse und ihrer Kommunikation in der Öffentlichkeit. Gerade durch die Multiplikator-Funktion sozialer Netzwerke können sich Nachrichten sehr schnell verbreiten. Bestenfalls werden so viele potentiell Betroffene frühzeitig vorgewarnt, schlimmstenfalls Panik und Chaos ausgelöst. Andererseits gilt, dass eine für einzelne Personen oder Gruppen von Betroffenen kritische Situation nicht zwangsläufig kritisch für die zuständigen Einrichtungen sind. So wäre beispielsweise ein umgestürzter Baum auf einer Anliegerstraße für die Bewohner ein großes Hindernis, würde aber eine deutlich niedrigere Priorität als das Räumen von Fernverkehrs- und Hauptstraßen haben.

### 3.4 Antizipieren von Bedrohungen und Möglichkeiten

Um sich langfristig auf Katastrophen und Krisen vorbereiten zu können, müssen zukünftige Einsatzszenarien und Handlungsmöglichkeiten geplant und evaluiert werden. Hierzu müssen innerhalb von und zwischen BOS interaktive Plattformen zur Simulation auf Basis vergangener Einsätze betrieben werden. Solche Analyse- und Trainingssysteme sollen dabei nicht nur das domänenbezogene Handeln, sondern auch die effiziente Nutzung der computerbasierten Werkzeuge adressieren.

Zur Modellierung komplexer soziotechnischer Systeme wie der BOS wird im Rahmen des Resilience-Engineering die *Functional Resonance Analysis Method (FRAM)* empfohlen (Hollnagel 2012). Sie lässt sich sowohl zur retrospektiven als auch zur prospektiven Analyse einsetzen und basiert auf der Annahme, dass ein bestimmtes Systemverhalten aus der alltäglichen Variabilität von Teilsystemen (Leistungsschwankungen) resultiert. Durch funktionale Kopplungen und Resonanz können ungewöhnlich starke, positive wie negative Effekte, eintreten, die sich nicht durch lineare Kombination von Ursachen erklären lassen.

Zwischen BOS und Öffentlichkeit sollte unabhängig von kritischen Ereignissen ein stetiger Austausch bestehen, um im Sinne von Frühwarnsystemen frühzeitig von kritischen Entwicklungen Kenntnis zu erlangen und freiwillige Helfer sowie Betroffene in begrenztem Maße auf mögliche Ernstfälle vorzubereiten (z. B. durch kleinere Schulungsmaßnahmen).

## 4 Zusammenfassung und Ausblick

Computerbasierte Werkzeuge werden zunehmend im Krisenmanagement eingesetzt werden, sowohl bei der Zusammenarbeit zuständiger Einrichtungen als auch bei der Einbeziehung freiwilliger Helfer und der (betroffenen) Öffentlichkeit. Da Krisen und Katastrophen unmittelbar und unter unzähligen Umständen auftreten können, müssen die entsprechenden Systeme unter ebenso vielfältigen Bedingungen funktionieren. Dies zu gewährleisten ist eine besondere Herausforderung. Resilience-Engineering dient zunächst dazu, Sicherheit aus einem anderen Blickwinkel zu betrachten und eine ganzheitliche Herangehensweise zu motivieren. Methoden zur Gewährleistung von Resilienz im Entwicklungsprozess gibt es mit Ausnahme der Functional Resonance Analysis Method (FRAM) bislang allerdings kaum. Es

besteht weiterer Forschungs- und Entwicklungsbedarf, insbesondere bzgl. der Modellierung sowie der formativen und summativen Evaluation von Resilienz im Allgemeinen und im Krisenmanagement im Besonderen. Dieser sollte von BOS, politischen Entscheidungsträgern und domänenspezifischen IT-Unternehmen adressiert werden.

### Literaturverzeichnis

- Beneito-Montagut, R., Anson, S., Shaw, D. & Brewster, C. (2013). Resilience: Two case studies on governmental social media use for emergency communication. *Proceedings of ISCRAM 2013 (12-15 May, 2013)*.
- Campbell, F. C. (2008). *Elements of Metallurgy and Engineering Alloys*. ASM International.
- Holling, C. S. (1973). Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics*, 4, 1-23.
- Hollnagel, E. (2012). *FRAM: The Functional Resonance Analysis Method. Modelling Complex Socio-technical Systems*. Aldershot: Ashgate.
- Hollnagel, E., Paries, J., Woods, D.D. & Wreathall, J. (2013). *Resilience Engineering in Practice - A Guidebook*. Aldershot: Ashgate.
- Hollnagel, E., Woods, D.D. & Levenson, N. (2006). *Resilience Engineering - Concepts and Precepts*. Aldershot: Ashgate.
- Kendra, J. M., & Wachtendorf, T. (2003). Elements of Resilience After the World Trade Center Disaster: Reconstituting New York City's Emergency Operations Centre. *Disasters*, 27(1), 37–53.
- Leonhardt, J., Hollnagel, E., Macchi, L. & Kirwan, B. (2009). *A White Paper on Resilience Engineering for ATM*. Eurocontrol.
- Mentler, T., Herczeg, M. (2013). Routine- und Ausnahmehetrieb im mobilen Kontext des Rettungsdienstes. In Boll, S., Maaß, S. & Malaka, R. (Hrsg.): *Mensch & Computer 2013*. München. 109-118.
- Merrick, D. F., Duffy, T. (2013). Utilizing Community Volunteered Information to Enhance Disaster Situational Awareness. *Proceedings of ISCRAM 2013 (12-15 May, 2013)*
- Resilience Engineering Association (2014). *About resilience engineering*. Verfügbar unter <http://www.resilience-engineering-association.org/>
- Reuter, C. & Ritzkatis, M. (2013). Unterstützung mobiler Geo-Kollaboration zur Lagebeurteilung von Feuerwehr und Polizei. In Alt, R. & Franczyk, B. (Hrsg.): *Proceedings of the 11th International Conference on Wirtschaftsinformatik*. Volume 2 (S. 1877–1891). Leipzig: Merkur.
- Ulich, E. (2001). *Arbeitspsychologie*. Zürich: Hochsch.-Verl. an der ETH.
- Vicente, K. J. (1999). *Cognitive work analysis. Toward safe, productive, and healthy computer-based work*. Mahwah: Lawrence Erlbaum Associates.
- Zander, M. (2011). *Handbuch Resilienzförderung*. Springer Verlag.

### Kontaktinformationen

Tilo Mentler (mentler@imis.uni-luebeck.de)