Diagnostische Repositorien zur Unterstützung kollaborativer Entscheidungsprozesse

Michael Herczeg

Kurzfassung

In vielen Anwendungssituationen stehen den Operateuren von Anlagen und Fahrzeugen beim Eintreten von Anomalien, Störungen und Störfällen keine oder nur einfachste diagnostische und entscheidungsunterstützende Hilfsmittel zur Verfügung. Die Folge sind mehr oder weniger systematische, teils zufällige Kollektionen von Beobachtungen. In den Schlussfolgerungs- und Entscheidungsprozessen und den damit verbundenen Erklärungsmodellen spiegeln sich diese unsystematischen Datensammlungen dann wider. Die Schlussfolgerungen basieren so auf unvollständigen und teils falschen Voraussetzungen und die Erklärungsmodelle erklären als Folge davon nur einen Teil der vorhandenen, aus den Beobachtungen abgeleiteten Symptome. Als weitere Störquelle treten aus psychologischen Gründen oft nur ökonomische Erklärungsmodelle auf, die leicht mit bekannten Maßnahmen zu behandeln sind, aber nicht alle Symptome berücksichtigen. Darüber hinaus treten besondere soziale Effekte bei der kollaborativen Problemlösung auf, die beispielsweise durch soziales Konsensbedürfnis und durch hierarchische Dominanz hervorgerufen werden.

In der Summe führen alle genannten Defizite zu subjektiven, unvollständigen und oft falschen Entscheidungen bei der Kontrolle und der Behebung eines kritischen Systemzustandes. Durch ein diagnostisches Repositorium mit semantischen Vernetzungen zwischen Symptomen, Diagnosen, Systemkomponenten, Schutzzielen und Handlungen sowie eine geeignete diagnostische Methode soll so weit wie möglich sichergestellt werden, dass die Entscheidungsfindung auf der Grundlage systematischer und möglichst vollständiger Erhebung und Verarbeitung von Beobachtungen durch eine Arbeitsgruppe stattfindet. Die Beobachtungen, Schlussfolgerungen und Maßnahmen werden dokumentiert und stehen späteren Analysen und Revisionen zur Verfügung. Der kollaborative Entscheidungsprozess wird auf diese Weise stärker objektiviert und systematisiert, so dass Entscheidungen für Behebungs- und Schutzmaßnahmen auf möglichst klarer und relevanter Faktenlage sowie nachvollziehbaren Modellbildungen erfolgen.

1. Einleitung

Treten in Systemen Anomalien, Störungen, Störfälle oder Unfälle – im Folgenden ohne Klassifikation unter Anomalien subsummiert – auf, so muss unter unterschiedlichen Randbedingungen eine Behandlung der Anomalie durch Beseitigung der Ursache vorgenommen werden oder, wenn dies nicht möglich ist, ein definiertes Sicherheitsziel erreicht werden. In sicherheitskritischen Anwendungsbereichen wird zu diesem Zweck ein organisatorisches Rahmensystem, auch ***Sicherheitsmanagementsystem*** genannt, geschaffen.

Der prinzipielle Ablauf der Entdeckung und Behandlung einer Anomalie wurde durch Rasmussen in einem Modell, der *„Decision-Ladder“* [Rasmussen 1984], in einzelne Phasen gegliedert (siehe Abbildung 1). Die linke Seite des Modells zeigt die aufsteigenden Phasen des diagnostischen Prozesses, die oben in die Bewertungs- und Entscheidungsphase und anschließend rechts absteigend in den Handlungsprozess einmündet.

erschienen in: Entscheidungsunterstützung für die Fahrzeug- und Prozessführung, Herausgeber: M. Grandt, DGLR-Bericht 2003-04, Deutsche Gesellschaft für Luft- und Raumfahrt, Bonn, 2003, pp. 117-131

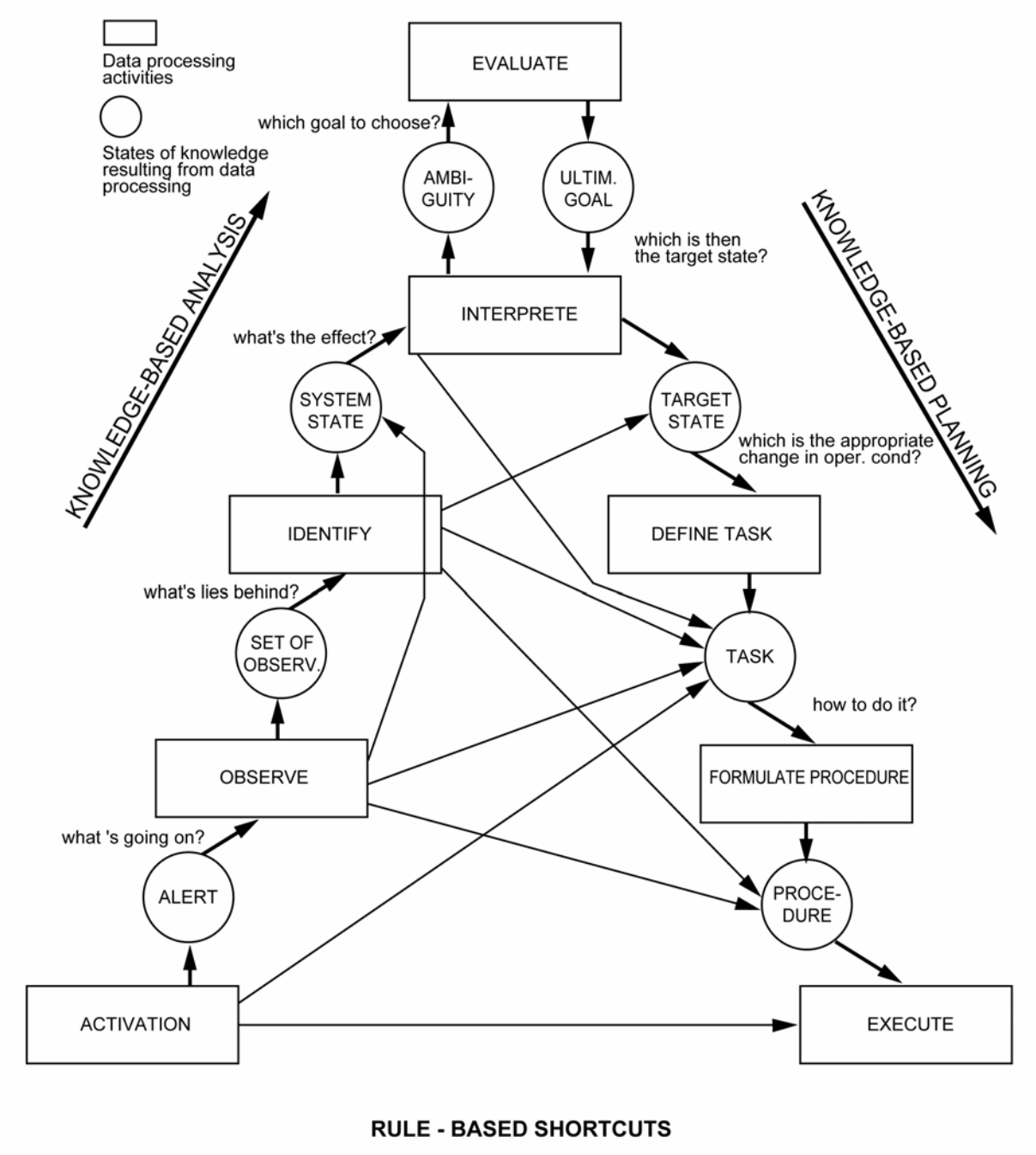

Abbildung 1: Decision-Ladder (nach [Rasmussen 1984])

Rasmussen weist auf eine Reihe von Fehlerquellen hin, die den prinzipiell transparenten und rationalen Problembehebungsprozess stören. So treten beispielsweise zwischen den Phasen gelegentlich „Kurzschlüsse“ auf (siehe lange Pfeile in Abbildung 1), die die Systematik des Prozesses unterbrechen und oft fehlerbehaftete Entscheidungen oder Handlungen nach sich ziehen. Die Gründe dafür sind unterschiedlich, beispielsweise Automatisierungen, falsche Regelanwendungen, Erkennungsfehler oder auch unvollständige Analyse oder Planung aus Gründen der Ökonomie oder Bequemlichkeit.

Die Fehleranfälligkeit dieses Prozesses verschärft sich noch durch die Beteiligung mehrerer Personen an der Behandlung der Anomalie, weil diese unterschiedliche Informationsstände

und inkongruente mentale Modelle vom System besitzen und diese durch eine Mischung aus formalen und informellen Kommunikationsprozessen in weitgehend undefinierter Weise abstimmen, wenn sie die Lage bewerten oder Entscheidungen treffen. Dem gegenüber kann eine Gruppe von Problemlösern, im folgenden Team oder Arbeitsstab genannt, ein umfassenderes und korrekteres Erklärungsmodell als ein Individuum erarbeiten und in einem gemeinsamen transparenten und dokumentierten Entscheidungsprozess reflektieren und kritisch abwägen und so einer bestmöglichen Lösung zuführen. Auch die genannten typischen Kurzschlussübergänge können durch eine kritische Problemlösung im Team in hohem Maße vermieden oder gemeinsam begründet und legitimiert werden. Die Beobachtungen, Symptome und Erklärungsmodelle entstehen und verblassen in den mentalen Modellen der am diagnostischen Prozess beteiligten Personen. Festgehalten werden nur vermeintlich relevante oder geklärte Informationen, der Rest verschwindet im diffusen informellen Kommunikationsprozess der Beteiligten ohne systematische Klärung oder spätere Nachvollziehbarkeit.

Im Folgenden soll eine Reihe von Anforderungen diskutiert werden, die eine Grundlage für möglichst transparente und zuverlässige kollaborative Analyse- und Entscheidungsprozesse darstellen. Die Anforderungen entstammen einer Reihe von Stör- und Unfallanalysen, insbesondere aus Luftfahrt und Kerntechnik, bei denen unsystematische Analysen, soziale Prozesse und wirtschaftlicher Druck als wesentliche Ursachen identifiziert werden konnten.

2. Anforderungen an die diagnostische Phase

Tritt eine Anomalie in einem System auf, so besteht die erste Leistung darin, diese und den Bedarf einer Intervention überhaupt zu erkennen. Dazu muss entweder der Prozess direkt oder über eine Instrumentierung beobachtet und mit dem Normalzustand verglichen werden. Wird eine Anomalie erkannt, müssen weitere Prozessdaten (Rohdaten) gesammelt werden, die helfen, die Anomalie hinsichtlich ihrer Ursachen und möglichen Folgen einzugrenzen oder zu erkennen. Die Rohdaten werden zunächst durch Verarbeitung in Symptome übergeführt. Eingrenzen muss im Bereich sicherheitskritischer Systeme heißen, dass Systemkomponenten oder Schutzziele systematisch (z.B. hierarchisch) analysiert werden. Lässt sich die Funktionsfähigkeit einer Systemkomponente nicht plausibel durch detaillierte Analysen nachweisen, ist sie als gestört einzustufen und im Sinne von Worst-Case-Annahmen auf mögliche Wirkungen zu untersuchen. Weitere Detaillierungen sind nicht zwangsläufig notwendig. Im Zweifelsfall wird das ganze System oder Teilsystem als gestört diagnostiziert und, wenn möglich, stillgelegt oder in einen anderen sicheren Zustand gebracht. Diese besondere Form der ***Vollständigkeit*** einer Analyse ist die Voraussetzung für den weiteren sicherheitsgerichteten Verlauf der Behandlung der Anomalie.

Die Diagnostik technischer Systeme lässt sich als ***Klassifikationsproblem*** beschreiben. Dabei sind Problemmerkmale (Symptome) auf Erklärungsmodelle (Diagnosen) abzubilden. Hierfür gibt es unterschiedliche Methoden. Die wichtigsten sind [Puppe 1990]:

- sichere Klassifikation (Entscheidungstabellen, Entscheidungsbäume)
- fallvergleichende Klassifikation (fallbasierte Diagnostik)
- statistische Klassifikation (probabilistische Diagnostik)
- heuristische Klassifikation (logikbasierte Diagnostik)
- modellbasierte Klassifikation (Fehlermodelle, funktionale Diagnostik)

Diese Methoden treten in den meisten praktischen Situationen in Mischformen auf, was dazu führt, das die Systematik und Vollständigkeit der Diagnostik und damit ihre Aussagefähigkeit und Sicherheit oft schwer zu fassen ist.

Im Bereich der ***bekannten und zu erwartenden Anomalien*** liegen für sicherheitskritische Anlagen meist vorbereitete Diagnostik- und Handlungsanweisungen vor. Diese werden oft in Form von Entscheidungstabellen und Entscheidungsbäumen für die Operateure vorbereitet. Auf diese Weise werden Standardproblemfälle im Allgemeinen systematisch, optimiert und daher auch sehr sicher abgearbeitet (sichere Klassifikation). Auch wenn solche Handlungsanweisungen nicht explizit vorliegen, sind Operateure meist in der Lage, in ihnen bekannten Problemsituationen durch automatisiertes oder regelbasiertes Wissen zuverlässig zu handeln [Rasmussen 1983].

Im Bereich der ***unerwarteten Anomalien*** liegen keine speziellen Erfahrungen und daraus abgeleitet optimierten Diagnostik- und Handlungsanweisungen vor. Deshalb müssen andere diagnostischen Methoden angewandt werden [Rasmussen, Goodstein 1988].

Die statistischen (probabilistischen) Verfahren setzen typischerweise auf dem Theorem von Bayes auf. Hierbei wird auf Grundlage einer Menge von Symptomen und A-Priori-Wahrscheinlichkeiten die wahrscheinlichste Lösung errechnet und ausgewählt. Die Voraussetzungen für die Anwendung dieser Verfahrens, wie die Unabhängigkeit der Symptome, die Vollständigkeit der Lösungsmenge, der wechselseitige Ausschluss von Lösungen sowie die Repräsentativität der Fallsammlungen und Gültigkeit der A-Priori-Wahrscheinlichkeiten sind im allgemeinen nicht gegeben, so dass diese Verfahren selten systematisch und sicher zur Anwendung gebracht werden kann.

Die in der Praxis am häufigsten angewandten Methoden sind die verbleibenden fallbasierten, heuristischen und modellbasierten Klassifikationsverfahren. Sie werden bei diagnostischen Prozessen von menschlichen Operateuren oft mehr oder weniger bewusst in gemischter Form angewandt. Gemeinsam ist diesen Methoden die Notwendigkeit Symptome und Erklärungsmodelle zu erfassen, zu diskutieren, zu bewerten und daraus Handlungsentscheidungen abzuleiten. Die Modellierung des betrachteten Systems kann dabei in mehreren Dimensionen erfolgen. Rasmussen [Rasmussen 1985] hat hierfür eine zweidimensionale Modellierung entlang der Dimensionen ***Dekomposition*** (Partonomie, Teilehierarchie) und ***Abstraktion*** vorgeschlagen (siehe Abbildung 2). Hinsichtlich der hier betrachteten Fragestellung kann man die Abstraktionshierarchie auf der obersten Ebene des Zwecks (*Functional Purpose*) neben den ***Produktionszielen*** (*Production Goals*) die ***Schutzziele*** (*Safety-Goals*) und auf der nächst niedrigeren Ebene der Abstrakten Funktionen *(Abstract Functions*) sowie den darunter liegenden Ebenen die Kausalstruktur modellieren. Die Dekompositionshiearchie wird auf der jeweiligen Abstraktionsebene als Teilehierarchie von Sicherheitszielen bzw. Funktionsstrukturen modelliert. Die Störungsanalyse lässt sich auf eine solche Systemmodellierung mental und auch technisch abbilden.

Die Systematik oder gar Vollständigkeit der Analyse erfordert eine lückenlose und transparente ***Dokumentation***, da Menschen insbesondere unter Beanspruchung und bei Unterbrechungen nur begrenzt systematisch und verlässlich arbeiten [Kantowitz, Sorkin 1987]. Hierfür müssen Hilfsmittel bereitgestellt und genutzt werden, die eine kausal- oder schutzzielorientierte Vorgehensweise isomorph zur oben genannten Systemmodellierung widerspiegeln und die erfassten oder noch zu erfassenden Beobachtungen bzw. die entwickelten Erklärungsmodelle mit zeitlicher, räumlicher und problembezogener weiterer Attributierung darstellen. Dabei ist im Rahmen kollaborativer Arbeit die jeweilige personelle Zuständigkeit zu vermerken und, falls Beobachtungen oder Handlungen getätigt wurden, von den jeweiligen Verantwortlichen auch zu signieren. Eine laufende oder spätere Rekonstruktion und Überprüfung der jeweiligen Aktivität und Verantwortung muss eindeutig möglich sein.

Die Beobachtungen und daraus abgeleiteten Symptome sowie die entwickelten Erklärungsmodelle oder Schutzziele sind hinsichtlich ihrer Bedeutung für die Anomalie und die weitere Vorgehensweise mit einer ***Priorisierung*** zu versehen. Bei Unsicherheiten oder Verzweigung der Analyse sind mehrere weitere Untersuchungspfade auch parallel zu planen und in eindeutige Zuständigkeiten zu übergeben. Die Priorisierung umfasst neben einem Ranking der Symptome auch die Aufgabenverteilung weiterer Analysen auf die einzelnen Akteure, mit klaren Aufgabenstellungen, Vorgehensweisen und Zeitvorgaben. Auch dies ist zu dokumentieren und im Prozessablauf hinsichtlich der vollständigen, angemessenen und zeitgerechten Abarbeitung organisatorisch zu sichern.

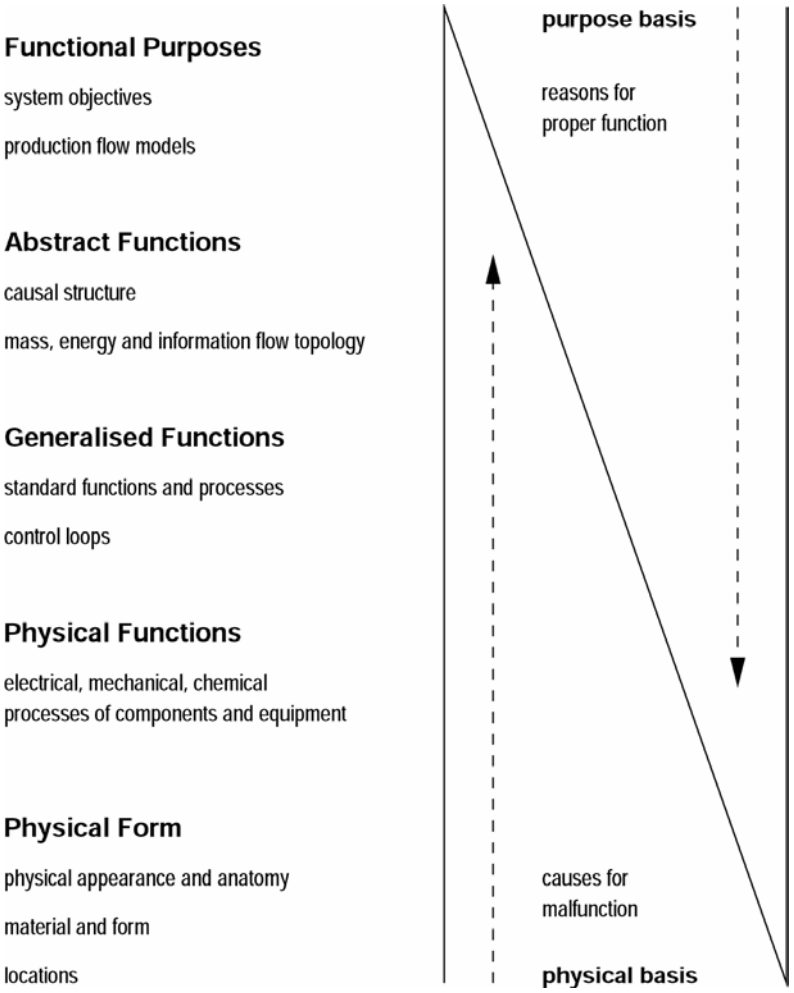

Abbildung 2: Abstraktionshierarchie (nach [Rasmussen 1985])

Diese ***diagnostische Dokumentation*** muss unabhängig von der Tragweite oder der zeitlichen Randbedingungen qualitätsgesichert praktiziert werden, damit die Vorgehensweise und der Stand der Diagnostik jederzeit von allen Beteiligten (auch Aufsichtsbehörden) hinterfragt und vom Team vervollständigt werden kann. Nur wenn eindeutige Eilbedürftigkeiten bei der Behandlung der Anomalie die Dokumentation unmöglich machen, muss sie auf einen späteren Zeitpunkt verschoben werden. Dies gilt allerdings nur für Anomalien in sehr schnellen Prozessen, die eine Handlung im Bereich von Sekunden oder wenigen Minuten erfordern. Allerdings kann selbst hier in fast allen denkbaren Fällen durch technische Unterstützung (z.B. Video-/Voicerecording, Notizen) eine solche Dokumentation für die spätere Analyse oder Revision realisiert werden. Es ist zu beobachten, dass insbesondere in der Teamarbeit Dokumentationsschritte oft vergessen oder einfach nicht getätigt werden. Gründe

können u.a. sein, dass eine solche Dokumentation von den Beteiligten nicht gewünscht wird, an das kollektive Gedächtnis geglaubt wird oder einfach keine Methoden bereitstehen, für die das Personal sensibilisiert und qualifiziert wurde.

3. Anforderungen an die Bewertungs- und Entscheidungsphase

Ist die Beobachtungs- und Bewertungsphase zu einem gewissen Grad erfolgt, d.h. es liegen erste auswertbare Beobachtungen vor, können im Falle einer Kausalanalyse erste ***Erklärungsmodelle*** entwickelt werden. Ist die Situation zeitkritisch, d.h. es besteht die Gefahr von weiteren Schäden an der Anlage oder der Umwelt während der Ursachenanalyse, so können stattdessen um die Symptomatik herum ***Schutzziele*** anvisiert werden. Der Unterschied zwischen Erklärungsmodellen und Schutzzielen ist hierbei sekundär, da es sich letztlich in beiden Fällen um abstrakte Modelle (siehe oben) des realen Prozesses handelt. Erklärungsmodelle versuchen dabei kausale Ursache-Wirkungsketten zu beschreiben, um dann von Ausgangszuständen möglichst sicher, effektiv und effizient zu Zielzuständen zu kommen. Schutzzielmodelle sind stattdessen meist so konstruiert, dass auch ohne Ist-Zustände zu kennen, sichere Zielzustände effektiv erreicht werden. Dabei wird die Ökonomie der Behebung aufgrund fehlender Optimierungsmodelle zugunsten schneller und sicherer Reaktionen im Sinne konservativer Entscheidungsfindung in den Hintergrund gestellt.

Werden zur Optimierung der Behebung Erklärungsmodelle entwickelt, muss sichergestellt werden, dass diese unter ***Berücksichtigung aller Beobachtungen*** abgestimmt und dokumentiert werden. Es muss eine ***von allen Beteiligten akzeptierte vollständige und schlüssige Erklärung*** entwickelt werden. Dies entspricht der sicherheitstechnisch außerordentlich wichtigen Methode der ***überdeckenden Klassifikation***. Konkurrierende Erklärungsmodelle müssen differenzialdiagnostisch gegeneinander verglichen, bewertet und ggf. priorisiert werden. Ohne den Zwang zur überdeckenden, kollektiv und differenzialdiagnostisch geprüften Klassifikation neigt ein menschlicher und wirtschaftlicher Problemlösungsprozess dazu, günstige Erklärungsmodelle überzugewichten und bewusst oder unbewusst Risiken einzugehen [Röbke et al. 1973]. Schwierige und komplexe Symptome werden aus Bequemlichkeit, Mangel an Erfahrung, Glauben an die eigene Unverletzlichkeit oder auch unzureichendem Sicherheitsbewusstsein auf Kosten der Sicherheit ausgeblendet (siehe Abbildung 3).

Bei kollaborativen Problemlöseprozessen müssen gerade die gemeinsame Entwicklung und das gemeinsame Verständnis der Analyse in den Vordergrund rücken. Treten unterschiedliche, insbesondere unverträgliche Einschätzungen auf, sind diese ebenfalls zu dokumentieren. Die weitere Priorisierung und Vorgehensweise muss durch den jeweils Verantwortlichen unter Berücksichtigung der vorhandenen, in der Gruppe eventuell auch unterschiedlichen oder gar widersprüchlichen Einschätzungen getroffen werden. Auch dies ist zusammen mit der Entscheidung für ein Erklärungsmodell festzuhalten.

Überdecken die entwickelten Erklärungsmodelle nicht schlüssig die Symptome (***Belastbarkeit des Erklärungsmodells***) so sind bei ausreichend vorhandener Zeit weitere Analysen vorzunehmen oder stattdessen schutzzielorientierte Vorgehensweisen zu wählen. Die jeweils gewählte Vorgehensweise ist zu begründen und zu dokumentieren.

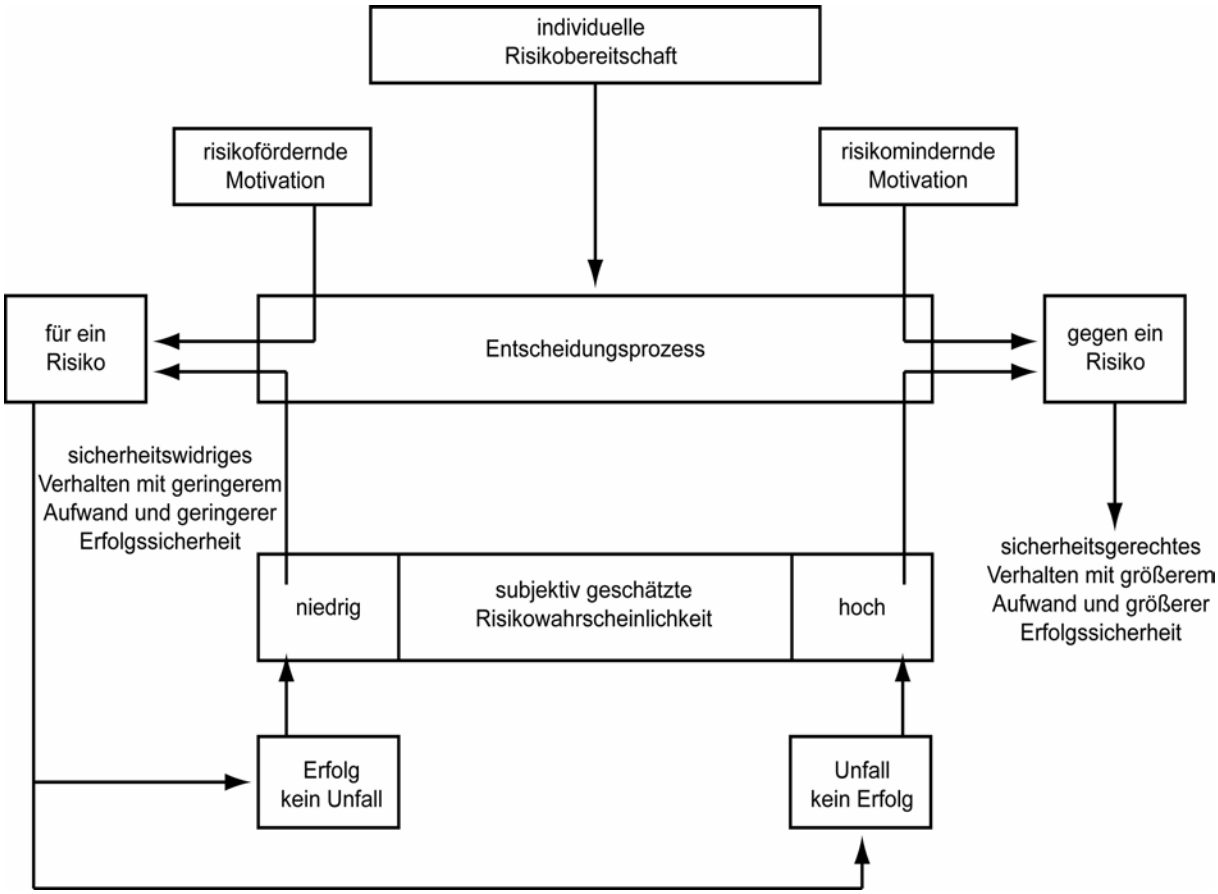

Abbildung 3: Einflüsse auf sicherheitswidriges Verhalten (nach [Röbke et al. 1973])

4. Das diagnostische Repositorium

Die oben dargestellten Anforderungen müssen durch geeignete Methoden auf die Praxis des Anlagenbetriebs abgebildet werden. Es soll an dieser Stelle nicht davon ausgegangen werden, dass weitere technische Hilfsmittel die Diagnose und die Planung der Maßnahmen selbst erleichtern oder sogar (halb-)automatisch leisten. Solche Möglichkeiten sollen alle als bereits ausgeschöpft angesehen werden und haben, falls sie vorhanden waren, den diagnostischen und evaluierenden Prozess bereits gestützt. Die Operateure stehen somit vor der Aufgabe durch geeignete Bewertungen und Aktivitäten die Anomalie zu behandeln. Zu diesem Zweck soll ihnen ein zur Unterstützung der Erfüllung der genannten Anforderungen eine Informationsstruktur in Form eines diagnostischen Repositoriums bereitgestellt werden, das mit den Symptomen, den daraus abgeleiteten Erklärungsmodellen oder Schutzzielen sowie den vorgenommenen Handlungen iterativ gefüllt wird. Es dient im Weiteren als Grundlage und Referenz für die systematische Bearbeitung von Anomalien.

Das ***Informationsmodell*** des Repositoriums sollte dazu eine folgende Grundstruktur aus den folgenden Kategorien bereitstellen. Weitere Verfeinerung für bestimmte Anwendungsfelder können bedarfsorientiert ergänzt werden.

4.1 Symptome (Beobachtungen)

Eine Anomalie wird anhand von besonderen Beobachtungen identifiziert, die dann mehr oder

weniger stark zu Symptomen abstrahiert werden. Nach Wahrnehmung der Anomalie tauchen üblicherweise durch die weitere Analyse weitere Symptome auf, da ein Systemfehler im Allgemeinen eine Vielzahl von Symptomen hervorruft. Nach Identifikation einer Anomalie sind alle Symptome zu dokumentieren. Die Symptome können von unterschiedlichen Beobachtern im Betrieb gesucht, beobachtet und erfasst und in einer Struktur wie der folgenden dokumentiert werden:

- Name des Symptoms
- Beschreibung des Symptoms
- Beobachter (Erstbeobachter sowie zuständige Person)
- Art der Beobachtung (direkt, instrumentell)
- Ort des Auftretens (Systemkomponente, Systembereich)
- Zeitpunkt des ersten Auftretens (eventuelle zeitliche Erscheinungsform, wie z.B. stabil, intermittierend, mit bestimmter Frequenz)
- Wichtigkeit des Symptoms
- Dringlichkeit des Symptoms
- Ursache (Referenz zu Erklärungsmodell, soweit schon vorhanden)
- Schutzziel (Referenz zu Schutzziel, soweit schon vorhanden)

Symptome werden über den gesamten diagnostischen Prozess gesammelt und in ihren Beschreibungen sukzessive ergänzt. Auch während der späteren Durchführung von Maßnahmen zur Behebung der Anomalie können neue Symptome auftreten, die dokumentiert werden müssen.

Ein verfeinertes diagnostisches Modell unterscheidet Beobachtungen und Symptome und ist dadurch zusätzlich in der Lage eventuell fehlerhafte Abstraktionen von Beobachtungen zu vereinfachten linguistischen Symptombegrifflichkeiten zu erkennen.

4.2 Erklärungsmodelle (Diagnosen)

Ein wichtiger Schritt nach der Feststellung von Symptomen ist die Entwicklung von Erklärungsmodellen. Diese sind meist technische Ursachenbeschreibungen, die ein oder mehrere Symptome im Sinne einer Kausalkette schlüssig erklären. Dazu sollte für ein Erklärungsmodell folgendes dokumentiert werden:

- Name des Erklärungsmodells
- Beschreibung des Erklärungsmodells
- erklärte Symptome (Referenz zu dokumentierten Symptomen)
- Systemkomponenten (Referenz auf betroffene Systemkomponenten)
- Bewertung des Erklärungsmodells (Bedeutung, Bedenken, Wahrscheinlichkeiten)

Die Erklärungsmodelle sind im Team zu diskutieren und auf ihre Schlüssigkeit (Überdeckung der Symptome, Wahrscheinlichkeiten) zu überprüfen. Gibt es in der Einschätzung von Erklärungsmodellen Bedenken einzelner Beteiligter im Team so sind diese in der Dokumentation festzuhalten. Erklärungsmodelle sind hinsichtlich ihrer Wahrscheinlichkeit zu bewerten. Hierbei müssen eventuelle unterschiedliche Einschätzungen der Beteiligten festgehalten werden.

Erklärungsmodelle liefern selbst im Sinne einer Kausalitätskette Hinweise auf weitere Symptome. Diese sind entweder schon durch Beobachtungen generiert worden oder ihr Vorliegen kann überprüft werden. Dieser Schritt der Überprüfung eines Erklärungsmodells

führt in eine diagnostische Iteration, die dann endet, sobald alle erwarteten Symptome überprüft wurden. Da einzelne Symptome durch unterschiedliche Erklärungsmodelle fundiert werden können, besteht die Möglichkeit zu differentialdiagnostischen Vergleichen.

4.3 Systemkomponenten

Systemkomponenten sind technische Bezugspunkte für Symptome, Erklärungsmodelle und Schutzziele. Sie werden je nach Abstraktionsgrad (siehe Abschnitt 2) der Diagnostik in unterschiedlicher Weise und zu unterschiedlichem Zweck modelliert und diskutiert. Sie sind Teil der auf diesen Abstraktionsebenen jeweils bedeutungsvollen Dekompositionshierarchien [Rasmussen 1985]. Für die hier diskutierten diagnostischen Methoden sollen Systemkomponenten neben den technologischen Eigenschaften ergänzend folgendermaßen modelliert sein:

- Name der Systemkomponente
- Beschreibung der Systemkomponente
- hierarchisch übergeordnete Systemkomponente (Referenz)
- hierarchisch untergeordnete Systemkomponente (Referenz)
- Symptome (Referenz zu Symptomen an dieser Komponente)
- Erklärungsmodelle (Referenz auf die mit dieser Komponente verbundenen Erklärungsmodelle)
- Schutzziele (Referenz auf die mit dieser Komponente verbundenen Schutzziele)

Systemkomponenten werden im Allgemeinen im Rahmen der Systementwicklung bereits detailliert modelliert. Derartige Modelle können in ein diagnostisches Repositorium eingebunden werden. Hierbei ist insbesondere auch die Aktualität eines Komponentenmodells zu betrachten, die bei redundanter Datenhaltung schnell verloren gehen kann.

4.4 Schutzziele

Bei oder auch statt der Entwicklung von Erklärungsmodellen werden aus Symptomen Schutzzielverletzungen abgeleitet. Die Erkennung von Schutzzielverletzungen ist in sicherheitskritischen Systemen wichtiger als die Diagnostik selbst. Schutzziele können auch durch andere Methoden als durch den diagnostischen Prozess entwickelt werden. Sie können vor allem aus einer vorgegebenen Schutzzielhierarchie abgeleitet werden [Rasmussen 1985]. Die Schutzziele können im Rahmen des hier beschriebenen Ansatzes folgendermaßen dokumentiert werden:

- Name des Schutzziels
- Beschreibung des Schutzziels
- hierarchisch übergeordnetes Schutzziel (Referenz)
- hierarchisch untergeordnete Schutzziele (Referenz)
- Erklärungsmodell (Referenz auf eventuell vorhandenes Erklärungsmodell, das zur Schutzzielverletzung führt)
- Aufgaben zur Erreichung des Schutzziels (Referenz auf Aufgaben)
- Schutzziel erreicht?

Müssen Schutzziele als nicht erreicht eingestuft werden, sind diese zu priorisieren und Maßnahmen zu ihrer Sicherstellung zu planen.

4.5 Aufgaben und Handlungen

Die Planung von Maßnahmen zur Erreichung von Schutzzielen muss letztlich in Handlungen übergeführt werden, die ebenfalls zu dokumentieren sind. Die Handlungen entstehen normalerweise durch die Annahme von Systemzuständen, die in andere Systemzustände übergeführt werden sollen. Die Handlungssequenzen lassen sich im Sinne der Handlungspsychologie als ***Aufgaben*** (Tätigkeiten, Tasks) betrachten:

- Name der Aufgabe
- Beschreibung der Aufgabe
- hierarchisch übergeordnete Aufgabe (Referenz)
- hierarchisch untergeordnete Aufgaben (Referenz)
- Zuständigkeit für die Durchführung
- Zuständigkeit für die Überprüfung der Durchführung (Qualitätssicherung)
- Zeitdauer der Ausführung der Aufgabe
- Besonderheiten beim Ausführen der Handlung
- mit der Aufgabe verbundenes Schutzziel (Referenz)
- mit der Aufgabe verbundenes Reparaturziel
- Aufgabe erfolgreich abgeschlossen?

Aufgaben bilden hierarchische Strukturen [Herczeg 1994, Herczeg 1999, Herczeg 2001], die in sequentielle oder parallele Handlungsabläufe überzuführen sind. Die über- und untergeordneten Aufgaben in der Informationsstruktur beziehen sich auf diese ***Aufgabenhierarchie***. Die mit Schutzzielen direkt verbundenen Aufgaben müssen nach Abschluss die Erreichung des jeweiligen Schutzziels mit sich bringen.

Aufgaben und Handlungen können in der Modellierung auch getrennt werden. Dies erlaubt Aufgabenstrukturen unabhängig von Ausführungen zu entwickeln und ermöglicht darüber hinaus alternative, parallele oder auch misslungene Handlungen besser zu modellieren.

5. Implementierungen

Die im vorausgegangenen Kapitel dargestellte minimale diagnostische Informationsstruktur führt während der Bearbeitung einer Anomalie zu Informationssammlungen beträchtlicher Komplexität. Dabei ist zu berücksichtigen, dass diese Informationen potentiell relevant sind und in jedem Fall beim systematischen diagnostischen Prozess. Steht dafür keine Methode der systematischen Sammlung und Bearbeitung zur Verfügung, findet bzw. verliert sich diese Information in den Köpfen der Mitglieder des Arbeitsstabs und des Betriebs. Genau dies war Ausgangspunkt unserer Betrachtungen. Die Frage, die bleibt, ist also, wie können wird den diagnostischen Prozess in einer Weise methodisch unterstützen, dass das Team in der Lage ist, die Problemstellung zielorientiert, systematisch, vollständig und transparent hinsichtlich der gewonnenen Informationen zu lösen.

Methodische Lösungen auf Grundlage einer solchen Informationsstruktur sind viele denkbar. An dieser Stelle sollen deshalb nur gewissermaßen zwei grundsätzliche Lösungen angedeutet werden, nämlich erstens eine komfortable computergestützte Groupware und zweitens eine Minimallösung die auf nichts anderem als papierbasierter Dokumentation aufbaut. Es ist gut vorstellbar, dass beide Lösungen zur Verfügung stehen, die computergestützte Groupware als normale betriebliche Lösung und die papierbasierte Lösung als Notfallsystem, falls das Computersystem nicht zur Verfügung steht.

5.1 Computergestützte Groupware

Ein mit Hilfe eines Computersystems realisiertes diagnostischen Repositoriums implementiert das dargestellte Informationsmodell mit Hilfe einer Datenbank. Ausgabemöglichkeiten erlauben das mit Daten gefüllte Informationsmodell zu präsentieren und zu inspizieren. Neue Beschreibungsentitäten (Instanzen der o.g. Kategorien) können mit formularartigen Benutzungsschnittstellen gemäß dem Modell angelegt und mit Daten gefüllt werden.

Durch verschiedene ***Sichten auf das Informationsmodell*** können verschiedene diagnostische Tätigkeiten unterstützt werden. Wichtige Sichten sind u.a.:

- Darstellung aller Symptome und ihr Bearbeitungsstand (Analyse, Auswertung) sowie den dazugehörigen Verantwortlichkeiten
- Darstellung aller Erklärungsmodelle und Überdeckung der Symptome durch die Erklärungsmodelle sowie ihre differenzialdiagnostische Bewertung (Wahrscheinlichkeiten) durch das Team im Arbeitsstab (auch abweichende Einschätzungen)
- Darstellung aller Schutzziele, ihre Prioritäten und ihr Status
- Darstellung geplanter und getätigter Handlungsabläufe, Zuständigkeiten und Bearbeitungszustände mit Bezug auf die Erklärungsmodelle (Begründung der Maßnahmen)

Weitergehende Systemunterstützungen durch ***wissensbasierte Systeme, insbesondere Expertensysteme*** sind über den gesamten Problemlösungsprozess denkbar [Rasmussen, Goodstein 1985, Puppe 1988, Puppe 1990], haben sich in der Praxis jedoch aufgrund diverser Probleme, wie technische Hindernisse, unklare Zuverlässigkeit, aufwändige Wissensakquisition und mangelndes Vertrauen in die Technologie bis heute nicht wesentlich verbreitet und weiterentwickelt. Stark arbeitsteilige Supervisory-Control-Systeme [Sheridan 1987, Sheridan 1988] weisen wiederum begrenzte Wissensrepräsentationsmechanismen auf und sind daher in selten auftretenden komplexen Problemsituationen wenig unterstützend.

5.2 Papierbasiertes Notfallsystem

Als Alternative zu computergestützten diagnostischen Repositorien sowie als Notfallmethode sofern technische Unterstützungssysteme nicht bereitstehen, kommen papierbasierte Lösungen in Frage. Dabei können für die einzelnen Kategorien Formulare entwickelt werden, in die die Daten aus dem diagnostischen Prozess erfasst werden können. Durch systematische fortlaufende Nummerierungs- und Ordnungssysteme kann die Konsistenzhaltung zwischen den Papierdokumenten erleichtert werden. Da in einem Prozess sehr viele betrachtete Entitäten auftreten können, ist eine Zuständigkeit für die systematische und vollständige Registratur der Dokumente notwendig. Durch Qualitätssicherungsmaßnahmen sind Konsistenz, Zuordnung zu Verantwortlichkeiten sowie die Einhaltung von Terminen und Zeiten sicherzustellen.

Die zusätzliche Bereitstellung von tabellarischen Übersichten erleichtert den Überblick über den Bearbeitungsstand und unterstützt die musterbasierte Erkennung von Systematik und Zusammenhängen.

In einem Ausbildungszentrum für Kernkraftwerkspersonal wird derzeit eine großformatige Schreibtischunterlage entwickelt, in die in ähnlich wie hier beschriebener Weise Beobachtungen jederzeit sofort erfasst und dokumentiert werden können. Dies weist auf ein wichtiges Prinzip jeder Methode hin. Die Schwelle zur Nutzung einer solchen Methode muss sehr gering sein, so dass jederzeit beim Auftreten auch harmlos erscheinender Anomalien die diagnostische Methode in Aktion tritt und nicht erst nachdem größerer Schaden oder

Zeitdruck entstanden ist. Diagnostik in sicherheitskritischen Anwendungsbereichen erfordert die ständige Aufmerksamkeit und Sorgfalt gerade im Fall der nicht durch Betriebshandbücher vorbereiteten Verfahrensweisen.

Zusammenfassung

Diagnostische und problemlösende Prozesse in sicherheitskritischen Anwendungsbereichen erfordern eine systematische Vorgehensweise sowie eine transparente und vollständige Dokumentation. In kollaborativen Arbeitskontexten ist die laufende Aktualität, Einsehbarkeit und Nachvollziehbarkeit von Analysen und Entscheidungen durch alle Beteiligten unabdingbare Voraussetzung, um irrationale und ausschließlich ökonomische Verhaltensweisen auf Kosten sicherheitsgerichteten Verhaltens zu verhindern. Systematik und Rationalität in der Arbeitsweise bedingen sich gegenseitig und bilden die Grundlage von qualitätsgesicherten Prozessen, insbesondere auch von Sicherheitsmanagement. Soziale Aushandlungsprozesse ohne Dokumentation neigen zu informellen und hierarchisch dominierten Entscheidungen bei denen kritische Reflektionen oft überlagert werden oder gar nicht stattfinden.

Diagnostische Repositorien bieten eine Informationsstruktur, um alle wichtigen Daten, Symptome, Erklärungsmodelle, Schutzziele und Handlungen zu erfassen und für einen Arbeitsstab und spätere Revisionen verfügbar zu halten. Informationen, Bewertungen, Entscheidungen und Handabläufe werden dokumentiert und allein deshalb von den Verantwortlichen ständiger kritischer Überprüfung unterzogen, um später die Verhaltensweisen begründen und rechtfertigen zu können. Solche diagnostische Repositorien können sowohl computergestützt als auch manuell realisiert werden. Kooperationsplattformen und Datenbanken können eine geeignete Grundlage computergestützter Repositorien bilden. Formulare und tabellarische Darstellungen erlauben derartige Repositorien auch in Papierform zu realisieren, um diese auch unabhängig von technischen Randbedingungen nutzen zu können.

Literatur

[Herczeg 1994] M. Herczeg: *Software-Ergonomie*, Addison-Wesley und Oldenbourg-Verlag, 1994.

[Herczeg 1999] M. Herczeg: *A Task Analysis Framework for Management Systems and Decision Support Systems*, in: Proceeding of AoM/IaoM, 17. International Conference on Computer Science, San Diego, California, August 1999, pp. 29-34.

[Herczeg 2000] M. Herczeg: *Sicherheitskritische Mensch-Maschine-Systeme*, in: FOCUS MUL 17, Heft 1, 2000, pp. 6-12.

[Herczeg 2001] M. Herczeg: *A Task Analysis and Design Framework for Management Systems and Decision Support Systems*, in: ACIS International Journal of Computer & Information Science, Vol. 2, No. 3, September 2001, pp. 127-138.

[Kantowitz, Sorkin 1987] B.H. Kantowitz, R.D. Sorkin: *Allocation of Functions*, in: G. Salvendy (Ed.): *Handbook of Human Factors*, John Wiley and Sons, 1997, pp 355-369.

[Kritzenberger, Herczeg 2001] H. Kritzenberger, M. Herczeg: *A Task- and Scenario-Based Analysis and Design Method for User-Centered Systems*, in: Proceedings of HCI International 2001, 9th International Conference on Human-Computer Interaction jointly with 4th International Conference on Engineering Psychology and Cognitive Ergonomics and 1st International Conference on Universal Access in Human-Computer Interaction, August 2001, New Orleans, Lawrence Erlbaum Associates, pp. 229-231.

[Puppe 1988] F. Puppe: *Einführung in Expertensysteme*. Studienreihe Informatik. Springer-Verlag. 1988.

[Puppe 1990] F. Puppe: *Problemlösungsmethoden in Expertensystemen*. Studienreihe Informatik. Springer-Verlag. 1990.

[Rasmussen 1983] J. Rasmussen: *Skills, Rules, and Knowledge; Signals, Signs, and Symbols, and Other Distinctions in Human Performance Models*, IEEE Transactions on Systems, Man, and Cybernetics, Vol. SMC-13, No. 3, May/June 1983, pp. 257-266.

[Rasmussen 1984] J. Rasmussen: *Strategies for State Identification and Diagnosis in Supervisory Control Tasks, and Design of Computer-Based Support Systems,* Advances in Man-Machine Systems Research, Vol.1, Denmark, August 1985, pp. 139-193.

[Rasmussen 1985] J. Rasmussen: *The Role of Hierarchical Knowledge Representation in Decisionmaking and System Management*, IEEE Transactions on Systems, Man, and Cybernetics, Vol. SMC-15, No. 2, March/April 1985, pp. 234-243.

[Rasmussen, Goodstein 1985] J. Rasmussen and L.P. Goodstein: *Decision Support in Supervisory Control*, Technical Report M-2525, Risø National Laboratory, Roskilde, Denmark, August 1985.

[Rasmussen, Goodstein 1988] J. Rasmussen and L.P. Goodstein: *Information Technology and Work*, in: M. Helander (Hrsg.): *Handbook of Human-Computer Interaction*, Elsevier Science Publishers B.V. (North Holland), Amsterdam, 1988, pp. 175-201.

[Röbke et al. 1973] R. Röbke, B. Schulte, K. Thimm: *Verhaltensvariabilität des Menschen als Unfallursache.* Bundesanstalt für Arbeitsschutz und Unfallforschung Dortmund. Wirtschaftsverlag NW. 1973.

[Sheridan 1987] T.B. Sheridan: *Supervisory Control*, In: G. Salvendy (Ed.): *Handbook of Human Factors*, John Wiley and Sons, 1997, pp. 1243-1268.

[Sheridan 1988] T.B. Sheridan: *Task Allocation and Supervisory Control*, In: M. Helander (Ed.): *Handbook of Human-Computer Interaction*, Elsevier Science Publishers B.V. (North Holland), Amsterdam, 1988, pp. 159-173.