Neue Methoden zur Bewertung der Zuverlässigkeit fortschrittlicher Mensch-Maschine-Schnittstellen digitaler leittechnischer Einrichtungen und personell-organisatorischer Einflüsse

GRS - 460

Gesellschaft für Anlagen-
und Reaktorsicherheit
(GRS) gGmbH

Neue Methoden zur Bewertung der Zuverlässigkeit fortschrittlicher Mensch-Maschine-Schnittstellen digitaler leittechnischer Einrichtungen und personell-organisatorischer Einflüsse

Ewgenij Piljugin
Werner Fassmann
Manuela Jopen
Jens Forner

August 2017

Anmerkung:

Das diesem Bericht zugrunde liegende F&E-Vorhaben wurde mit Mitteln des Bundesministeriums für Wirtschaft und Energie (BMWi) unter dem Kennzeichen RS1525 durchgeführt.

Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Auftragnehmer.

Der Bericht gibt die Auffassung und Meinung des Auftragnehmers wieder und muss nicht mit der Meinung des Auftraggebers übereinstimmen.

GRS - 460
ISBN 978-3-946607-43-4

Deskriptoren

Analysemethoden, Leittechnik, Mensch-Maschine-Schnittstelle, Modellierung, personell-organisatorische Einflüsse, programmierbare logische Schaltungen, qualitative und quantitative Bewertung, Sicherheit, Sicherheitskultur, Zuverlässigkeit

Kurzfassung

Die GRS verfolgt mit dem vom Bundesministerium für Wirtschaft und Energie (BMWi) geförderten Forschungs- und Entwicklungsvorhaben RS1525 generell das Ziel, methodische Ansätze und Werkzeuge für Sicherheitsanalysen in der Kerntechnik weiterzuentwickeln. Diese Arbeiten sollen dazu beitragen, die Belastbarkeit bzw. Aussagesicherheit der Analysen menschlicher Zuverlässigkeit bei Nutzung rechner- und bildschirmbasierter Mensch-Maschine-Schnittstellen (AP 1), der Zuverlässigkeit digitaler Leittechnik (AP 2) und sicherheitskultureller sowie organisatorischer Einflussfaktoren beim Einsatz sicherheitsrelevanter Technologien (AP 3) abzusichern und weiter zu verbessern.

Im Fokus des Teilvorhabens AP 1 stand die Entwicklung einer Methode für die Analyse und Bewertung der Zuverlässigkeit, mit der das Personal sicherheitsrelevante Prozesse in modernen, mit computer-basierten Leitwarten mit digitalen Mensch-Maschine-Schnittstellen beobachtet und führt. Die Entwicklungsarbeiten waren insbesondere auf die Beanspruchung des Personals in den Bereichen des Erkennens, Verstehens, Denkens, Urteilens, Entscheidens, Planens und der zugehörigen Gedächtnisleistungen (kognitive Beanspruchung) konzentriert.

Im Teilvorhaben AP 2 wurde eine Methode zur Bewertung der Sicherheit- und Zuverlässigkeit digitaler Leittechnik entwickelt, die auf der Basis von PLD-Technologien (Programmable Logic Devices) aufgebaut ist.

Das Teilvorhaben AP 3 umfasst zwei Vorstudien zur Weiterentwicklung von Methoden zur Bewertung personell-organisatorischer Einflüsse:

- Gegenstand der ersten Vorstudie ist die Evaluierung von Methoden für die qualitative und quantitative Bewertung des Beitrags einer Sicherheitskultur zum sicheren Betrieb. Hierzu wurden Faktoren erfasst, die an der Steuerung menschlichen Handelns beteiligt sind. Mittels dieser Vorstudie soll gezeigt werden, inwieweit der Beitrag von Merkmalen der Sicherheitskultur in die Analyse und Bewertung menschlicher Zuverlässigkeit einbezogen und auch quantifiziert werden kann.
- Gegenstand der zweiten Vorstudie ist die Ermittlung organisatorischer Faktoren (also Strukturen und Prozesse der Organisation), welche die Auslösung und Beherrschung von Katastrophenereignissen beeinflussen. Ziel dieser Vorstudie war es, anhand ausgewählter Beispiele zu untersuchen, ob sich bei aufgetretenen Un-

fallereignissen technologieübergreifende, charakteristische organisatorische Einflussfaktoren identifizieren lassen, die einen Unfallablauf signifikant beeinflusst haben, und ob es Möglichkeiten zur Bewertung der Signifikanz solcher Einflussfaktoren gibt.

In AP 1 und AP 2 wurde zunächst der Stand von Wissenschaft und Technik hinsichtlich der Bewertungsmethoden für rechner- und bildschirmbasierter Mensch-Maschine-Schnittstellen und der technischen Eigenschaften der PLD basierten Leittechnik ermittelt. Anschließend wurde in AP 1 eine Methode für die quantitative Bewertung der Zuverlässigkeit schnittstellenspezifischer Aktivitäten in einer rechner- und bildschirmbasierten Warte und ihres Beitrages zur Zuverlässigkeit der Prozessführungsaufgaben entwickelt. Die Arbeitsergebnisse sind in den Kapiteln 3.1 und 4.1 des vorliegenden Berichts zusammengefasst.

Das Arbeitsergebnis im AP 2 ist die Entwicklung eines Ansatzes zur systematischen sicherheitstechnischen Bewertung PLD-basierter Leittechnik, der für die gesamte Bandbreite des Einsatzes von PLD-basierten leittechnischen Einrichtungen von einzelnen Komponenten bis hin zu ganzen leittechnischen Systemen eingesetzt werden kann. Der CAMIC-Ansatz (**C**yclic **A**nalytic **M**ethodology for **I**&**C**) ist auf dem bewährten PDCA-Zyklus (Plan-Do-Check-Act) aufgebaut und enthält alle erforderlichen Elemente des Bewertungsprozesses (u. a. Analyseschritte, Eingangsinformationen, Entscheidungskriterien) und wird durch Flussdiagramme unterstützt. Hierzu wurden die Analyse- und Bewertungsschritte der CAMIC-Methode mittels eines modellbasierten Ansatzes (u. a. Black-Box- und Grey-Box-Modelle einer PLD-basierten Antriebsteuerung) erprobt. Wesentliche Erkenntnisse aus der Entwicklung und Erprobung der CAMIC-Methode und Informationen zu der PLD-basierter Leittechnik sind in den Kapiteln 3.2 und 4.2 des vorliegenden Berichts dargestellt.

Im Rahmen der ersten Vorstudie (AP 3) wurden wichtige Erkenntnisse der Literaturstudie ausgewertet, dokumentiert und anschließend ein Konzept zur Vorgehensweise bei der quantitativen Bewertung einer Sicherheitskultur entwickelt.

Die zweite Vorstudie (AP 3) zur Bewertung der Auswirkungen organisatorischer Einflussfaktoren ermittelte, dass aus den zugänglichen Informationsquellen in ihrer Signifikanz bewertbare organisatorische Einflussfaktoren identifiziert werden konnten, die die Entstehung und den Verlauf von Katastrophen beeinflussen. Die gewonnenen Erkenntnisse legten es nahe, in einer weiterführenden Studie umfassend und vertieft sol-

che Einflussfaktoren zu ermitteln, zu charakterisieren und in Bezug auf ihre mögliche Sicherheitsrelevanz für den Betrieb kerntechnischer Anlagen zu diskutieren und zu bewerten. Ein Projekt für eine solche Studie ist bereits konzipiert, beantragt und bewilligt.

Die Ergebnisse der Vorstudien sind in den Kapiteln 3.3 und 4.3 des Berichts dokumentiert.

Abstract

The following report has been prepared on behalf of the German Federal Ministry for Economic Affairs and Energy (BMWi) in the frame of the project RS1525. The general objective of the project is to develop and/or to improve methodological approaches and tools for safety and reliability analysis of nuclear installations. The overall project was divided into three tasks:

- Task 1: "Development of a methodology for the analysis and evaluation of advanced human-machine interfaces". The methodology should be applied for the assessment of the reliability of the personnel's activities working in a computer-based control room with modern man-machine-interfaces. The work focused on an assessment methodology concerning demands on personnel in the areas of identification, understanding, thinking, judgment, decision making, planning and the associated contribution of memory (cognitive demands).

- Task 2: "Evaluation of the reliability of digital instrumentation and control system". Main objective of this task is development of a method to assess the reliability of digital instrumentation and control equipment, which is manufactured using PLD (Programmable Logic Devices) technologies.

- Task 3 comprises two preliminary studies:

  - The first study focused on the evaluation of methods for the qualitative and quantitative assessment of the contribution of a safety culture to safe operation of nuclear installations. Topics of this preliminary study are factors which belong or contribute to the psychological processes underlying human action. The study shall show how the aspects of safety culture can be included and also can be quantified in the analysis and assessment in human reliability analysis.

  - The second study focused on identification of organizational factors (i.e. structures and processes of the organization) which can initiate and/or can affect control of catastrophic events. The aim of this preliminary study is to identify such characteristic organizational factors on the basis of selected examples of accident events that have occurred in several technological areas.

At the beginning, the studies concerning the state of the art in the field of analysis and evaluation of modern digital human-machine interfaces (Task 1) and in the area of reliability analysis of PLD-based equipment of digital instrumentation and control systems

(Task 2) were performed. Subsequently, GRS experts have developed in the framework of Task 1 a method for the quantitative assessment of the reliability of interface-specific activities in computerized control rooms and their contribution to the reliability of the process management tasks. The work results of Task 1 are presented in chapters 3.1 and 4.1 of the report.

In the framework of Task 2 a systematic approach for safety and reliability assessment of digital I&C was developed on the basis of the proven generic PDCA methodology (Plan-Do-Check-Act). The CAMIC (**C**yclic **A**nalytic **M**ethodology for **I**&**C**) approach is focused on aspects of fault prevention and failure control during design, manufacturing and use of the I&C equipment. The CAMIC approach provides guidance for systematic evaluation of the safety and reliability aspects and defines the elements and the decision criteria for individual analysis steps. The CAMIC methodology was tested applying generic models of I&C equipment. The black-box and gray-box modelling were made for the fault conditions and afterwards their potential effects on the required functions were analyzed. The results of the study, a description of the CAMIC approach and test results are documented in chapters 3.2 and 4.2 of the report.

The first preliminary study of Task 3 comprises:

- Evaluation of findings concerning the qualitative and quantitative assessment of safety cultural factors,
- Development of a concept for a quantification of the contribution of safety culture to safety.

The second preliminary study of Task 3 provides evaluation and identification of organizational factors (i.e. structures and processes of the organization) which can initiate and/or affect control of catastrophic events on the basis of selected accidents.

The results of both studies are presented in chapters 3.3 and 4.3 of the report. Chapter 4 of the report comprises a summary and gives an outlook on future work.

Inhaltsverzeichnis

1 Zielsetzung

Für jede sicherheitsrelevante bzw. risikobehaftete Technologie gilt, dass ihre Sicherheit von der Zuverlässigkeit abhängt, mit der Mensch, Technik und Organisation ihre jeweilige Funktion beim Betrieb und bei der Beherrschung von Ereignissen erfüllen. Die Beurteilung des Einsatzes sicherheitsrelevanter Technologien (u. a. Kerntechnik, Bahn- und Verkehrstechnik, Luft- und Raumfahrttechnik) erfolgt generell auf der Basis von Sicherheitsanalysen. Die umfassenden deterministischen und probabilistischen Sicherheitsanalysen führen die Erkenntnisse der Sicherheitsforschung, Kenntnisse über die Auslegung und Betriebsweise, Betriebserfahrung und nutzbare Ergebnisse des allgemeinen wissenschaftlich-technischen Erkenntnisfortschrittes zu einer Gesamtbewertung des Sicherheitszustandes der untersuchten Anlage zusammen und schaffen damit belastbare Grundlagen für Entscheidungen über die Notwendigkeit und den Nutzen sicherheitstechnischer Verbesserungen.

Die technologischen Fortschritte und die neuen Erkenntnisse müssen kontinuierlich in der Sicherheitsforschung im Allgemeinen und in der Reaktorsicherheitsforschung im Besonderen berücksichtigt werden. Digitale Leittechnik kommt sowohl in der nichtnuklearen Industrie als auch teilweise in der Kerntechnik (u. a. Großbild- und Berührungsbildschirme in Prozessleitwarten, digitale Schutz-, Steuerungs- und Messeinrichtungen, rechnerbasierte Automatisierungssysteme) zum Einsatz. Derzeit fehlen anerkannte und praktikable Methoden im kerntechnischen Bereich, um die Zuverlässigkeit digitaler Leittechnik (insbesondere der Software) zu analysieren und zu bewerten.

Des Weiteren besteht ein dringender Bedarf an Methoden für die Analyse und Bewertung der Zuverlässigkeit, mit der das Personal Aufgaben der Prozessüberwachung und Prozessführung mit den Informations- und Bedieneinrichtungen erfüllt, die mit Hilfe moderner Computer- und Bildschirmtechnologien, z. B. in Form von Bildschirmwarten, realisiert sind. Nachfolgend werden solche Informations- und Bedieneinrichtungen generisch auch als „fortschrittliche Mensch-Maschine-Schnittstellen“ oder „rechnerbasierte Mensch-Maschine-Schnittstellen“ bezeichnet.

Zuverlässiges Handeln beim Einsatz moderner sicherheitsrelevanter Technologien hängt ferner wesentlich davon ab, dass das Personal sicherheitsbewusst und verantwortlich handelt. Die Gesamtheit an Merkmalen und Einstellungen in Unternehmen und von Personen wird, soweit sie für die Sicherheit wichtig ist, zusammenfassend als Sicherheitskultur bezeichnet. Das sicherheitstechnisch optimale Handeln hängt darüber

hinaus auch davon ab, inwieweit es durch die Strukturen und Prozesse der Unternehmensorganisation unterstützt wird.

Sicherheitskultur, organisatorische Aspekte des sicheren Betriebs und Sicherheitsaspekte bei der Einführung digitaler Leittechnik sowie rechner- und bildschirmbasierten Prozessüberwachung und Prozessbedienung sind seit Jahren Gegenstand umfangreicher Untersuchungen und Empfehlungen. Aus diesem Sachstand ergeben sich die Arbeitspakete (Teilvorhaben), mit denen die GRS beabsichtigt, weitere methodische Ansätze zu entwickeln bzw. Möglichkeiten aufzuzeigen, um die Lücken in den bereits bestehenden Methoden zu schließen.

Die GRS verfolgt mit diesem Vorhaben generell das Ziel, methodische Ansätze und Werkzeuge für Sicherheitsanalysen weiterzuentwickeln. Diese Arbeiten sollen dazu beitragen, die Belastbarkeit bzw. Aussagesicherheit der Analysen menschlicher Zuverlässigkeit bei Nutzung rechner- und bildschirmbasierter Mensch-Maschine-Schnittstellen, der Zuverlässigkeit digitaler Leittechnik und sicherheitskultureller sowie organisatorischer Einflussfaktoren beim Einsatz sicherheitsrelevanter Technologien abzusichern und weiter zu verbessern.

2 Wissenschaftliche und technische Aufgabenstellung

2.1 Analyse und Bewertung fortschrittlicher Mensch-Maschine-Schnittstelle

Mensch, Technik und Organisation bilden ein System, dessen Sicherheit und Zuverlässigkeit wesentlich auch von den Faktoren abhängt, die sich auf die zuverlässige Überwachung und Führung sicherheitsrelevanter, technischer Prozesse durch den Menschen auswirken. Zu diesen Faktoren gehören die Schnittstellen zwischen Mensch und Maschine, also die Informations- und Bedieneinrichtungen sowie den Informationen, die diese Einrichtungen dem Menschen z. B. in Form von Alarmen, Meldungen, Messwerten, Schalterstellungen darbieten.

Moderne digitale Computer- und Bildschirmtechnik bietet im Vergleich zu analoger Leittechnik und konventionellen Benutzungsoberflächen deutlich vielfältigere Möglichkeiten, Schnittstellen auszulegen und zu gestalten. Daher kommen weltweit auch in Kernkraftwerken und sonstigen kerntechnischen Anlagen computer- und bildschirmbasierte Benutzungsoberflächen zum Einsatz, um Aufgaben des Personals innerhalb und außerhalb der Warten zu unterstützen.

Für internationale und nationale Regelwerke sind Anforderungen an computer- und bildschirmbasierte Benutzungsoberflächen (Mensch-Maschine-Schnittstelle) bisher erarbeitet worden, die eine rein qualitative Beurteilung unterstützen. Derartige Beurteilungen lassen also offen, welchen quantitativen Beitrag eine Benutzungsoberfläche zu Sicherheit und Zuverlässigkeit leistet.

Weltweit sind unterschiedliche Analyse- und Bewertungsmethoden entwickelt worden, um den Beitrag computer- und bildschirmbasierter Benutzungsoberflächen zur sicheren und zuverlässigen Prozessüberwachung und Prozessführung in der probabilistischen Sicherheitsanalyse zu berücksichtigen. Derzeit liegt aber noch keine allgemein anerkannte Methode vor.

Aufgrund dieses Sachstands besteht ein erheblicher Bedarf an einer fachlich fundierten, wesentliche Einschränkungen anderer Ansätze vermeidenden und allgemein zugänglichen Methode für die Analyse und Bewertung der Zuverlässigkeit, mit der das Personal kerntechnischer Anlagen seine sicherheitstechnischen Aufgaben unter Einsatz von computer- und bildschirmbasierten Benutzungsoberflächen erfüllt.

Ziel der Arbeit in dem Vorhaben ist es, eine Methode für die Analyse und Bewertung der Zuverlässigkeit zu entwickeln und zu erproben, mit der das Personal in Kernkraftwerken innerhalb oder außerhalb der Leitwarte sicherheitsrelevante Prozesse über die rechnergestützten Benutzungsoberflächen überwacht und führt. Der Anwendungsbereich der Methode soll generisch sein und sich an die Gestaltung von Warten in den Kraftwerken orientieren, die mit Hilfe moderner Computer- und Bildschirmtechnologie und den zugehörigen Bedieneinrichtungen realisiert sind.

Die Entwicklungsarbeiten sollen sich auf die Möglichkeiten konzentrieren, die der Stand von Wissenschaft und Technik bietet, um kognitive Beanspruchungen durch die Arbeit mit einer Benutzungsoberfläche praxisgerecht zu erfassen, die Fehlerpotentiale zu analysieren und bei der Quantifizierung der Handlungszuverlässigkeit zu berücksichtigen. Dabei sind kognitive Beanspruchungen in den Bereichen des Erkennens, Verstehens, Denkens, Urteilens, Entscheidens, Planens und die zugehörigen Gedächtnisleistungen in dem Umfang einzubeziehen, der für die Interaktion mit einer modernen, rechner- und bildschirmbasierten Schnittstelle wichtig ist.

2.2 Sicherheitstechnische Bewertung digitaler leittechnischer Einrichtungen

Programmierbare und rechnerbasierte Leittechnik wird bereits seit Jahrzehnten zur Automatisierung von Prozessen in der Industrie (u. a. Maschinenbau, Chemieindustrie, Energieerzeugung und -verteilung, Automobil- und Luftfahrtindustrie) eingesetzt. Auch in der Kerntechnik werden programmierbare und rechnerbasierte leittechnische Einrichtungen bereits auf allen Ebenen der Signalverarbeitung der Prozessleittechnik eingesetzt, u. a.

- in der Anregeebene mit Messwerterfassung (z. B. Smart-Sensoren bzw. Messumformer, Baugruppen der Signalaufbereitung),
- in der Logik- bzw. Funktionsverarbeitungsebene (z. B. Baugruppen der Grenzwertüberwachung, Auswahllogik, logische Signalverknüpfungen),
- in der Steuerungsebene (z. B. Baugruppen der Einzelantriebssteuerung, der Funktionsgruppensteuerung und Vorrangsteuerung),
- in der Koppelebene (z. B. Schaltanlagen und deren elektrische Schutzeinrichtungen),

- Kommunikation zwischen Einrichtungen einer und/oder verschiedener Ebenen der betrieblichen und Sicherheitsleittechnik (z. B. Netzwerkbaugruppen).

Für einige Bereiche programmierbarer und rechnerbasierter Leittechnik wird zunehmend eine Technologie eingesetzt, die auf programmierbaren logischen Schaltungen (PLD – Programmable Logic Device) basiert. Die PLD-basierten Einrichtungen übernehmen, im Gegensatz zur rechnerbasierten Leittechnik, derzeit noch wenige komplexe Funktionen in der Prozessleittechnik und werden in der Regel in einem sicherheitsrelevanten Leittechniksystem dezentral eingesetzt. Anwendungsbeispiele sind die Umwandlung und Überwachung elektrischer Signale von Sensoren, die Antriebssteuerung und die Schnittstellen der Datenkommunikation. Diese dezentralen Einrichtungen können sowohl in ein übergeordnetes Leittechniksystem integriert werden als auch autark Leittechnik-Funktionen ausführen.

Grundsätzlich soll die erforderliche funktionale Sicherheit der Automatisierungstechnik durch die Erfüllung der Anforderungen aktueller Industriestandards (u. a. /DIN 06/, /DIN 07/, /DIN 13/, /DIN 81/) in Bezug auf die Anwendung von Maßnahmen zur Fehlervermeidung und zur Fehlerbeherrschung erreicht werden. Sofern PLD-basierte Einrichtungen für sicherheitsrelevante Funktionen der Automatisierungs- und Prozessleittechnik eingesetzt werden, muss die für den Einsatzzweck erforderliche Zuverlässigkeit im Rahmen von Zertifizierungs- bzw. Qualifizierungsverfahren (/KAT 13/, /DIN 11/) nachgewiesen werden.

Die Entwicklung von Methoden zur Bewertung der Zuverlässigkeit und der Sicherheit programmierbarer und rechnerbasierter leittechnischer Komponenten, insbesondere bei einem geplanten Einsatz in sicherheitstechnisch wichtiger Leittechnik, steht seit ihrer Einführung im Fokus nationaler und internationaler Forschungsaktivitäten. Die ersten Betriebserfahrungen (/NEA 15/, /NRC 10/) zeigen, dass die Funktionalität von PLD-basierten Geräten grundsätzlich durch eine komplexe softwarebasierte Auslegung der Hardware realisiert wird.

Des Weiteren hat sich gezeigt, dass die Bewertungsmethoden nicht mit der gleichen Geschwindigkeit entwickelt werden wie die Funktionalität der auf PLD-Technologie basierten Leittechnik fortschreitet. Die Notwendigkeit der Entwicklung von Methoden zur Zuverlässigkeitsbewertung bzw. der Verbesserung der Analysetechnik, insbesondere für die Bewertung der PLD-basierten Leittechnik, wurde auch international, u. a. von

IRSN /DIN 13/, /FAA 96/, /GAS 02/, /GAS 09/ und der U.S. NRC /ORN 07/ erkannt und in die Forschungsaktivitäten der USA zur Reaktorsicherheit (z. B. /NRC 10/) integriert.

Die Forschungsarbeiten der GRS im Rahmen des vom Bundesministerium für Wirtschaft und Energie (BMWi) geförderten Forschungs- und Entwicklungsvorhabens RS1525 sehen vor, methodische Ansätze zur Bewertung der Zuverlässigkeit der PLD-basierten Leittechnik zu entwickeln. Zu den zu betrachtenden Einrichtungen zählen u. a.:

- digitale Messeinrichtungen (z. B. elektronische Smart-Messumformer),
- digitale Signalübertragung, Kommunikationsnetzwerke (z. B. Netzwerk-Schnittstellen),
- digitale Steuerungs-, Schutz- und Überwachungseinrichtungen der elektrischen Energieversorgung (z. B. digitale Feldgeräte der Schaltanlagen: Schutzschaltgeräte und Sicherungssysteme),
- Steuerungen von Hebe- und Zerlegungseinrichtungen, Antriebsteuerung.

Die Zielsetzung dieses Vorhabens sieht vor, ein Konzept für die Analyse der Auswirkungen potentieller Fehlfunktionen, ausgehend von generischen Modellen PLD-basierter Einrichtungen, bereitzustellen. Hierzu soll die Anwendbarkeit der bereits bekannten Methoden der Zuverlässigkeitsanalyse der Leittechnik überprüft werden.

2.3 Methoden zu Bewertung personell-organisatorischer Einflüsse

2.3.1 Teilvorhaben „Vorstudie zu Methoden für die qualitative und quantitative Bewertung des Beitrags einer Sicherheitskultur zum sicheren Betrieb“

Die Sicherheitskultur besteht ganz allgemein aus Faktoren, die ein sorgsames, sicherheitsbewusstes Handeln des Personals unterstützen und dazu beitragen sollen, Fehler mit schädlichen Folgen für Mensch und Umwelt zu verhindern bzw. zu bewältigen (z. B. /IAE 91/). Sie trägt somit wesentlich zur sicheren Nutzung von Risikotechnologien bei. Dazu gehören neben kerntechnischen Anlagen auch chemische, petrochemische, gentechnische usw. Industrien sowie Einrichtungen in den Bereichen Straßen- und Schienenverkehr, Schiff-, Luft- und Raumfahrt, medizinische Behandlung oder die Handhabung moderner Waffensysteme. Darüber hinaus wird die sichere und zuverläs-

sige Aufgabenerfüllung in vielen Bereichen mit einer Schlüsselfunktion für Leben, Gesundheit und Sicherheit des Menschen auf die Sicherheitskultur zurückgeführt (/REA 99/, /STR 09/).

Dieser großen Bedeutung entsprechend gibt es zur Sicherheitskultur weltweit zahlreiche theoretische und empirische Untersuchungen, vielfältige Ansätze für die praktische Förderung und mannigfache Entwicklungen im Bereich internationaler und nationaler Regelwerke. Zu den theoretischen Untersuchungen gehören auch solche, die sich mit der Quantifizierung des Beitrags der Sicherheitskultur zu Sicherheit bzw. Risiken beschäftigen. Ansätze für die Quantifizierung sind wichtig, weil sie den Erkenntnisstand zu Wesen und Wirkung der Sicherheitskultur deutlich erweitern:

- Eine tragfähige Quantifizierung setzt als unabdingbaren ersten Schritt voraus, die Merkmale der Sicherheitskultur, ihre Wechselwirkungen mit anderen Faktoren, z. B. mit den sicherheitstechnischen Vorkehrungen in einem Unternehmen, um die Ursache-Wirkungs-Zusammenhänge zwischen Sicherheitskultur, Mensch, Technik, Organisation und Sicherheit möglichst genau zu klären bzw. zu modellieren. Ohne diesen Schritt führt eine Quantifizierung von Risiken, Fehlerwahrscheinlichkeiten usw. zu Ergebnissen, die aller Voraussicht nach nicht oder kaum nachvollziehbar, reproduzierbar und valide sind.

- Quantitative Bewertungen ermöglichen es, den Beitrag der Unternehmenskultur zur Sicherheit genauer zu fassen, als es mit qualitativen Beurteilungen möglich ist, die auf binäre oder abgestufte Urteile hinauslaufen. Man denke an qualitative Beurteilungen der Art: „die bestehende Unternehmenskultur ist der Sicherheit förderlich“ oder „ … trägt in hohem Maß zur Sicherheit der kerntechnischen Anlagen des Unternehmens bei“. Eine tragfähige quantitative Bewertung kann zudem mit den Beiträgen anderer Faktoren, wie z. B. den technischen und organisatorischen Vorkehrungen gegen sicherheitstechnisch bedeutsame Fehler, zu einer Gesamtbewertung verbunden werden, sofern die Beiträge der Sicherheitskultur und der übrigen Faktoren auf einer gemeinsamen Skala quantifiziert werden. Aufsichtsbehörden, Betreiber, Gutachter und weitere Interessenten würden mit einem fundierten und praktikablen Quantifizierungsansatz über ein Instrument verfügen, das Beurteilungen und Entscheidungen im Bereich der menschlichen, technischen, organisatorischen und sicherheitskulturellen Faktoren mit ihren Wechselwirkungen und ihren jeweiligen Beiträgen zur Sicherheit unterstützt.

Es gibt weltweit verschiedene Ansätze, die Sicherheitskultur einer Quantifizierung zuzuführen. Die vorliegende Untersuchung strebt dagegen einen Quantifizierungsansatz an, der wesentlich auf veröffentlichten Erkenntnissen und auf Daten aufbaut, die in der probabilistischen Sicherheitsanalyse entweder bereits genutzt werden oder in einem Entwicklungsprozess für die Quantifizierung des Beitrags der Sicherheitskultur zur Sicherheit aufbereitet werden können. Gemeint sind zum einen die Datenbestände für die Bewertung menschlicher Zuverlässigkeit in der probabilistischen Sicherheitsanalyse. Zum anderen ist an einen Rückgriff auf die empirischen Erkenntnisse gedacht, die in Projekten der jüngsten Vergangenheit bereits erschlossen worden sind, um Methoden für die qualitative Beurteilung der Sicherheitskultur und einen Musterprozess für ihre Förderung zu entwickeln (/GRS 15b/, /GRS 16/). Dieser Bestand an empirischen Erkenntnissen enthält auch umfassende statistische Informationen, die für den angestrebten Quantifizierungsansatz nutzbar, aber noch nicht ausgewertet worden sind.

Eine Weiterentwicklung der Modellierung der Sicherheitskultur und der Methodik für ihre Beurteilung, erlaubt den Beitrag der Sicherheitskultur zur Zuverlässigkeit sicherheitsbezogenen Handelns im System der menschlichen, technischen und organisatorischen Faktoren zuverlässigen Handelns genauer als bisher erfassen und beurteilen zu können.

Die vorliegende Vorstudie verfolgt das Ziel, einen Arbeitsplan für die Entwicklung einer Methode zu erstellen, mit der man die wesentlichen Merkmale der Sicherheitskultur in die Analyse und Bewertung menschlicher Zuverlässigkeit einbeziehen und quantifizieren kann. Die Methodenentwicklung selbst ist nicht Gegenstand dieser Untersuchung. Zu klären sind vielmehr die fachlichen Grundlagen, das prinzipielle Vorgehen und das Ergebnis der entsprechenden Entwicklungsarbeiten.

Zur Erreichung des Untersuchungszieles sind die drei folgenden Arbeitsschritte vorgesehen:

- nutzbare Erkenntnisse aus Wissenschaft und Technik zu ermitteln,
- ein geeignetes Vorgehen zur Weiterentwicklung der Methoden für die Analyse und die quantitative Bewertung menschlicher Zuverlässigkeit möglichst detailliert zu erarbeiten und

- das erwartete Ergebnis der Entwicklungsarbeiten zu beschreiben. Aus dieser Beschreibung hat insbesondere hervorzugehen, wie die Quantifizierung des Beitrags der Sicherheitskultur mit der weiterentwickelten Methode die Genauigkeit der Analyse und Bewertung der menschlichen Zuverlässigkeit erhöhen kann.

2.3.2 Teilvorhaben „Vorstudie zur Analyse der Auswirkungen organisatorischer Einflussfaktoren auf die Auslösung und Beherrschung von Katastrophenereignissen“

Die Auswertung der Ursachen für nukleare Unfälle und deren Abläufe zeigt, dass diese häufig durch aus sicherheitstechnischer Perspektive ungeeigneter Organisationsstrukturen und eine ebensolche Prozessorganisation negativ beeinflusst wurden. Gleiches gilt auch für große Unfallereignisse bei nicht nuklearen Technologien. Das betrifft so-wohl die Gründe, die zu einem Unfallereignis führten, als auch Ereignisse, die beim Versuch der Beherrschung eines Unfallablaufs auftraten. Dies können organisatorische Defizite sein, die die Entstehung eines Unfalls begünstigten, die Notfallmaßnahmen zur Beherrschung eines Unfalls negativ beeinflussten oder die Umweltauswirkungen infolge des Unfalls beeinflussten.

Ziel dieser Vorstudie ist es, anhand ausgewählter Beispiele zu untersuchen, ob sich bei in der Vergangenheit aufgetretenen Unfallereignissen technologieübergreifende, charakteristische organisatorische Einflussfaktoren identifizieren lassen, die einen Unfallablauf signifikant beeinflusst haben, und ob es Möglichkeiten zur Bewertung der Signifikanz solcher Einflussfaktoren gibt. Dabei soll auch geprüft werden, welche organisatorischen Einflussfaktoren ggf. positive Auswirkungen auf die Beherrschung des Unfallereignisses, auf Notfallmaßnahmen oder auf die Begrenzung von Umweltauswirkungen hatten.

Des Weiteren zielt die Vorstudie darauf ab, Merkmale organisatorischer Einflussfaktoren abzuleiten, durch welche die Zuverlässigkeit komplexer Prozesse und Notfallkonzepte beeinflusst wird und die grundsätzlich auch auf Kernkraftwerke übertragbar sind. Prozesse werden hier im Sinne der organisatorischen Prozesse eines Managementsystems verstanden.

Die Untersuchungen beziehen sich auf ausgewählte Beispiele, um die Tragfähigkeit dieses Untersuchungsansatzes zu prüfen und ihn den Erkenntnissen entsprechend ggf. weiterzuentwickeln.

3 Durchgeführte Arbeiten und Ergebnisse

3.1 Methode für die Analyse und Bewertung fortschrittlicher Mensch-Maschine-Schnittstelle (AP 1)

3.1.1 Recherchen zum Stand von Wissenschaft und Technik

Die Recherche des wissenschaftlich-technischen Erkenntnisstandes ist von den folgenden Fragestellungen ausgegangen, um den Überblick über diesen Stand auf die Aspekte zu konzentrieren, die für die Entwicklung der angestrebten Analyse- und Bewertungsmethode eine vorrangige Bedeutung haben:

- Welche Kriterien gibt es für die Automatisierung der Funktionen in einem System aus Mensch, Technik und Organisation und für die Aufteilung sicherheitstechnischer Aufgaben auf Personal und rechner- und bildschirmbasierte Schnittstellen?
- Nach welchen Kriterien ist die Arbeitsteilung zwischen Personen festgelegt, die mit Unterstützung rechner- und bildschirmbasierter Schnittstellen sicherheitstechnische Aufgaben im Team erfüllen?
- Welche Erkenntnisse gibt es zu den kognitiven (also Erkennen, Denken, Urteilen, Planen, Entscheiden, Gedächtnis etc. betreffenden) und den sonstigen Beanspruchungen des Personals bei sicherheitstechnischen Aufgaben, die das Personal mit Unterstützung rechner- und bildschirmbasierter Benutzungsoberflächen zu erfüllen hat?
- Von welchen Faktoren und von welchen Merkmalen rechner- und bildschirmbasierter Schnittstellen hängen Art und Höhe der Beanspruchung(en) ab?
- Wann liegen „günstige“ bzw. „ungünstige“ Beanspruchungen vor, die dadurch definiert sind, dass sie die Aufgabenerfüllung unterstützen bzw. erschweren oder verhindern?
- Wie entsteht Stress bei sicherheitstechnischen Aufgaben im Prozess der Beanspruchung und wie wirkt er?
- Welche Erkenntnisse gibt es zu den Zusammenhängen zwischen Beanspruchungen, Stress und Zuverlässigkeit der Erfüllung sicherheitstechnischer Aufgaben?

- Welche Reife haben die Erfassungs- und Beurteilungsmethoden für Beanspruchungen und Stress erreicht?

Die Ergebnisse der Recherchen zu den o. g. Fragen sind im Technischen Bericht GRS-A-3889 zusammengefasst. Dort sind zahlreiche empirische und analytische Methoden bewertet. Empirische Methoden zielen auf die Erhebung von Informationen zum subjektiven Erleben der Beanspruchung oder auf Maße für Verhalten und Leistung ab. Bei den analytischen Methoden geht es um die Modellierung der Belastungssituation und die Schätzung der mentalen Beanspruchungshöhe auf der Basis von Annahmen über die Kognition. Analytische Methoden berücksichtigen meist Faktoren wie Zeitdruck, Anforderungen an Informationsverarbeitungsprozesse und Stress. Bei allen Methoden sind vor einer möglichen praktischen Anwendung Aspekte wie v. a. die allgemeinen Gütekriterien psychologischer Tests (Objektivität, Reliabilität und Validität), der Erfassungsaufwand, apparative Voraussetzungen und denkbare, die Ergebnisse verfälschende Wechselwirkungen zwischen Messvorgang und Messgröße zu beurteilen.

Dennoch befinden sich einige Methoden noch in der Entwicklungs- und ersten Anwendungsphase. Die Analyse- und Bewertungsmethode des vorliegenden Vorhabens stützt sich deshalb im Wesentlichen auf ein fachlich fundiertes Expertenurteil, was die Ermittlung und Beurteilung der Beanspruchung betrifft.

3.1.2 Methodenentwicklung für die Aufgabenanalyse

Die im Vorhaben entwickelte Analysemethode soll eine systematische Ermittlung menschlicher Fehler unterstützen, die bei der Interaktion mit einer rechner- und bildschirmbasierten Schnittstelle auftreten können und nachteilige Auswirkungen auf die zuverlässige Bearbeitung sicherheitsbezogener Aufgaben der Prozessüberwachung und Prozessführung hätten, sofern diese Fehler nicht korrigiert oder nachteilige Folgen dieser Fehler für die Sicherheit nicht unterbunden werden.

Die Methodenbeschreibung nutzt die folgenden Begriffe mit den jeweils angegebenen Bedeutungen:

- „Benutzungsoberfläche“ und „Schnittstelle“ dienen als bedeutungsgleiche Begriffe.
- Eine Aufgabe der Prozessüberwachung und Prozessführung umfasst „Primäraufgaben“ und „Sekundäraufgaben“.

- „Primäraufgabe“ steht für die Arbeiten
  - Zustand bzw. Verhalten von Prozess und Anlage zu diagnostizieren,
  - Entscheidungen zu treffen, welches Vorgehen (wie z. B. schutzzielorientierte Prozeduren auf Grund der Diagnose) erforderlich ist,
  - Schritte des erforderlichen Vorgehens in Form der Kontrollen bestimmter Prozess- und Anlagenparameter bzw. bestimmter Eingriffe in Prozess und Anlage auszuführen.
- „Sekundäraufgabe“ bezeichnet innerhalb der Aufgabe alle Schritte, die erforderlich sind, um die Primäraufgabe(n) durchführen zu können. Sekundäraufgaben sind
  - die Interaktionen mit der Benutzungsoberfläche, die nachfolgend auch „schnittstellenspezifische Aktivitäten“ heißen,
  - Kommunikationen zwischen Mitgliedern des Teams der Operateure oder allgemein der Nutzer einer Schnittstelle,
  - Zugriff auf und Verwendung darüber hinausgehender Arbeitsmittel und Quellen. Man denke z. B. an Unterlagen in Papierform oder in elektronisch gespeicherten Dokumenten auf die kein Zugriff über die Schnittstelle möglich ist, und an Personen, wie z. B. Mitglieder eines Kraftwerkskrisenstabes, die in den vorgesehenen Situationen die Überwachung und Führung der Anlage koordinieren.

Die Unterscheidung zwischen Primär- und Sekundäraufgaben ist nach dem Stand von Wissenschaft und Technik üblich und sinnvoll, weil die Ausführung derselben Prozessführungsaufgabe sehr unterschiedlich gestaltet sein kann, was die Auslegung der Schnittstelle, die Zusammensetzung des Operateur-Teams und die Bereitstellung weiterer Arbeitsmittel und Quellen betrifft.

Hierzu gehören z. B. solche Aspekte wie die Zahl der Operateure, die Anzahl der Bildschirmarbeitsplätze in einer Warte, die Anzahl der Bildschirme pro Arbeitsplatz, die Ausstattung der Arbeitsplätze mit berührungsempfindlichen oder nicht berührungsempfindlichen Bildschirmen, die Anzahl der Bildschirmseiten, Art, Inhalt und Layout auf den Bildschirmen dargebotener Informationen. Je nach Auslegung der Schnittstelle kann sich der Zugriff auf die Informationen bzw. Informations- und Bedieneinrichtungen für die Primäraufgaben sehr unterschiedlich gestalten. Der Operateur muss sich z. B. durch mehr oder minder viele Bildschirmseiten „durchklicken“, bis er eine Anzeige mit

dem erforderlichen Prozessparameter bzw. eine Schaltfläche vor sich hat, mit der er den Schaltzustand eines Systems verändern kann.

Diese auslegungsabhängigen schnittstellenspezifischen Aktivitäten können mehr oder minder zeitaufwändig und fehlerträchtig sein. Sie können auch dazu beitragen, die Zuverlässigkeit der Primäraufgabe (Kontrolle eines Prozessparameters, Ausführung einer Schalthandlung) beeinträchtigen, aber auch erhöhen. Man denke etwa an die Möglichkeiten, in enger Nachbarschaft auf dem Bildschirm präsentierte Informationen oder Bedieneinrichtungen zu verwechseln bzw. Kontrollen zu programmieren, die vom Operateur die erforderliche Schalthandlung anfordern, wenn sie innerhalb einer festgelegten Zeitspanne nicht erfolgt, und die Eingabe des Operateurs auf Richtigkeit zu prüfen.

Die Entwicklung der Analysemethode besteht zu einem guten Teil aus der Übertragung der Schritte, die jede Aufgabenanalyse unabhängig davon durchlaufen muss, welche Mensch-Maschine-Schnittstellen die Erfüllung der zu analysierenden Aufgaben unterstützen. Diese übertragbaren Schritte sind im Einzelnen die Auswahl der Aufgaben, die in die Analyse eingehen, und die prinzipiellen Vorgehensweisen zur Beschaffung erforderlicher Informationen zur Modellierung des Handlungsablaufs bei der Aufgabenbearbeitung und zur Erstellung des sogenannten HRA-Baumes (HRA – Human Reliability Analysis), der die einzelnen Erfolgs- und Fehlerpfade bei der Aufgabenbearbeitung repräsentiert. Der Technische Bericht /GRS-A-3889/ enthält eine Anleitung, die durch den gesamten Analyseprozess führt und eine Beschreibung der Entwicklung der Analysemethode. Die Beschreibung umfasst wesentliche analyserelevante Aspekte, u. a. Festlegung von generischen Kriterien für die qualitative Beurteilung der Beanspruchung durch schnittstellenspezifische Aktivitäten und die Folgen der Beanspruchung, mit der die Primäraufgabe bearbeitet wird. Die Kriterien berücksichtigen auch die ergonomische Auslegung der Benutzeroberfläche. Es folgt eine Kurzdarstellung der entwickelten Methode.

Als fachlicher Ausgangspunkt des Entwicklungsprozesses dienen empirisch fundierte Erkenntnisse über die Beanspruchung des Menschen bei der Bearbeitung von Aufgaben, weil diese Beanspruchung den Schlüsselfaktor für Aufgabenerfüllung, Leistung und Zuverlässigkeit darstellt. Die Begriffe der psychischen Belastung und Beanspruchung sind in der DIN-Norm /DIN 87/ wie folgt festgelegt:

- „Psychische Belastung“ bezeichnet „die Gesamtheit der erfassbaren Einflüsse, die von außen auf den Menschen zukommen und auf ihn psychisch einwirken“. Äußere Einflüsse sind u. a. die Dauer der Tätigkeit, Umgebungsfaktoren, wie z. B. die Lichtverhältnisse, ferner Tätigkeitsanforderungen (wie etwa der aufgabenbedingte Zeitdruck) und sonstige Rahmenbedingungen des Handelns, zu denen auch Gefährdungen zählen.

- „Psychische Beanspruchung“ ist „die individuelle, zeitlich unmittelbare und nicht langfristige Auswirkung der psychischen Belastung im Menschen in Abhängigkeit von seinen individuellen Voraussetzungen und seinem Zustand“. Zu den inneren Voraussetzungen und dem Zustand des Menschen zählen z. B. Einstellungen, Fähigkeiten, die Gesundheit und die aktuelle Verfassung der betroffenen Person.

Mit Blick auf die Methodenentwicklung bedürfen diese Begriffsbestimmungen der Erläuterung und Ergänzung:

- Es entspricht der Alltagserfahrung und dem wissenschaftlichen Erkenntnisstand, dass im Allgemeinen eine Wechselwirkung zwischen der Beanspruchung und der Belastung besteht:

  - Es kommt zum einen darauf an, ob und wie die Person mit ihrem Wissen und ihrer Erfahrung die Art der Belastung und ihre Handlungsmöglichkeiten in der belastenden Situation erkennt und versteht. Zum anderen wertet der Mensch die aus seiner Sicht vorliegende Belastung und die von ihm erkannten Handlungsmöglichkeiten. Aus der Wertung können sich u.U. ganz unterschiedliche Verhaltensweisen und Auswirkungen auf die weitere Beanspruchung ergeben.

  - Auf schnittstellenspezifische Aktivitäten bezogen bedeutet dies konkret: Nutzer könnten z. B. erkennen, dass der Zugriff auf eine bestimmte Bildschirmseite „zu viel“ Zeit kostet, und ihre Beanspruchung durch die Belastung, die der zeitaufwendige Zugriff darstellt, mindern, indem sie Möglichkeiten nutzen, einen Schnellzugriff auf diese Seite einzurichten, oder indem sie auf leichter zugängliche Bildschirmseiten zugreifen, die aus ihrer Sicht die gleichen Informationen und Bedienoptionen bieten, wie die schwerer zugängliche Seite. Diese Wertung kann falsch sein und das weitere Vorgehen zur Erfüllung einer Aufgabe verfälschen.

- Von außen kommende Anforderungen und Aufträge sind Belastungen im Sinne der obigen Begriffsbestimmung /DIN 87/, weil und sofern sie auf den Menschen „psychisch einwirken“, seine Sinnesorgane also so weit stimulieren, dass er etwas wahrnimmt und dadurch einen Anstoß empfängt, sich mit der Belastung auseinanderzusetzen und die damit verbundene Beanspruchung auf sich zu nehmen. Wie jede Belastung interagieren Aufträge und Anforderungen von außen mit der Psyche. Die Beanspruchung hängt von dieser Interaktion ab.

Das empirisch fundierte „Auftrags-Auseinandersetzungs-Konzept“ erfasst die oben beschriebene Wechselwirkung bzw. aktive Auseinandersetzung des Menschen mit Aufträgen und Anforderungen /RIC 14/. Die Methodenentwicklung greift auf diesen Ansatz zurück, weil die Nutzung einer Schnittstelle Spielräume bieten kann, die eigene Beanspruchung aktiv zu verändern. Die Darstellung des Ansatzes in Abb. 3.1 ist im Vergleich zur Originalquelle /RIC 14/ stark vereinfacht und auf eine computer- und bildschirmbasierte Benutzungsoberfläche bezogen.

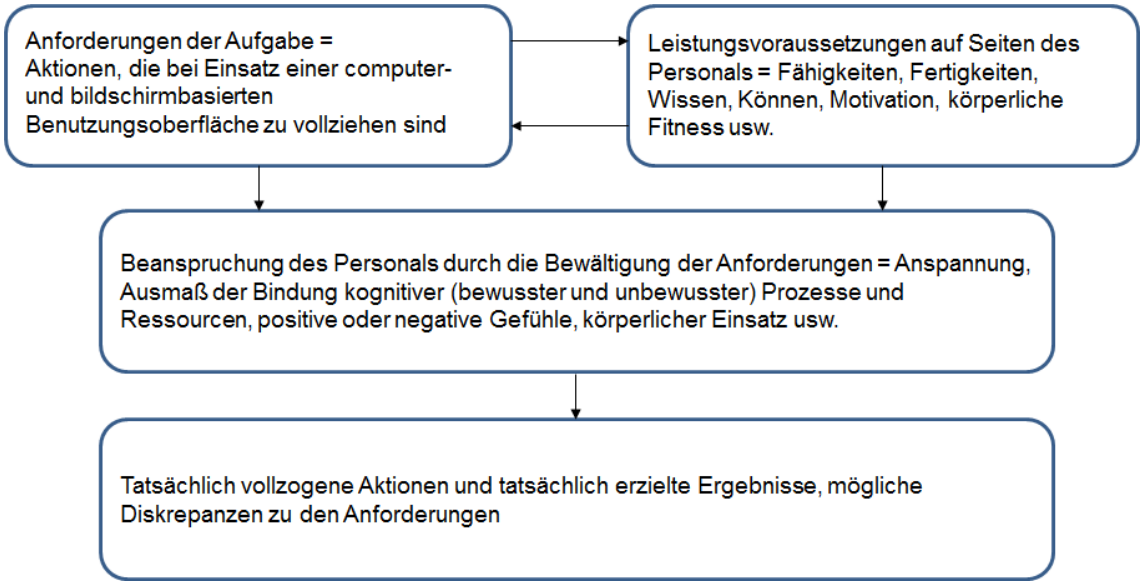

Abb. 3.1 Übersicht zum Auftrags-Auseinandersetzungskonzept

Die Beanspruchung resultiert aus der Wechselwirkung zwischen Anforderungen an den Menschen und Leistungsvoraussetzungen auf Seiten des Menschen. Art und Höhe der Beanspruchung hängen davon ab, inwieweit sich die Person mit ihren Leistungsvoraussetzungen einsetzt, um die Anforderungen zu erfüllen. Zu den Leistungsvoraussetzungen gehört auch die Bereitschaft oder Motivation, sich den Anforderungen zu stellen und sie zu erfüllen bzw. sich ihnen, soweit möglich, zu entziehen.

Man spricht von Überforderung, wenn die Anforderungen zu hoch sind, um von der Person mit ihren Leistungsvoraussetzungen erfüllt zu werden. Unterforderung liegt dagegen vor, wenn die Erfüllung der Anforderungen die Leistungsvoraussetzungen auf Seiten der Person bei weitem nicht in Anspruch nimmt. Über- und Unterforderung sind Fehlerquellen: Bei ersteren ist die Person physisch und (oder) psychisch, also kognitiv, emotional bzw. motivational außerstande, das geforderte Soll zu erbringen. Bei Unterforderungen muss man mit fehlerträchtigen Einbußen der Aufmerksamkeit, Wachheit, Bereitschaft zur Leistung usw. rechnen. Es sollte also möglichst ein Gleichgewicht zwischen Anforderungen und Leistungsvoraussetzungen bestehen. Aus diesen Erkenntnissen folgt ein Beurteilungskriterium:

- Anforderungen sollen zu Beanspruchungen führen, denen die Person aufgrund ihrer Leistungsvoraussetzungen gewachsen ist.
- Zumindest aber soll die Bewältigung der Anforderungen nicht mit Unter- oder Überforderungen einhergehen.

Erfüllen Anforderungen dieses Beurteilungskriterium, bieten sie eine gute Voraussetzung dafür, dass die Person die Anforderungen erfüllt und geforderte Leistungen erbringt. Inakzeptable Abweichungen von geforderten Leistungen bzw. Aktionen heißen auch „Fehler“ (human error) /SWA 83/. Somit haben Analyse und Beurteilung der Beanspruchung und der Beanspruchungsfolgen für die Analyse der Handlungszuverlässigkeit eine zentrale Bedeutung.

Stress entsteht, wenn die Überforderung zu einem Misserfolg führt oder aus der Sicht des Betroffenen zu einem Misserfolg führen wird, der wegen seiner negativen Folgen z. B. für Leben, Gesundheit, Selbstwertgefühl usw. emotional negativ besetzt ist und im Extremfall in Panik mit einer entsprechenden Desorganisation des Handelns umschlagen kann.

Abb. 3.1 führt unter den Anforderungen der Aufgabe an das Personal die Aktivitäten (mit ihren nicht eigens genannten ergonomischen Rahmenbedingungen) auf, die der Einsatz einer rechner- und bildschirmbasierten Benutzungsoberfläche dem Personal abverlangt. Diese Aktivitäten und Rahmenbedingungen sind zu ermitteln, um die zugehörigen Beanspruchungen genauer bestimmen und beurteilen zu können.

Schnittstellenspezifische Aktivitäten und zugehörige ergonomische Rahmenbedingungen

Die Systematik einschlägiger Aktivitäten und Rahmenbedingungen erfüllt mehrere wichtige Aufgaben:

- Die Zusammenstellung schnittstellenspezifischer Aktivitäten unterstützt die systematische und standardisierte Erfassung und Beschreibung
  - des geforderten Nutzerverhaltens, also der Anforderung, bestimmte Aktivitäten an bzw. mit der rechner- und bildschirmbasierten Schnittstelle zu vollziehen.
  - des tatsächlichen Nutzerverhaltens, also der beobachteten, tatsächlich vollzogenen Aktivitäten an bzw. mit dieser Schnittstelle.
  - der eventuellen Unterschiede zwischen dem tatsächlichen und dem geforderten Nutzerverhalten, die auch zur fehlerhaften Bearbeitung einer sicherheitstechnisch bedeutsamen Primäraufgabe führen oder beitragen können.
  - der Aktivitäten, die dazu führen oder beitragen, dass der Nutzer sicherheitstechnisch bedeutsame Fehler erkennt, behebt oder ihre Folgen für die Sicherheit entweder beherrscht oder abmildert.
- Die Zusammenstellung ergonomischer Rahmenbedingungen der schnittstellenspezifischen Aktivitäten
  - ermöglicht die gezielte Recherche des Fachwissens, wie diese Rahmenbedingungen so auszulegen sind, dass die Leistungsvoraussetzungen des Menschen möglichst optimal beansprucht, zumindest aber weder über- noch unterfordert werden.
  - unterstützt dadurch die Erklärung sicherheitstechnisch bedeutsamer Fehler durch eine Über- oder Unterforderung im Bereich der Sekundäraufgabe,
  - Fehler können aber auch dann auftreten, wenn die Beanspruchung optimal ist. Die Methode trägt dem dadurch Rechnung, dass Fehler als stochastische Ereignisse definiert werden (z. B. /SWA 83/).

Beide Zusammenstellungen unterstützen auch die Recherche einschlägiger Informationen über den Handlungsablauf bei der Aufgabenbearbeitung, indem man das Perso-

nal gezielt nach diesen Aktivitäten und Rahmenbedingungen befragt bzw. zu beiden Themenbereichen systematische Beobachtungen anstellt.

Die Ergebnisse der Recherchen zeigen, dass es noch keine einheitliche, allgemein anerkannte Zusammenstellung einschlägiger Aktivitäten und Rahmenbedingungen gibt. Die vorliegende Methodenentwicklung versucht, diese Beschränkungen wie folgt zu überwinden:

- Neben den Anforderungen der schnittstellenspezifischen Aktivitäten werden auch die Anforderungen der Primäraufgabe und der weiteren Sekundäraufgaben betrachtet. Die Methodenentwicklung strebt also eine Bestimmung schnittstellenspezifischer Aktivitäten unter Beachtung ihrer Zusammenhänge mit anderen Teilen der Gesamtaufgabe (Primäraufgabe, weitere Sekundäraufgaben) an.
- Es wurde ein systematisches Verfahren erstellt und genutzt, um die schnittstellenspezifischen Aktivitäten systematisch zu bestimmen. Es besteht darin, sich über die Herausforderungen klar zu werden, vor denen ein Operateur steht, wenn er den Auftrag zu einer bestimmten Aufgabe erhält und eine Benutzungsoberfläche vor sich hat, die ihm aktuell bestimmte Informationen bzw. Informations- und Bedieneinrichtungen präsentiert. Die Herausforderungen sind als Fragen formuliert. Ihre Beantwortung ermöglicht die Bestimmung der einzelnen schnittstellenspezifischen Aktivitäten, mit denen die Herausforderungen gemeistert werden können:
  - Was brauche ich an Informationen, Informations- und Bedieneinrichtungen, um die Aufgabe auftragsgemäß auszuführen?
  - Welche dieser Informationen, Informations- und Bedieneinrichtungen habe ich auf der Benutzungsoberfläche bereits vor Augen bzw. zur Hand?
  - Wo finde ich die benötigten Informationen, Informations- und Bedieneinrichtungen, die mir die Benutzungsoberfläche noch nicht präsentiert?
  - Wie muss ich mit den aktuell präsentierten Informationen, Informations- und Bedieneinrichtungen interagieren, um zu den noch nicht präsentierten Informationen, Informations- und Bedieneinrichtungen zu gelangen?
- Die Nutzung einer rechner- und bildschirmbasierten Benutzungsoberfläche stellt Anforderungen in den Bereichen der Kognition und der Aktion. Eine Zusammenstellung schnittstellenspezifischer Aktivitäten hat beide Bereiche zu berücksichtigen.

- Bei den kognitiven Aktivitäten stellt sich das Problem, dass sie sich der direkten Beobachtung entziehen. Die Methodenentwicklung stützt sich daher auf eine Einteilung dieser Aktivitäten, die einem erfahrungswissenschaftlich fundierten Modell entnommen und ohne kognitionswissenschaftliches Fachwissen verständlich ist. Man kann den Nutzern einer Schnittstelle also direkt konkrete Fragen zur Bewältigung kognitiver Anforderungen stellen, indem man dieser Einteilung einschlägige Fragen zugrunde legt. Als fachliche Grundlage dient das Modell der Tätigkeitsregulation nach Hacker /HAC 14/. In Anlehnung an dieses Modell unterscheidet der vorliegende Ansatz die kognitiven Aktivitäten der Aufmerksamkeit, Wahrnehmung, Diagnose, Zielformulierung, Planung des Vorgehens, Entscheidung über die Ausführung des Geplanten und das Behalten bzw. Erinnern als hauptsächlichen Gedächtnisleistungen, die mit den übrigen kognitiven Aktivitäten untrennbar verbunden sind.

- Was die schnittstellenspezifischen, kognitiven Aktivitäten betrifft, liegt der Schwerpunkt auf der Entdeckung, Erkennung und Einordnung der Informationen von der Benutzungsoberfläche, dem Erinnern des Wissens, das der Operateur durch Training und Berufstätigkeit erworben und mit den Informationen von der Benutzungsoberfläche verbindet sowie die zugehörigen Gedächtnisleistungen. Weitere kognitive Aktivitäten können ebenfalls beansprucht werden. Man denke z. B. an die Möglichkeit, dass der Operateur mangels geeigneter Benutzerführung darüber nachdenken muss, wo der Designer eine bestimmte Information auf der Benutzungsoberfläche „versteckt“ haben könnte.

- Aktionen im Bereich der schnittstellenspezifischen Aktivitäten sind v.a. die direkt beobachtbaren Eingaben bzw. Eingriffe der Operateure.

- Die Aktionen und kognitiven Aktivitäten sind ohne Bezug auf einen bestimmten Typ rechner- und bildschirmbasierter Benutzungsoberflächen zu formulieren, um auf Benutzungsoberflächen sehr unterschiedlicher Auslegung anwendbar zu sein.

- Aktionen und kognitive Aktivitäten sind als Anforderungen (Sollverhalten bzw. Sollleistungen) formuliert, um sie klar von den Beanspruchungen zu trennen, die sich aus der aktiven Auseinandersetzung mit diesen Anforderungen ergeben.

Es folgt die Zusammenstellung der Aktionen und Aktivitäten, die unter diesen methodologischen Vorgaben erarbeitet worden ist. Die ergonomischen Rahmenbedingungen werden im Anschluss an diese Zusammenstellung aufgeführt.

- In Bezug auf die Kognition bestehen die Anforderungen an die schnittstellenspezifischen Aktivitäten darin,

  - dargebotene Informationen, Informations- und Bedieneinrichtungen für die Primäraufgabe bzw. für die Interaktion mit der Benutzungsoberfläche (d. h. Zugriff auf Bildschirmseiten, Öffnen und Schließen von Fenstern auf dem Bildschirm usw.) wahrzunehmen (also nicht zu übersehen).

  - gesuchte Informationen, Informations- und Bedieneinrichtungen für die anstehende Primäraufgabe oder für die Interaktion mit der Benutzungsoberfläche auf der Benutzungsoberfläche korrekt zu orten (also nicht als Folge eines Versehens z. B. statt der geforderten Information eine benachbart dargebotene Information abzulesen).

  - dargebotene Informationen, Informations- und Bedieneinrichtungen für die Interaktion mit der Benutzungsoberfläche von denjenigen der Primäraufgabe zu unterscheiden (also z. B. eine Schaltfläche für den Zugriff auf Informationen und eine Schaltfläche für die Änderung des Schaltzustands einer Pumpe nicht miteinander zu verwechseln).

  - Plausibilität des für die Primäraufgabe oder Interaktion mit der Benutzungsoberfläche Dargebotenen festzustellen (also Unplausibles nicht mit Plausiblem zu verwechseln).

  - Relevanz bzw. Irrelevanz des Dargebotenen für die anstehende Primäraufgabe oder Interaktion mit der Benutzungsoberfläche festzustellen (also nicht Irrelevantes mit Relevantem zu verwechseln).

  - für die Primäraufgabe oder Interaktion mit der Benutzungsoberfläche Dargebotenes, das zu einem späteren Zeitpunkt zu nutzen ist, im Gedächtnis zu behalten (also nicht zu unterlassen, erforderliche Merkleistungen auszuführen).

  - für die Primäraufgabe oder Interaktion mit der Benutzungsoberfläche: Behaltenes bei Bedarf zu erinnern (Behaltenes also nicht zu vergessen oder zu vernachlässigen).

  - für die Primäraufgabe oder Interaktion mit der Benutzungsoberfläche: weitere, regel- bzw. wissensbasierte kognitive Aktivitäten (z. B. Diagnose von Ist-Zuständen, Auswahl erforderlicher Prozeduren, Entwicklung des erforderlichen

wissensbasierten Vorgehens, Klärung der Frage „wo findet man welche Information und wie greift man auf sie zu?“ usw.) auszuführen (statt diese Schritte auszulassen oder fehlerhaft auszuführen).

- für die Primäraufgabe oder Interaktion mit der Benutzungsoberfläche: über Ziele und Zusammenhänge der einzelnen Aktivitäten und Aktionen den Überblick zu behalten, nach Unterbrechungen (z. B. Wartezeiten, bis ein Füllstand erreicht ist) die zur korrekten Fortsetzung der unterbrochenen Aufgabe erforderlichen Aktivitäten (und Aktionen) auszuführen (statt sie zu unterlassen oder mit anderen zu verwechseln).

- bei unterschiedlichen parallel zu bearbeitenden Primäraufgaben: diese auseinanderzuhalten und ihre Bearbeitung zu koordinieren (statt Aufgabenteile zu unterlassen oder zu verwechseln).

- In Bezug auf die Aktionen der Primäraufgabe besteht die Anforderung, erforderliche Eingriffe in Anlage, Systeme und Prozesse auszuführen (sie also nicht zu unterlassen oder bei einer Schalthandlung aus Versehen den Zustand eines Systems zu verändern, dessen Bedieneinrichtung derjenigen benachbart ist, die eigentlich zu betätigen gewesen wäre). Zu Verwechslungsfehlern beim Ablesen von Informationen: siehe oben die Aktivität Gesuchtes korrekt zu orten.

- In Bezug auf die Aktionen der Interaktion mit der Benutzungsoberfläche bestehen die Anforderungen,

  - auf benötigte Informationen, Informations- und Bedieneinrichtungen zuzugreifen (statt den Zugriff zu unterlassen), dazu eventuelle erforderliche Wechsel des Arbeitsplatzes oder Verlagerungen der Aufmerksamkeit von einem Teil der Benutzungsoberfläche auf einen anderen zu vollziehen,

  - dargebotene nicht benötigte Informationen, Informations- und Bedieneinrichtungen soweit erforderlich und technisch möglich auszublenden (satt dies zu unterlassen und Bildschirme mit irrelevanten Ausgaben belegt zu lassen),

  - dargebotene Informationen, Informations- und Bedieneinrichtungen aufgabengerecht anzuordnen (soweit technisch möglich, z. B. durch Ziehen mit der Maus), statt dies zu unterlassen und mit weniger übersichtlichen und damit fehlerträchtigeren räumlichen Anordnungen zu arbeiten,

- die Form der Darstellung dargebotener Informationen, Informations- und Bedieneinrichtungen aufgabengerecht zu ändern, soweit dies technisch (z. B. durch Wahl zwischen digitaler und analoger Anzeige) möglich ist, statt dies zu unterlassen und mit suboptimalen, fehlerträchtigeren Darstellungsformen zu arbeiten,

- Dargebotenes für eine spätere Nutzung elektronisch zu speichern, soweit die Benutzungsoberfläche dafür die technischen Voraussetzungen bietet (statt dies zu unterlassen und sich z. B. auf sein Gedächtnis zu verlassen).

- In Bezug auf die weiteren Sekundäraufgaben der Kommunikation bzw. Nutzung weiterer Quellen enthält die vorliegende Zusammenstellungen die Anforderungen:
  - aufgabenbezogene Fragen zu stellen bzw. zu beantworten,
  - Anweisungen zu erteilen,
  - Rückmeldung über die Ausführung einer Anweisung zu geben,
  - erforderliche Aufzeichnungen anzulegen (z. B. Notizen über erhaltene Aufträge, Ausfüllen von Formularen in Papierform),
  - auf erforderliche Informationen zuzugreifen, deren Quelle weder die Benutzungsoberfläche noch die Kommunikation mit anderen Personen sind (z. B. Handbücher in Papierform),
  - diese sonstigen Quellen zu nutzen. Bei allen diesen Aktionen sind im Prinzip Unterlassungs- und Verwechslungsfehler möglich.

Leistung und Zuverlässigkeit der Ausführung hängen von den Rahmenbedingungen ab, unter denen das Personal die aufgeführten Aktivitäten und Aktionen zu vollziehen hat. Die vorliegende Zusammenstellung beschränkt sich auf die Gestaltungsaspekte der Schnittstelle. Anforderungen an Umgebungsfaktoren sind der Fachliteratur zu entnehmen (z. B. /SAL 12/).

Die Rahmenbedingungen sind so formuliert, dass sie in allgemeiner Form den Sollzustand zum Ausdruck bringen, der mit Blick auf die Beanspruchung des Personals anzustreben ist. Im Beurteilungsprozess dient dieser Sollzustand als Referenz.

- Informations- und Bedieneinrichtungen sollen für die Primäraufgabe und für die Interaktion mit der Schnittstelle selbst

- übersichtlich angeordnet und gruppiert sein,
- soweit möglich mit ihrer Anordnung und Gruppierung der Reihenfolge entsprechen, mit der sie im Arbeitsablauf zu nutzen sind,
- von der Arbeitsposition aus leicht erkennbar sein,
- eindeutig bezeichnet sein, wobei ein unmissverständlicher Bezug der Bezeichnung auf die gemeinte Einrichtung zu bestehen hat,
- ein Erscheinungsbild aufweisen, aus dem klar ihre Funktion hervorgeht (z. B. Zugehörigkeit zur Primäraufgabe oder zu den Einrichtungen für die Interaktion mit der Benutzungsoberfläche). Die Einrichtungen sollten also möglichst selbsterklärend sein. Man denke z. B. an eine schematische Darstellung, an der Dampferzeuger sofort als solcher erkennbar sind.

- Dargebotene Information sollen für die Primäraufgabe und für die Interaktion mit der Schnittstelle nach Möglichkeit so aufbereitet sein oder aufbereitet werden können, dass der Operateur sie bei der anstehenden Aufgabe direkt nutzen kann. Es sollte z. B. die Notwendigkeit entfallen, Messwerte umzurechnen. Das kann bedeuten, für interschiedliche Aufgaben verschiedene Arten der Aufbereitung derselben Informationen bereitzustellen oder zu ermöglichen und eventuellen Möglichkeiten der Verwechslungen dieser verschiedenen Arten vorzubeugen.
- In Bezug auf die Informationen, Informations- und Bedieneinrichtungen für schnittstellenspezifische Aktivitäten laufen die aufgeführten Anforderungen darauf hinaus, eine Benutzerführung vorzusehen, die den Nutzer effektiv dabei unterstützt, benötigte Informationen, Informations- und Bedieneinrichtungen für die anstehende Aufgabe zu finden.
- Die vorliegende Zusammenstellung umfasst auch Anforderungen, wie die Benutzungsoberfläche Aktionen im Bereich der Primäraufgabe und schnittstellenspezifische Aktionen unterstützen soll. Gefordert werden, soweit technisch realisierbar,
  - die Anzeige, dass eine Informations- und Bedieneinrichtung bzw. eine Automatik im bestimmungsgemäßen Zustand sind,
  - eine automatische Anforderung von Eingaben bzw. Eingriffen, wenn diese innerhalb einer definierten Zeitspanne unterbleiben,

- automatisch generierte Information bzw. Auswahllisten, welche Eingaben bzw. Eingriffe möglich und zulässig sind,
- automatische Aufforderung, Eingaben bzw. Eingriffe zu bestätigen, damit sie wirksam werden, und, soweit möglich, Information über die Konsequenzen der Bestätigung,
- mitlaufende automatische Kontrolle der Eingaben auf Richtigkeit, automatische Annullierung fehlerhafter Eingaben,
- Rücknahme fehlerhafter Eingaben zu ermöglichen,
- Schutz gegen unbeabsichtigte fehlerhafte Eingriffe bzw. Eingaben,
- Rückmeldung, dass eine Eingabe oder ein Eingriff zu automatischen Aktionen geführt haben, die noch laufen (z. B. dass ein Ventil automatisch zufährt),
- Rückmeldung, dass eine Eingabe oder ein Eingriff das vorgesehene Ergebnis erzielt haben (z. B. den Schaltzustand verändert haben) oder gescheitert sind,
- Übereinstimmung der Aktion, durch die Eingriff bzw. Eingabe realisiert werden, mit Nutzerwartungen.

- Der Zugriff auf benötigte Informationen, Informations- und Bedieneinrichtungen soll zügig erfolgen können, also weder zu viele noch zu zeitaufwändige schnittstellenspezifische Aktivitäten und Aktionen erfordern.

Mit dieser Zusammenstellung sind die Anforderungen insbesondere der schnittstellenspezifischen Aktivitäten und Aktionen erfasst und beschrieben. Als dritter Entwicklungsschritt ist ein qualitatives Kriterium für die Beurteilung zu erarbeiten.

Ein generisches beanspruchungsbezogenes Beurteilungskriterium

Mangels praktikabler Methoden muss der Schritt von den Anforderungen zur Beanspruchung über ein Expertenurteil auf Basis der erfragten und beobachteten Informationen über die Auseinandersetzung mit den Anforderungen erfolgen. Die Beanspruchung kann für die einzelnen Arbeitsschritte einer Aufgabe u. U. sehr unterschiedlich sein. Sie ist daher für die einzelnen Arbeitsschritte getrennt zu untersuchen, zu beurteilen und einzuschätzen. Die vorliegende Methode sieht dazu die beiden Stufen vor:

1. Erkenntnisse über die Anforderungen und die Auseinandersetzung des Personals mit diesen Anforderungen sind pro Arbeitsschritt zu einer Gesamtbeurteilung zusammenzuführen, wie gut die Schnittstelle die Erfüllung eines Arbeitsschritts innerhalb der betrachteten Aufgabe unterstützt.

2. Grundlage dieser Beurteilung die Beanspruchung einzuschätzen, die mit der Nutzung der Schnittstelle beim betrachteten Arbeitsschritt einhergeht.

Die zusammenfassende Beurteilung hebt auf die Unterstützung einer möglichst reibungslosen Bearbeitung der Aufgabe durch die Schnittstelle ab. Hierzu ist zu klären:

- Stellt die Benutzungsoberfläche für einen Arbeitsschritt der Primäraufgabe Informationen, Informations- und Bedieneinrichtungen bereit, die aufgabengerecht und ergonomisch möglichst optimal gestaltet sind und die das Personal zügig finden und auf der Benutzungsoberfläche ausgeben kann?

  - Aufgabengerecht sind Informationen, wenn sie nach Prüfung auf Richtigkeit direkt für die anstehende Aktion der Primäraufgabe (z. B. die Ausführung der anstehenden Anweisung einer Prozedur) nutzbar sind,

  - Aufgabengerecht sind Informations- und Bedieneinrichtungen, wenn sie auf Bildschirmseiten möglichst in der Reihenfolge angeordnet sind, in der sie zu nutzen sind.

  - Sind Zusammenhänge „auf einem Blick“ zu erfassen, sollen die einzelnen Elemente und Elementbeziehungen des Zusammenhangs in der Präsentation so gruppiert sein, dass die Beziehungen zwischen den präsentierten Anlagenteilen, Systemen, Komponenten bzw. system- und verfahrenstechnischen Zusammenhängen zutreffend veranschaulicht sind.

- Sind die Informationen, Informations- und Bedieneinrichtungen für die Primäraufgabe durch ihre ergonomische Gestaltung gut sichtbar, übersichtlich, leicht erkennbar, inhaltlich klar, konsistent und, wenn das Dargebotene Priorität besitzt, entsprechend auffällig (z. B. Alarme, Warnungen usw.)?

- Sind die Informationen, Informations- und Bedieneinrichtungen, die der Operateur für einen Schritt der Primäraufgabe benötigt, vom jeweils Dargebotenen aus erreichbar, indem das Personal einer vertretbar großen Zahl gut sichtbarer, übersichtlicher, leicht erkennbarer, inhaltlich klarer, konsistenter und lückenloser Hinweise auf der Benutzungsoberfläche folgt und die evtl. erforderlichen, eindeutig zugeordneten und leicht ausführbaren Eingaben (z. B. Klick für Seitenwechsel) vornimmt?

Liegt also insgesamt eine effiziente Nutzerführung zu benötigten Informationen, Informations- und Bedieneinrichtungen für die Primäraufgabe vor?

Sind diese Kriterien erfüllt, ist die erwartete Beanspruchung des Personals durch die Nutzung der Benutzungsoberfläche unerheblich. Im Idealfall ist es also problemlos, Aktivitäten und Aktionen auszuführen, die von der Schnittstelle vorgesehen also schnittstellenspezifisch sind, um auf benötigte Informationen zuzugreifen, diese Informationen zu verstehen und erforderliche Eingriffe bzw. Eingaben vorzunehmen. Das Personal „hat den Kopf frei“ für Zustand bzw. Verhalten von Anlage, Systemen, Komponenten und Prozessen, für das Vorgehen zur Erhaltung bzw. Erreichung eines sicheren Zustands der Anlage usw.

Abweichungen von den Kriterien erhöhen die Beanspruchung des Personals durch die Nutzung der Benutzungsoberfläche. Das Personal ist mehr oder minder oft, lange und (oder) intensiv damit beschäftigt, Unzulänglichkeiten der Benutzungsoberfläche zu meistern, und ist entsprechend stark von Anlage, Systemen, Prozessen, usw. „abgelenkt“ (z. B. durch zeitraubende Überlegungen, auf welchen Bildschirmseiten benötigte Informationen usw. zu finden sind, oder starke Konzentration auf die Bewegung zur exakten Positionierung der Maus auf der erforderlichen, zu kleinen Schaltfläche usw.).

Evaluierung der Möglichkeit einer Ratingskala für Beanspruchungen

Die Beanspruchung durch die Nutzung einer Schnittstelle kann gering, sie kann aber auch erheblich sein, wenn der Nutzer einen erheblichen Teil seiner Zeit und seines Denkens aufwenden muss, um zu erkennen, wo auf der Benutzungsoberfläche benötigte Informationen, Informations- und Bedieneinrichtungen zu finden sind und wie er auf sie zugreifen kann. In solchen Fällen wird die Benutzungsoberfläche zum Problem, das die Bearbeitung der Primäraufgabe zumindest hinauszögert oder Anlass gibt, mit suboptimalen Informationen zu arbeiten oder Eingriffe mit anderen als den vorgesehenen Bedieneinrichtungen vorzunehmen, was sich nachteilig auf die Zuverlässigkeit der Primäraufgabenerfüllung auswirken kann. Es liegt nahe, dass

- von einer kausalen Beziehung zwischen nutzerunfreundlicher Gestaltung, Beanspruchung, Fehlerpotential und Einbußen bei der zuverlässigen Aufgabenerfüllung auszugehen ist,
- dieser Zusammenhang mit einer Rating-Skala erfasst wird und die Erfassung und Beurteilung der Beanspruchung und des daraus folgenden Fehlerpotentials unter-

stützt. Die Skala hätte zwischen den Extremen einer minimalen und einer maximalen Beanspruchung durch die schnittstellenspezifischen Aktivitäten weitere, dazwischenliegende Stufen aufzuweisen.

Dennoch wurde dieser Ansatz im Zuge der Entwicklungsarbeiten nicht weiter verfolgt, weil die monotone Beziehung zwischen wachsender Beanspruchung und erhöhter Fehleranfälligkeit des Handelns nicht immer erfüllt ist. Wenn der Anwender eine nutzerunfreundliche Schnittstelle nutzt, wird er Routinen entwickeln, um die Nutzungsprobleme zu überwinden. Er könnte sich also angewöhnen, leicht zugängliche Informationen, Informations- und Bedieneinrichtungen zu nutzen, statt der objektiv oder zumindest aus seiner Sicht schwerer zugänglichen. Das Ergebnis könnte also eine minimale Beanspruchung, aber eine hohes Fehlerpotential des Handelns sein, wenn die tatsächlich genutzten Informationen, Informations- und Bedieneinrichtungen störanfälliger und deshalb für die anstehende Aufgabe einer Störfallbeherrschung ungeeignet sind.

Die Methode sieht deshalb eine auf Expertenurteil basierende Beurteilung der Beanspruchung durch schnittstellenspezifische Aktivitäten vor. Diese Beanspruchung ist dem (im oben vorgestellten Beurteilungskriterium entsprechend), im Idealfall minimal. Bei Abweichungen von diesem Idealfall ist zu analysieren und zu beurteilen, welche Fehler daraus für die Primäraufgabe resultieren können.

3.1.3 Überprüfung der Analyse- und Bewertungsmethode

Gemäß Zielsetzung des Vorhabens sollte die Methode hinsichtlich Anwendbarkeit erprobt werden. Hierzu wurden Experten des „Halden Reactor Projects (HRP)“ um eine Bewertung gebeten, inwieweit die Methode einen praktikablen Analyse- und Bewertungsansatz bildet. Die Bewertungsgrundlagen sollen die Erkenntnisse aus den empirischen Studien des HRP zu Operateur-Tätigkeiten in der Warte und zur Unterstützung dieser Handlungen mit rechner- und bildschirmbasierten Schnittstellen bilden. Des Weiteren wurden die HRP-Experten dazu eingeladen, ggf. Verbesserungsvorschläge zu formulieren, die für Weiterentwicklungen der Methode dokumentiert werden.

Die Rückmeldung des HRP /HRP 17/ bringt zum einen das Gesamturteil zum Ausdruck, dass die Methode für den avisierten Anwendungszweck gelungen ist. Die Methodenbeschreibung bietet einem Anwender eine klare und effiziente Anleitung. Zum

anderen umfasst die Rückmeldung wichtige, konstruktive Hinweise, Anregungen und Empfehlungen, u. a.

- Die Dokumentation der Methode sollte eine kurze Beschreibung der Voraussetzungen (Wissen, Erfahrung) des Methodenanwenders enthalten. Zu dieser Beschreibung sollten auch Referenzen auf Quellen gehören, mit denen sich der Anwender bei Bedarf das notwendige Grundlagenwissen aneignen kann.
- In der Dokumentation sollten Überblicksdiagramme die Übersicht zu den Fehlermöglichkeiten erleichtern, die mit der Methode bewertbar sind. Hierzu wäre auch ein Anhang mit einem kompletten Anwendungsbeispiel sinnvoll.
- Weitere Empfehlungen und Anregungen beziehen sich darauf, Ergänzungen einzelner Fehlerbeschreibungen, Änderungen von Formulierungen und die Klärung von Begriffen vorzunehmen, die ohne einen fachwissenschaftlichen Hintergrund auf dem Gebiet der Arbeitspsychologie Verständnisschwierigkeiten erzeugen können /HRP 17/.

Diese Hinweise, Anregungen und Empfehlungen werden in einer Weiterentwicklung der Methode im Detail berücksichtigt.

3.2 Zuverlässigkeitsbewertung digitaler leittechnischer Einrichtungen (AP 2)

3.2.1 Sachstand zu PLD-basierten Einrichtungen

Der Ursprung der programmierbaren logischen Schaltungen (PLD - Programmable Logic Device) beginnt in den 60-er Jahren mit Herstellung und Einsatz von integrierten Schaltkreisen (IC - Integrated Circuit) in der Elektronikindustrie. Unter ICs versteht man allgemein Schaltungen aus Halbleiterbauelementen (hauptsächlich Transistoren) inklusive ihrer Verdrahtung auf einem Substrat. Die Komplexität solcher Schaltungen nahm rasch zu und bereits einige Jahrzehnte später wurden Schaltungen mit Transistordichten von einigen Tausend Bauelementen auf einem Chip realisiert. Dieser Trend blieb im Wesentlichen erhalten, so dass heutzutage Mikroprozessoren mit 10 Milliarden Transistoren pro Chip und PLDs mit 20 Milliarden Transistoren pro Chip erhältlich sind.

ICs werden von verschiedenen Herstellern (z. B. Unterhaltungselektronik, Netzwerkkommunikation, Automobil- und Flugzeugindustrie, Prozessleittechnik) für ihre Zwecke

entwickelt, welche dann von Halbleiterherstellern produziert werden. Solche Schaltungen (u. a. Bausteine einer Baugruppe), die zumeist auf ganz bestimmte Anwendungen zugeschnitten sind, bezeichnet man als ASICs (Application Specific Integrated Circuit). Die Entwicklung der ASIC-Schaltungen ist sehr aufwendig und daher mit hohen Kosten verbunden, so dass sie in der Regel nur durch entsprechend hohe Stückzahlen rentabel sind. Aus diesem Grund wurden programmierbare Logikschaltungen zur Realisierung von digitalen Funktionen entwickelt, um eine wiederholbare Programmierbarkeit der Schaltung zu ermöglichen. Während ein einfacher ASIC nach der Herstellung nicht mehr verändert werden kann, bietet ein PLD daher gerade in der Entwicklungsphase eines ICs sehr große Vorteile. In der Anfangszeit waren PLDs wenig komplex, aber in den letzten Jahren haben sich speziell CPLD- und FPGA-Bausteine immer weiter entwickelt, so dass sie heutzutage für viele industrielle Anwendungen eine erforderliche Leistungsfähigkeit aufweisen. Es existiert bereits eine große Bandbreite an hochintegrierten Schaltkreisen, die sich anhand ihrer Komplexität, ihrer Größe, ihrer Leistungsfähigkeit und ihrer Flexibilität im Hinblick auf Änderungen der Logik der Signalverarbeitung unterscheidet.

Aufgrund der immensen Entwicklungsgeschwindigkeit der Technologie bestehen zwischen den komplexeren auf dem Markt verfügbaren ICs im Hinblick auf ihre Anwendbarkeit teilweise nur noch geringe Unterschiede. Dies führt dazu, dass diese ICs in der Literatur teilweise synonym behandelt werden und auch eine Gruppierung der verschiedenen Komponenten je nach Betrachtungsweise unterschiedlich ausfällt. In Abb. 3.2 sind die verschiedenen ICs entsprechend ihrer Komplexität und ihrer Unterschiede in der Konfigurierung so dargestellt, wie Hersteller sie vielfach einordnen.

Man unterscheidet hierbei zunächst zwischen ICs, welche bei der Herstellung programmiert und dann nicht mehr verändert werden können („Full Custom Design“) und solchen, die nach der Herstellung vom Anwender programmiert werden können („Semi Custom Design“). In Prozessleittechnik, Steuerung und elektrischen Schutzeinrichtungen der Kraftwerke werden bereits die ASIC, FPGA und CPLD basierten Baugruppen eingesetzt.

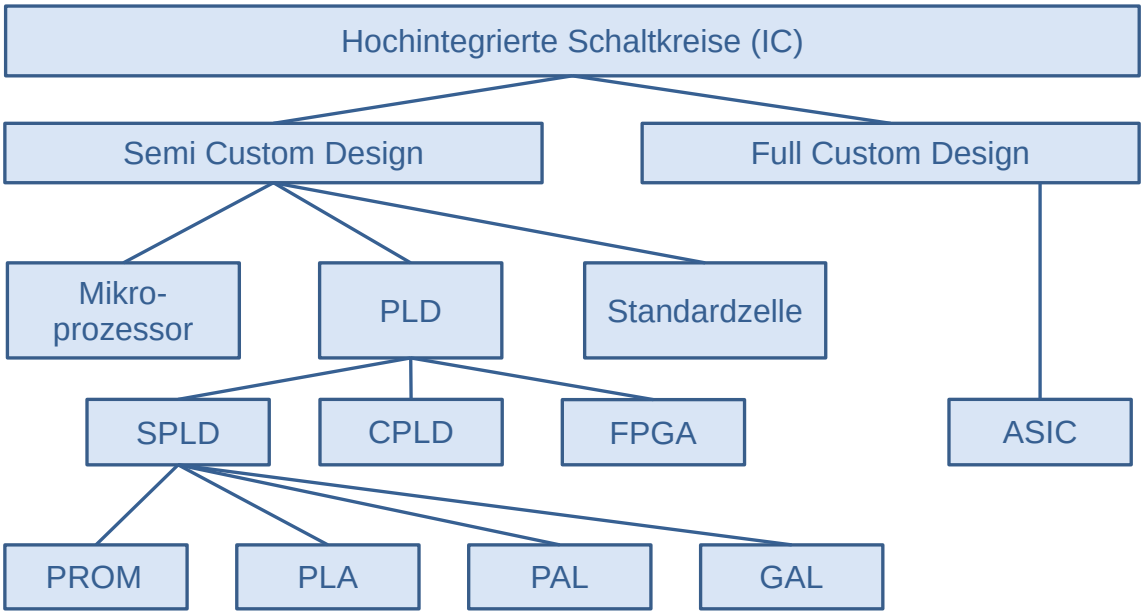

Abb. 3.2 Unterscheidung von ICs hinsichtlich ihrer Herstellungs-Technologien

Die Auslegung (Design) einer komplexen IC-Schaltung kann anhand der verschiedenen Abstraktionsebenen eines Y-Diagramms (Abb. 3.3) dargestellt werden. Hier zeigen die Radiuslinien die drei möglichen Darstellungsformen eines IC-Designs: Struktur, Verhalten und Geometrie bzw. Implementierung. Die konzentrischen Kreise zeigen die verschiedenen Abstraktionsebenen eines Designs. Je näher eine Abstraktionsebene zum Zentrum liegt, desto detaillierter ist die Beschreibung des Designs auf dieser Ebene /KES 13/.

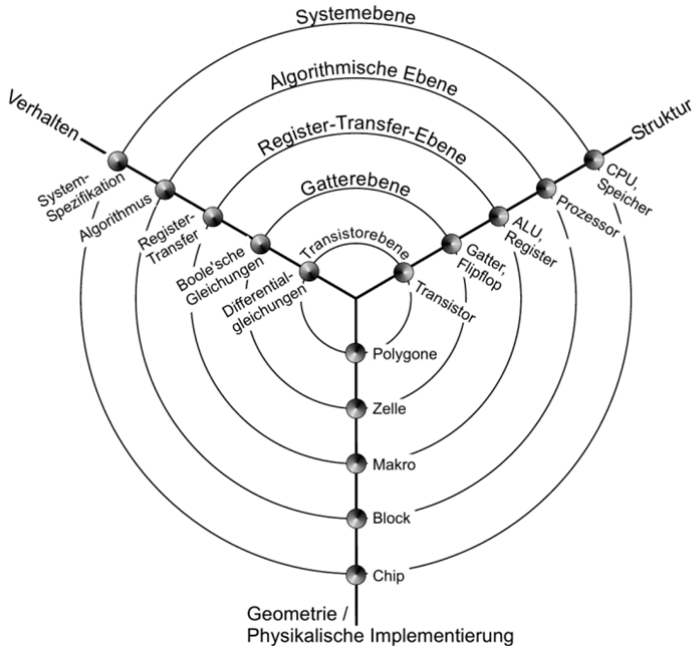

Abb. 3.3 Y-Diagramm zur Beschreibung der Vorgehensweise beim Entwurf einer integrierten Digitalschaltung /KES 13/

Programmierung von PLD: Unterschiede zwischen Hardwarebeschreibungssprachen und Software

Unter der Programmierung (wird auch als Konfiguration bezeichnet) von PLDs versteht man nicht die Vorgabe zeitlicher Abläufe, wie das bei der Programmierung von Software oder Steuerungen der mikroprozessor-basierten Baugruppe der Fall ist. Vielmehr werden Schaltungsstrukturen mittels Hardwarebeschreibungssprachen (HDL - Hardware Description Language) oder in Form von Schaltplänen erstellt und anschließend diese Daten als Konfiguration in den PLD übertragen. Auf diese Weise werden die Verschaltung der vorgegebenen Elemente und die Funktionsweise einzelner Blöcke festgelegt.

Folgende Unterschiede bestehen darüber hinaus zwischen Produktentwicklungsprozessen mit HDLs und Software /IAE 16/:

- Software wird in einer High-Level-Sprache (Source-Code) geschrieben, kompiliert und dann zur Erzeugung binären Codes fertiggestellt, der typisch für Mikroprozessoren ist, wo er sequentiell ausgeführt wird,
- HDL ist ebenfalls eine High-Level-Sprache. Statt jedoch einen binären Code zu erzeugen, der sequentiell abgearbeitet wird, wird die Beschreibung durch Syn-

these und Routing-Prozesse übersetzt in einen PLD-spezifischen Bitstream, durch den der Chip über physikalisch verbundene Logikelemente entsprechend der vorgesehenen Anwendung konfiguriert wird. Diese Konfiguration ergibt eine parallele Ausführung aller logisch unabhängigen Operationen, im Gegensatz zu den typischerweise seriellen Prozessen in Mikroprozessor-basierten Plattformen.

Üblicherweise wird zu Beginn einer Entwicklung eines PLD-Bausteins (u. a. ASIC, FPGA) eine Spezifikation erstellt. Diese ist die wesentliche Schnittstelle von Entwickler und Kunde und beschreibt die Eigenschaften und Funktionen, die die Schaltung erfüllen soll.

Zunächst wird ein Modell der Schaltung auf algorithmischer oder Systemebene entwickelt, welches dann durch eine funktionale Simulation auf seine Korrektheit überprüft wird. Dieses Modell wird mittels einer Hardwarebeschreibungssprache umgesetzt und kann wiederum simuliert werden. Üblicherweise wird dieses Ergebnis mit dem Ergebnis der Simulation auf System- oder algorithmischer Ebene verglichen, um sicherzustellen, dass beide Simulationen die gleichen Funktionen ausführen. Die Logiksynthese generiert ein Gattermodell. Das Gattermodell wird dann mit weiteren Werkzeugen mittels einer Layout-Synthese (auch als „Place and Route“ bezeichnet) in eine physikalische Realisierung umgesetzt. Nach der physikalischen Realisierung (Chip-Herstellung) kann die implementierte Schaltung am realen PLD (Hardware) erprobt werden.

Bei der Entwicklung einer ASIC- oder FPGA-Hardware sind Hardwarebeschreibungssprachen ein wichtiges Werkzeug. Den in Europa vorherrschenden industriellen Standard stellt hierbei die Hardwarebeschreibungssprache VHDL[1] dar, die für die Beschreibung von Schaltungen und Systemen und für die Simulation dieser Beschreibungen vorgesehen ist. VHDL wurde Anfang der 80er Jahre in den USA entwickelt und standardisiert, die derzeit aktuellste Version ist IEEE Standard 1076-2008 /IEE 08/.

Eine ebenfalls häufig eingesetzte Hardwarebeschreibungssprache ist Verilog[2]. Verilog wurde von der Firma Gateway Design Automation entwickelt. Verilog wurde 1995 als

---

1 VHDL: VHSIC Hardware Description Language, wobei VHSIC für “Very High Speed Integrated Circuit” steht.

2 Verilog: Verifying Logic.

IEEE 1364-1995 standardisiert, welcher 2001 als IEEE 1364-2001 /IEE 01/ aktualisiert wurde. /KES 13/, /SUT 01/

Bewertungsmethoden für PLD-basierte leittechnische Einrichtungen

Im Rahmen dieses Vorhabens wurden Recherchen zu Bewertungsmethoden sicherheitstechnischer Aspekte von PLD-basierter Leittechnik (PLD-LTE) durchgeführt. Eine Kurzübersicht der Merkmale ist in Tab. 3.1 für die Verfahren aufgeführt, die bereits für die Analyse von Leittechniksystemen /DIN 05/ eingesetzt wurden.

Tab. 3.1 Merkmale von Zuverlässigkeitsanalyseverfahren

	Geeignet für komplexe Systeme	Geeignet für neuartige Systemauslegung	Deduktiv (D), Induktiv (I)	Akzeptanz und Allgemeingültigkeit	Verfügbarkeit von Werkzeugen
Fehlzustandsbaumanalyse / Fault Tree Analysis - FTA	Ja	Ja	D	Hoch	Hoch
Ereignisbaumanalyse / Event Tree Analysis - ETA	Nein	Nein	I	Mittel	Mittel
Fehlzustandsart- und auswirkungsanalyse / Failure Mode and Effect Analysis - FMEA	Nein	Nein	I	Hoch	Hoch
Zuverlässigkeitsblockdiagramm	Nein	Nein	D	Mittel	Mittel
Markov-Analyse	Ja	Ja	D	Mittel	Mittel
Petrinetze	Ja	Ja	D	Niedrig	Niedrig
Monte-Carlo-Simulation	Ja	Ja		Modellabh.	Niedrig
Vorhersage der Ausfallrate	Nein	Ja	I	Hoch	Hoch
Prognose, Auffinden der Ursache, Abschätzen der Auswirkungen - PAAG / Hazard and Operability - HAZOP	Ja	Ja	I	Mittel	Mittel

Weitere Informationen zu den Bewertungsmethoden sind im Technischen Bericht /GRS-A-3890/ dokumentiert.

3.2.2 Bewertungsansatz für PLD-basierte leittechnische Einrichtungen

Im Rahmen des Vorhabens wurde ein Bewertungsansatz für den Einsatz von PLD-basierten leittechnischen Einrichtungen (im Weiteren als PLD-LTE bezeichnet: u. a.

Baugruppen und Geräte der Leittechnik) in Kernkraftwerken entwickelt. Er umfasst Analysen der verschiedenen Typen von PLD-LTE und die Untersuchung der Auswirkungen von möglichen Fehlzuständen dieser Einrichtungen auf Leittechnik-Systeme und leittechnische Funktionen ebenso wie die Untersuchung hinsichtlich der Vermeidung von Fehlzustandsauswirkungen. Der entwickelte Bewertungsansatz umfasst die gesamte Signalverarbeitungskette von der Signalerfassung bis zur Steuerung einer verfahrenstechnischen Komponente.

Die Vorgehensweise des entwickelten Bewertungsansatzes wird als CAMIC-Methode (Cyclic Analytic Methodology for Instrumentation and Control) bezeichnet und im Bericht /GRS-A-3890/ ausführlich beschrieben. Es folgt eine Kurzdarstellung der Methode.

Kurzbeschreibung der CAMIC-Methode

Die PLD-basierten Einrichtungen können in der Leittechnik von Kernkraftwerken vielfach und an verschiedenen Positionen in der Signalverarbeitung eines Leittechniksystems (u. a. Messwerterfassung und -verarbeitung, Daten- und Signalübertragung, Antriebssteuerung) eingesetzt werden. Daher ist es erforderlich, einen Bewertungsansatz zu verfolgen, der flexibel für unterschiedliche Zielstellungen (u. a. Bewertung des Defense-in-Depth-Konzepts, Bewertung des Einzelfehler-Ausfalls, Bewertung des GVA-Potentials, Entwicklung einer Modernisierungsstrategie, Identifizierung von Verbesserungsmöglichkeiten) eingesetzt werden kann.

Im Zusammenhang mit der Bewertung kommt grundsätzlich eine Vielzahl von Fragestellungen in Betracht, für deren Beantwortung unterschiedliche Bewertungsmethoden notwendig sind:

- Welche Fehlzustandsarten der Einrichtung sind möglich und welche Auswirkungen (z. B. auf das Leittechnik-System, in dem die PLD-LTE eingesetzt ist) ergeben sich daraus?
- Wie hoch ist die Wahrscheinlichkeit, dass es zu bestimmten Fehlfunktionen der Einrichtung kommt?
- Sind systematische Ausfälle (u. a. GVA der zu bewertenden PLD-LTE) im entsprechenden Leittechnik-System zu erwarten?

Neben den o. g. Fragen hinsichtlich der Ausfallarten und der Auswirkungen einer zu bewertenden Einrichtung, die sich überwiegend nach Anwendung eines der im Folgenden vorgestellten Analysewerkzeuge beantworten lassen, ergibt sich für die Bewertung des Einsatzes von mehreren baugleichen Einrichtungen innerhalb eines Kernkraftwerks ein deutlich komplexeres Bild. Ein einzelnes Analysewerkzeug bzw. -methode reicht hier zumeist nicht mehr aus, um mögliche Auswirkungen der Fehlfunktionen von PLD-LTE abzuschätzen und zu bewerten. Vielmehr ist es notwendig, mehrere Analysemethoden (z. B. FMEA, FTA, GVA-Analyse) aufeinander aufbauend einzusetzen.

Der im Rahmen dieses Projekts entwickelte CAMIC-Bewertungsansatz (Cyclic Analytic Methodology for I&C) kombiniert hierbei unter anderem die folgenden Analysewerkzeuge:

- **FMEA – Fehlzustandsart- und - auswirkungsanalyse** /DIN 06/, /DIN 15a/
  - Generische Untersuchung und Analyse der Ausfallmöglichkeiten einer PLD-LTE, sowohl hinsichtlich der Hard- und Software der PLD-LTE als auch hinsichtlich ihres Lebenszyklus
  - Generische Untersuchung und Analyse der Fehlzustandsauswirkungen einer PLD-LTE auf das LT-System oder die LT-Funktion
  - Ermittlung der Erkennbarkeit des Auftretens eines bestimmten Fehlzustandes
  - Ermittlung von GVA-Kandidaten
- FTA – Fehlzustandsbaumanalyse (Fault Tree Analysis) /DIN 07/
  - Analyse der Ursachen eines bestimmten, zu vermeidenden Ausfalls (u. a. Funktionsausfall) mittels Top-down-Vorgehensweise
  - Ermittlung der Minimalschnitte der Kombinationen der Fehlzustände, die zu einem Ausfall führen
  - Quantitative Analyse der Ausfälle von PLD-LTE, sofern entsprechende Daten zur Verfügung stehen
- Anwendung der von der GRS entwickelten Diversitätsmatrix /GRS 15/
  - Untersuchung der Diversitätseigenschaften der in der Signalverarbeitung beteiligten Komponenten hinsichtlich der Vermeidung bzw. Beherrschung der pos-

tulierten bzw. in vorausgehenden Analyseschritten ermittelten GVA in der Leittechnik

- GVA-Analyse: Bewertung des GVA-Potentials innerhalb Leittechnik-Systeme oder -Funktionen.

Prozess der Bewertung

Die Bewertung von leittechnischen Einrichtungen ist als Prozess zu verstehen. Der PDCA-Zyklus ist durch seinen generellen Ansatz vielfältig einsetzbar und bietet die Möglichkeit, die vier Schritte „Plan, Do, Check, Act“ (PDCA) an spezielle Frage- und Zielstellungen anzupassen /DIN 15/. Auf dem Gebiet der analytischen Bewertung von leittechnischen Einrichtungen kann diese Methode für folgende **Zielstellungen** angepasst werden:

- Auslegung bzw. Design der Leittechnik eines Kernkraftwerks,
- Bewertung des Ist-Zustands und Entwicklung von Verbesserungsvorschlägen,
- Bewertung eines neuen Produkts oder seiner Betriebsarten,
- Fehlzustands-, Ursachen- und Auswirkungsanalyse,
- Bewertung des GVA-Potentials.

Diese Vorgehensweise kann für alle **Lebenszyklus-Phasen** der Leittechnik angewendet werden, z. B. Auslegung, Fertigung, Montage und Inbetriebnahme, Betrieb, Instandhaltung und Modernisierung.

Im Folgenden wird der Prozess für die Bewertung von PLD-LTE beschrieben, welche für den Einsatz in Leittechniksystemen eines Kernkraftwerks vorgesehen sind. Dieser Bewertungsprozess ist in Abb. 3.4 dargestellt und ausführlich im Technischen Bericht /GRS-A-3890/ beschrieben.

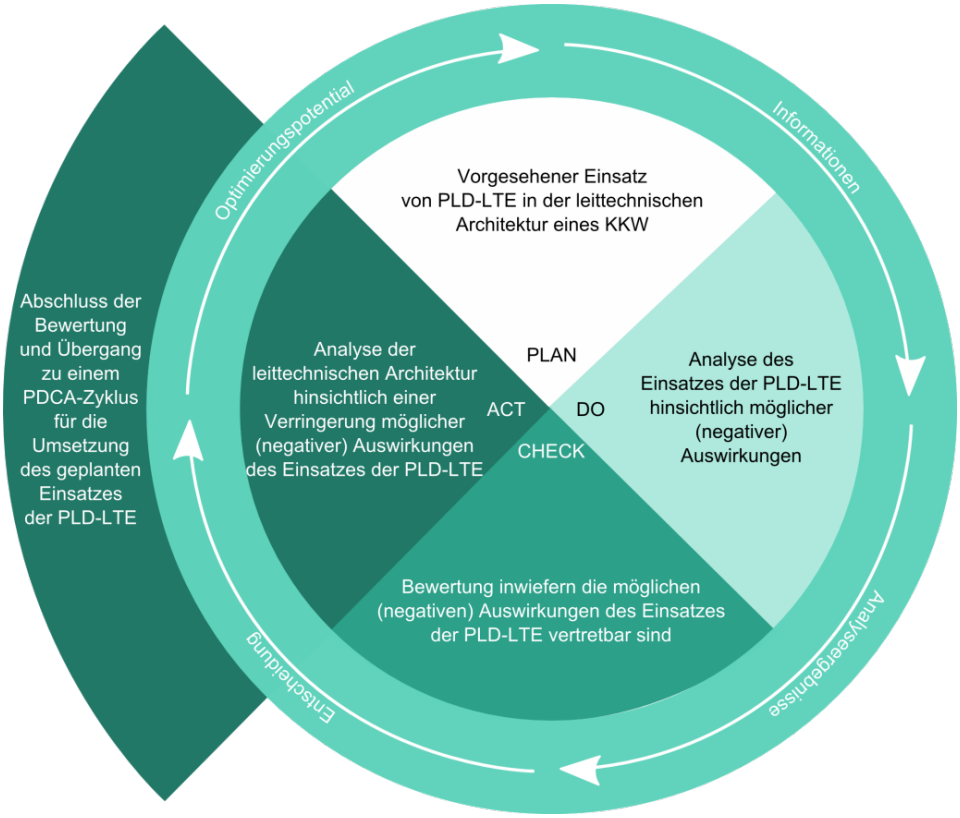

Abb. 3.4 Beispiel der CAMIC-Vorgehensweise bei der Bewertung von PLD basierten leittechnischen Einrichtungen

Der Bewertungsansatz umfasst folgende Prozessschritte:

- **PLAN:** Im Prozessschritt PLAN erfolgt das Zusammenstellen aller für die Analyse relevanten Informationen hinsichtlich des geplanten Einsatzes von PLD-LTE Einrichtungen sowie aller Anforderungen, die beim Einsatz dieser Einrichtungen erfüllt werden müssen.

- **DO:** Zunächst wird im Prozessschritt DO eine grobe Einschätzung des geplanten (neuen oder modifizierten) Leittechnik-Systems vorgenommen. Darauf aufbauend erfolgt eine Analyse des vorgesehenen Einsatzes der PLD-LTE durch Anwendung einer auf die Situation abgestimmten Abfolge von Analyseschritten. Im Bewertungsansatz ist diese Abfolge von Analyseschritten zu Beginn der Analyse noch nicht im Einzelnen vorgegeben, sondern wird unter Berücksichtigung von Zwischenergebnissen der Analyse durch Entscheidungskriterien (Decision Making Criteria) festgelegt. Dieser Teil der Analyse liefert eine Aussage über die möglichen (negativen) Auswirkungen eines Fehlzustandes der PLD-LTE bei vorgesehenem Einsatz.

- **CHECK:** Der wesentliche Aspekt des Prozessschrittes CHECK ist die Bewertung der Analyseergebnisse dahingehend, ob die aufgrund des Einsatzes der PLD-LTE möglichen Auswirkungen akzeptabel sind. Hierzu erfolgt ein Abgleich der Analyseergebnisse mit den im Prozessschritt PLAN zusammengestellten Anforderungen.
- **ACT:** Im Prozessschritt ACT muss aufbauend auf den Ergebnissen des Prozessschrittes CHECK eine Entscheidung getroffen werden, ob der Einsatz der PLD-LTE wie vorgesehen erfolgen kann. Kann und soll der Einsatz der PLD-LTE wie vorgesehen erfolgen, wird die Bewertung des Einsatzes der PLD-LTE abgeschlossen. Ist dies nicht der Fall, kann eine weitere Analyse des gesamten Leittechnik-Systems mit dem Fokus auf der Identifikation von für die Ausbreitung von Fehlzustandsauswirkungen erfolgen. Dieser Teil der Analyse kann ggf. Hinweise auf Möglichkeiten zur Vermeidung oder Verringerung der bei Einsatz der PLD-LTE möglichen (negativen) Auswirkungen liefern.

Nach dem Durchlaufen aller Prozessschritte führen die gewonnenen Erkenntnisse möglicherweise zu Änderungen an den Planungen für den Einsatz der PLD-LTE und daher zu einer Veränderung der für die Analyse relevanten und den Analyseschritten zugrunde gelegten Informationen. Diese Informationen können bei einer erneuten Bewertung im Prozessschritt PLAN verwendet werden. Ein negativer Prozessabschluss, d. h. Ausstieg aus diesem PDCA-Zyklus, ist prinzipiell in jedem Prozessschritt durch eine vordefinierte Entscheidung möglich, wird aber zumeist im Prozessschritt ACT erfolgen.

Elemente des Bewertungsansatzes

Die Vorgehensweise des hier entwickelten Bewertungsansatzes stützt sich für alle Prozessschritte auf die nachfolgenden Elemente.

- Analyseschritte und Eingangsinformationen
  - Die Durchführung von Analyseschritten ist zu verstehen als entweder die Anwendung eines Analysewerkzeugs oder ein Teilschritt bei der Anwendung eines Analysewerkzeugs. Bei einem Analyseschritt kann es sich auch um einen Schritt handeln, der für die strukturierte Vorgehensweise im Prozess der Bewertung notwendig, aber keinem Analysewerkzeug zuzuordnen ist. Ein Analyseschritt ist nur dann durchführbar, wenn die für ihn erforderlichen Eingangsinformationen und Zwischenergebnisse vorliegen.

- Bei den Eingangsinformationen handelt es sich um für die Durchführung eines Analyseschrittes notwendige Informationen. Bei Eingangsinformationen kann es sich um Unterlagen, handeln, die beispielsweise Informationen über das System und/oder die Einrichtung oder weitere technische Anforderungen enthalten. Da die erforderlichen Informationen in sehr unterschiedlicher Form und in verschiedenen Dokumenten vorliegen können, wird bei den für einen Analyseschritt erforderlichen Informationen allgemein auf den sachlichen Inhalt der Informationen verwiesen.

- Entscheidungskriterien (Decision Making Process)
  - Die Entscheidungskriterien im CAMIC-Ansatz sind als Fragen formuliert. Die Antworten auf diese Fragen bestimmen schrittweise die genaue Abfolge der Analyseschritte. Hierbei ist anzumerken, dass jede Änderung am geplanten Einsatz der PLD-LTE gegenüber einem vorherigen Durchlaufen des PDCA-Zyklus diese Abfolge ändern kann.
  - Die Entscheidungskriterien sind im Technischen Bericht /GRS-A-3890/ zusammengefasst und erläutert. Die Frage, ob ein Entscheidungskriterium erfüllt ist, wird während der Bewertung des Einsatzes der PLD-LTE auf Grundlage von Eingangsinformationen oder Zwischenergebnissen der Analyse entschieden. Ein Entscheidungskriterium kann entweder erfüllt oder nicht erfüllt sein und muss im Workflow-Diagramm (Decision Making Diagram) mit „ja“ oder „nein“ beantwortet werden.

- Zwischenergebnisse
  - Bei Zwischenergebnissen handelt es sich um die Ergebnisse eines Analyseschrittes (output), die entweder in einem folgenden Analyseschritt oder für die Beurteilung eines folgenden Entscheidungskriteriums verwendet werden (input) oder anhand derer sich entscheiden lässt, ob ein nachgeordnetes Entscheidungskriterium erfüllt ist.

- Start-, Halte- und Endpunkte
  - **Startpunkt**: Der Startpunkt bildet die Ausgangssituation für die Anwendung des Bewertungsansatzes. Die Ausgangssituation spiegelt den Gegenstand der Bewertung vor dem ersten Durchlaufen des PDCA-Zyklus wieder.

- **Haltepunkte**: Haltepunkte beschreiben mögliche Situationen, wie sie sich am Ende eines Prozessschrittes darstellen. Gleichzeitig stellen die verschiedenen Haltepunkte jeweils eine Ausgangssituation für den folgenden Prozessschritt dar, wobei der folgende Prozessschritt weitere Haltepunkte des vorhergehenden Prozessschrittes aufgreifen muss.

- **Endpunkte**: Die Endpunkte beschreiben mögliche Situationen am Ende der Anwendung des Bewertungsansatzes. Endpunkte können daher immer nur mit entweder einem positiven oder einem negativen Prozessabschluss, d. h. Ausstieg aus dem PDCA-Zyklus für die Bewertung des Einsatzes von PLD-LTE und ggf. einem Übergang zu einem anderen Prozess verbunden sein (Beginn der Umsetzung oder Verwerfen der Pläne).

- Einzelne Elemente der für die Bewertung des vorgesehenen Einsatzes von PLD-LTE entwickelten CAMIC-Methodik wie Analyseschritte und dafür relevante Entscheidungskriterien werden im Technischen Bericht /GRS-A-3890/ für alle Prozessschritte in einer Matrix zusammengefasst und mit einer Kennung versehen. Diese Kennung wird in den Workflow-Diagrammen des CAMIC-Ansatzes durchgehend verwendet.

- Kennzeichnung:

  - jedem Analyseschritt und jedem Entscheidungskriterium sowie jeder Eingangsinformation und jedem Zwischenergebnis wird eine Kennung zugeordnet, die wie folgt aufgebaut ist:

    - „A“ für Analyseschritt

    - „I“ für Eingangsinformation

    - „E“ für Entscheidungskriterium

    - „Z“ für die Art Zwischenergebnis

    - Anschließend folgt ein Bindestrich mit anschließendem Hinweis auf den Prozessschritt („P“ für Plan, „D“ für Do, „C“ für Check und „A“ für Act), gefolgt von einer fortlaufenden Nummer.

- Durchführung der Bewertung

  - Das Ziel der Bewertung von PLD-LTE ist die Beantwortung der Frage, ob die relevanten Anforderungen an diese Einrichtungen (u. a. Kerntechnisches Re-

gelwerk, Standards, Spezifikationen) erfüllt sind. Lässt sich diese Frage hingegen nicht eindeutig bejahen, muss eine Entscheidung getroffen werden, ob weitere Maßnahmen zur Erfüllung der Anforderungen ergriffen werden oder die Planungen zum Einsatz von PLD-LTE verworfen werden müssen.

Der im Vorhaben entwickelte CAMIC-Bewertungsansatz umfasst alle für die Analyse erforderlichen Prozessschritte des PDCA-Zyklus. Die Vorgehensweise alle Prozessschritte ist im Technischen Bericht /GRS-A-3890/ anhand von Tabellen und Workflow-Diagrammen dargestellt und beschrieben.

3.2.3 Modellbasierte Erprobung der entwickelten CAMIC-Methode

Beispielhafte Anwendung einer von der CAMIC-Bewertungsmethode vorgeschlagenen Analyse

Die PLD-LTE können sich in einer Vielzahl von Aspekten unterscheiden, die für ihre sicherheitstechnische Bewertung von Funktionen, Systemen und Komponenten relevant sind:

- Funktionen der Einrichtungen: u. a. Messen, Steuern, Regeln, Schutz, Datenübertragung, Mensch-Maschine-Schnittstelle,
- Interne Architektur der Baugruppe / des Gerätes wie z. B. einfache oder redundante Struktur, Selbstüberwachung,
- Technologie bzw. Bauweise (z. B. PLD-LTE als hochintegriertes SoC - System-of-the-Chip oder als komplexe Baugruppen mit einem Mikroprozessor und Speicherkomponenten),
- Art und Inhalt der technischen Dokumentation (u. a. Schaltpläne, Black und/oder White Box Komponenten der Hard- und Software),
- Qualifizierung von Baugruppen einschließlich Software (u. a. Prüf- und Analyseergebnisse, neue oder betriebsbewährte Technologie),
- Einsatzbereich und Betriebsbedingungen (z. B. Strahlenbelastung, elektromagnetische Verträglichkeit),
- Betriebsführung (u. a. Konfigurationsmanagement, Prüfwerkzeuge für Instandhaltung).

Die o. g. Aspekte können die Sicherheits- und Zuverlässigkeitsbewertung der jeweiligen Baugruppe entscheidend beeinflussen und sehr spezifisch sein, so dass die Übertragbarkeit der Analyseergebnisse zwischen unterschiedlichen PLD-basierten Einrichtungen hinsichtlich der Fehlerursachen, -erkennung, -vermeidung und -beherrschung nicht immer zweifelsfrei und nachvollziehbar erreichbar ist. Hiermit war es auch bei der Entwicklung des CAMIC-Ansatzes erforderlich, die gewählte Vorgehensweise zunächst anhand der Anwendung der FMEA-Methode zu erproben.

Die bewährte Vorgehensweise hierzu ist die Nutzung des modellbasierten Ansatzes, in dem die typischen Merkmale von generischen PLD-LTE berücksichtigt werden. Hierbei soll das Modell generell nur die als wichtig angesehenen Eigenschaften des Vorbilds berücksichtigen, um durch diese Vereinfachung zu einem überschaubaren Abbild zu gelangen, welcher sich später durch weitere Analysen bewerten und/oder mittels experimentellen Untersuchungen validieren lässt.

Modellbasierte Vorgehensweise

Für die Modellentwicklung wurden zunächst die typischen Merkmale bzw. Funktionen der Antriebssteuerung zugrunde gelegt, weil in diesem Bereich bereits mehrere Typen von PLD-LTE mit unterschiedlichen Funktionalitäten (redundante Verarbeitung, automatische Überwachung, Kommunikation usw.) in der Prozessleittechnik eingesetzt werden und hierzu bereits einige generische Informationen verfügbar sind. Des Weiteren wurden typischerweise zuerst wichtige Funktionen (u. a. logische Verknüpfungen der Steuerung) der Antriebssteuerungsbaugruppen modelliert, die dort auf der FPG-Basis implementiert sind. Da die Informationen zu den PLD-LTE nicht immer im erforderlichen Umfang und Detaillierungsgrad zur Verfügung stehen, kann die Modellierung schrittweise mit zunehmender Detaillierungstiefe anhand von Modellannahmen und Erfahrungsrückfluss aus der Modellanalyse erfolgen. Hierzu wurden folgende Modellierungsansätze eingesetzt:

- Blackbox-Modelle beschreiben das Verhalten der Ein- und Ausgangssignale der Baugruppe (System, Teilsystem) in deskriptiver Weise und verwenden einen allgemeinen Modellansatz (u. a. regel- und wissensbasierte Modellierung, Analogiebetrachtungen) zur Approximation des Verhaltens der Baugruppe im Falle des Auftretens eines oder mehrerer Fehler,
- Whitebox-Modelle stellen kausale Zusammenhänge innerhalb einer Baugruppe oder eines Systems dar. Die funktionalen Zusammenhänge können anhand vor-

handener Informationen analytisch beschrieben und modelliert werden, wobei hierzu die iterative Vorgehensweise eingesetzt werden kann. Mit Software-Werkzeugen können auch Simulationsmodelle (z. B. MATLAB/Simulink) und Fehlzustandsbaummodelle (z. B. RiskSpectrum) erstellt werden,

- Greybox-Modelle sind eine Mischform von Blackbox- und Whitebox-Modellen.

Die Erprobung der Anwendbarkeit der FMEA-Analyse für die Zielsetzung der CAMIC-Vorgehensweise macht es erforderlich, folgende Annahmen und Festlegungen zu treffen:

- Fehlzustandsarten der Betrachtungseinheiten sollen durch die FMEA-Analyse **abhängig** von der Abstraktionsebene festgelegt werden (s. Abb. 3.5).
- Die globalen Fehlzustandsauswirkungen (-effekte) sollen **unabhängig** von der Abstraktionsebene in folgende zwei Kategorien unterteilt werden:
  - Fehlanregung (spurious failure): aktiver Fehler, der zur unerwünschten Anregung einer Funktion (Aktion) führt,
  - Ausfall bei Anforderung (failure on demand): aktiver oder passiver Fehler einer Betrachtungseinheit im Anforderungsfall, der zur unerwünschten Anregung einer Funktion führt oder die Ausführung einer Funktion (z. B. Ausfall einer Diode in Sperrrichtung) verhindert.
- Auswirkungsbreite einer Fehlzustandsart bzw. einer Ursache soll als Einzelausfall einer Betrachtungseinheit (z. B. Ein- oder Ausgangssignal) oder GVA-Ausfall (CCF) mehrerer Betrachtungseinheiten (z. B. Ausfall gleichartiger Komponenten innerhalb einer Baugruppe bzw. eines Systems) definiert werden.
- Die Fehlererkennung einer Fehlzustandsart soll in zwei Kategorien unterteilt werden:
  - Selbstmeldend, u. a. Erkennung einer Fehlzustandsart unmittelbar nach dem Auftreten durch Selbstüberwachung einer Betrachtungseinheit oder durch Anregung einer unerwünschten Funktion auf der Systemebene,
  - Nicht selbstmeldend: Fehleridentifizierung durch automatische und/oder manuelle Prüfungen der Betrachtungseinheit.

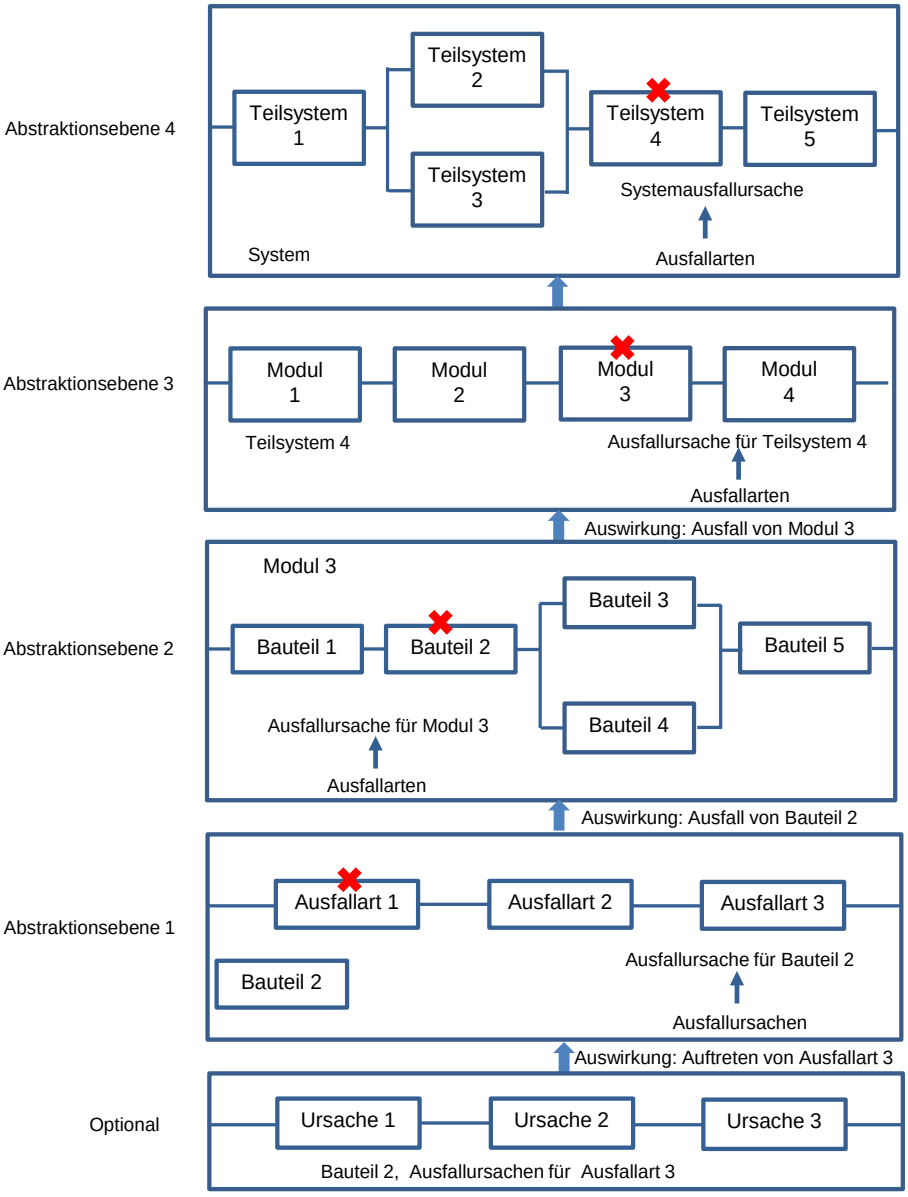

Abb. 3.5 Zusammenhang zwischen Fehlzustandsarten und -auswirkungen /DIN 06/

Anmerkung: Das Auftreten einer Fehlzustandsart ist mit einem roten Kreuz markiert

Modell AS-PLD-BB der Antriebssteuerung

Im Vorhaben wurde zunächst ein Blackbox-Modell einer generischen Antriebssteuerbaugruppe erstellt, um die wesentlichen Funktionen der Ein- und Ausgangssignale auf den Abstraktionsebenen von 2 bis 4 (siehe Abb. 3.5) zu erfassen. Die Antriebssteuerbaugruppen werden zur Ansteuerung und Überwachung von Antrieben in der Steuerungsebene eines Leittechniksystems eingesetzt. Um eine Bewertung potentieller Fehlzustandsarten und Fehlzustandsauswirkungen auf Modellbasis zu ermöglichen, werden weitere Annahmen hinsichtlich der internen und externen Signalverarbeitung

(Greybox-Modell) getroffen. Für die Modellierung wurde die Steuerung eines durchlaufenden Antriebs (z. B. Motor einer Pumpe) zugrunde gelegt. Die Steuerbefehle der Antriebssteuerbaugruppe (Motor EIN und AUS) werden in der Schaltanlage über die Koppelrelais an den Leistungsschalter weitergegeben. Das Modell besteht im Wesentlichen aus drei Funktionsmodulen (s. Abb. 3.6):

- Befehlsmodul (FPGA Baustein) verarbeitet
  - die Steuerbefehle von der Steuerstelle (Handbefehl AUS/EIN),
  - die Steuerbefehle der automatischen Steuerung/Regelung (Automatikbefehl AUS/EIN),
  - die Schutzbefehle von Schutzverriegelungen, Sicherheitsleittechnik (Schutzbefehl AUS/EIN),
  - ggf. Rückmeldungen aus der Koppelebene, (z. B. Meldung Motor AUS/EIN) der Schaltanlage.
- Überwachungsmodul überwacht die Rückmeldungen aus der Koppelebene, z. B.
  - Schaltzustand der Schaltgeräte (EIN/AUS),
  - Fehler der Stromversorgung (u. a. Abzweigstörung),
  - Laufzeitüberwachung (Ausgabe eines Störungssignals, wenn nicht innerhalb der Überwachungszeit eine entsprechende Stellungsänderung des Schaltgerätes erfolgte).
- Stromversorgungsmodul der Baugruppe.

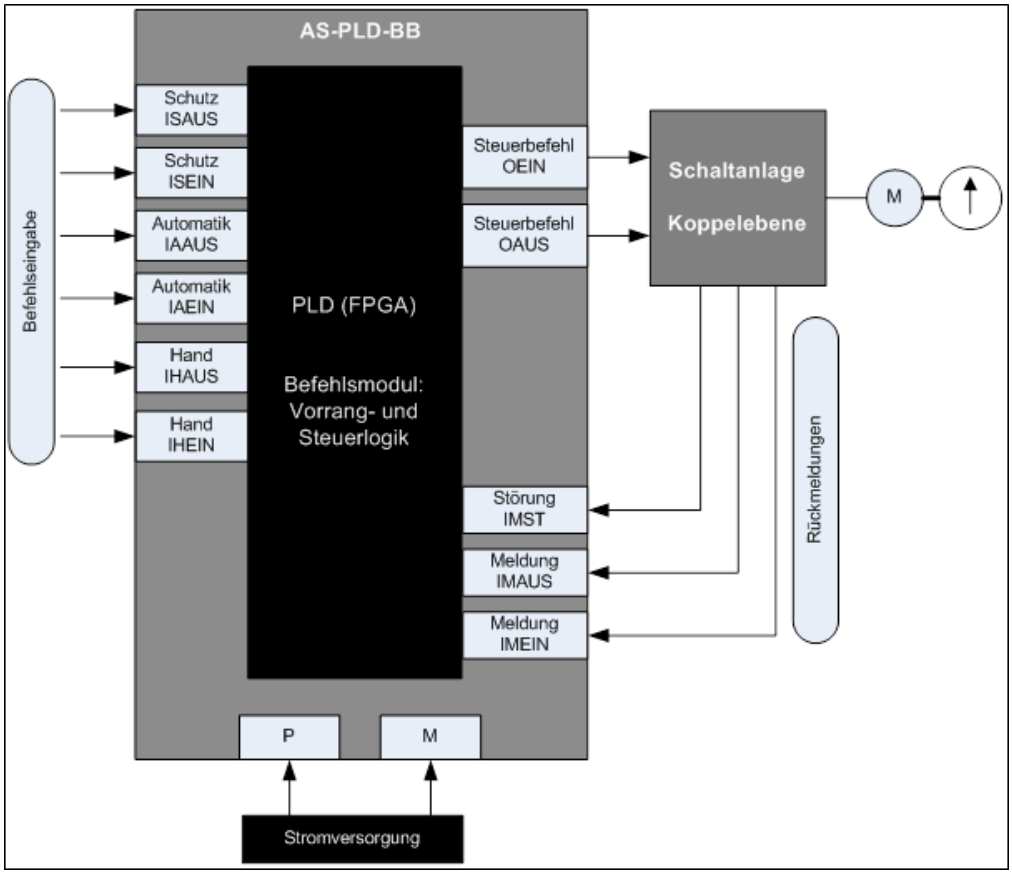

Abb. 3.6 Funktionsblockdiagramm des Modells der Antriebssteuerung

Auf der Modellbasis erfolgte die FMEA-Analyse, hierzu wurden auch folgende Aspekte untersucht:

- Ermittlung von Erkennungsmöglichkeiten der Fehlzustandsarten: entweder selbstmeldend, d. h. unmittelbar nach dem Auftreten des Fehlzustandes oder Erkennung im Rahmen von Prüfungen,
- Ermittlung der Fehlzustandsarten, die als potentielle GVA-Ausfälle analysiert werden sollen,
- Validierung des Modells hinsichtlich Modellierungstiefe und Nachvollziehbarkeit der Ergebnisse.

Danach wurde die Modellierung der Antriebsteuerung hinsichtlich der Spezifizierung der Signalverarbeitung im Befehlsmodul (z. B. Grey-Box-Modell für zeitabhängige Abläufe, Fehlererkennung und -meldung) und Berücksichtigung redundanter Signalverarbeitung erweitert. Die Modellierung und die FMEA-Analyse sind im Technischen Bericht /GRS-A-3890/ dokumentiert.

3.3 Vorstudien zur Weiterentwicklung von Methoden zu Bewertung personell-organisatorischer Einflüsse (AP 3)

3.3.1 Methoden für die qualitative und quantitative Bewertung des Beitrags der Sicherheitskultur zum sicheren Betrieb eines Kernkraftwerks

Die Recherchen im Rahmen der Vorstudie dienten dazu, Erkenntnisse aus Wissenschaft und Technik zu ermitteln, auf denen die Entwicklung einer Methode für die quantitative Bewertung des Beitrags der Sicherheitskultur zur Zuverlässigkeit sicherheitsbezogenen Handelns aufzubauen hat.

Im Einzelnen ist

- den weiteren Arbeiten einen geeigneten Begriff der Sicherheitskultur zu Grunde zu legen und die Auswahl dieses Begriffs zu begründen,
- zu klären, was unter dem quantitativen Beitrag der Sicherheitskultur zur menschlichen Zuverlässigkeit zu verstehen ist, welche Ursache-Wirkungs-Beziehungen also zwischen Sicherheitskultur, weiteren Rahmenbedingungen der Aufgabenerfüllung, Handeln und Zuverlässigkeit bestehen,
- einen Satz von Kriterien zu formulieren, welche Erkenntnisse prinzipiell nutzbar sind, um diese Ursache-Wirkungs-Beziehung auch quantitativ zu erfassen,
- der Bestand an fachlich fundierten Publikationen zu ermitteln, die den Kriterien der Nutzbarkeit entsprechen und die Ergebnisse zu dokumentieren,
- zu beurteilen, ob die nutzbaren Publikationen genug Information bieten, um einen erfolgversprechenden Arbeitsplan für die Entwicklung der angestrebten Methode zu erstellen.

Als Grundlage wurde der Begriff der Sicherheitskultur aus dem deutschen kerntechnischen Regelwerk /BMU 15/ übernommen. Er geht auf den Sicherheitskulturbegriff aus dem Regelwerk der IAEA /IAE 07/ zurück, erweitert ihn aber um wichtige Aspekte:

– „Die Sicherheitskultur ist durch eine, für die Gewährleistung der Sicherheit der Anlage erforderliche, sicherheitsgerichtete Grundhaltung, Verantwortung und Handlungsweise aller Mitarbeiter bestimmt. Sicherheitskultur umfasst dazu die Gesamtheit der Eigenschaften und Verhaltensweisen innerhalb eines Unternehmens und beim Einzelnen, die dazu dienen, dass die nukleare Sicherheit als eine übergeord-

nete Priorität die Aufmerksamkeit erhält, die sie aufgrund ihrer Bedeutung erfordert."

- „Die Grundlage für einen sicheren Betrieb von Kernkraftwerken ist das sicherheitsgerichtete Zusammenwirken personeller, technischer und organisatorischer Faktoren (Mensch-Technik-Organisation). Die Vernetzung dieser Faktoren mit dem Ziel eines sicherheitsgerichteten Handelns ist auch Grundlage für eine hohe Sicherheitskultur."

Der Sicherheitskulturbegriff des Regelwerks bietet wichtige und konkrete Ansatzpunkte für die genauere Planung der angestrebten Methodenentwicklung:

- Der Begriff aus dem Regelwerk bestimmt in allgemeiner Form das Wesen und die Aufgabe der Sicherheitskultur. Sie Ist ein Netzwerk vielfältiger Merkmale, Aktivitäten und Vorkehrungen im Unternehmen bzw. auf Seiten der Personen, die in oder für ein Betreiberunternehmen arbeiten und hat die Aufgabe, die Sicherheit im Unternehmen bzw. im Handeln des Mitarbeiters durch angemessene Priorisierung der Sicherheit zu fördern.
- Diese Bestimmung der Sicherheitskultur legt auch einen allgemeinen Beurteilungsmaßstab fest:
  - Eine real bestehende Unternehmenskultur ist danach zu beurteilen, inwieweit sie Merkmale, Aktivitäten und Vorkehrungen umfasst, die zur Sicherheitskultur entsprechenden Regelwerksbegriff gehören.
  - die Sicherheit der kerntechnischen Anlagen des Unternehmens fördert bzw. zur Förderung der Sicherheit beiträgt.

Das Regelwerk der IAEA ermöglicht eine Präzisierung der Merkmale, Aktivitäten und Vorkehrungen, die eine Sicherheitskultur auszeichnen und die eine real bestehende Unternehmenskultur aufweisen sollte. Die IAEA unterscheidet fünf übergeordneten „Charakteristika" mit jeweils mehreren, detaillierteren „Attributen" /IAE 09/. Charakteristika der Sicherheitskultur sind:

1. Sicherheit ist ein eindeutig anerkannter Wert.
2. Sicherheit ist ein klares Ziel der Führung.
3. Die Verantwortung für die Sicherheit ist klar.

4. Sicherheit wird in allen Aktivitäten berücksichtigt.

5. Sicherheit wird durch Lernen vorangetrieben.

Charakteristika und Attribute haben sich aus einem jahrelangen Entwicklungsprozess unter Beteiligung vieler Experten ergeben und unterstützen eine qualitative Beurteilung.

Das deutsche Regelwerk verbindet die Sicherheitskultur explizit mit dem System aus Mensch, Technik und Organisation. Dieses System ist laut Regelwerk „Grundlage“ der Sicherheitskultur. Die zu entwickelnde Quantifizierungsmethode würde sich auch auf Methoden und Daten für die quantitative Bewertung der Zuverlässigkeit stützen können, mit der Mitarbeiter des Unternehmens auf allen Ebenen der Unternehmenshierarchie sicherheitstechnisch wichtige Aufgaben in Abhängigkeit von menschlichen, technischen und organisatorischen Faktoren erfüllen. Es ist mit grundlegenden Erkenntnissen zur Bewertung der Handlungszuverlässigkeit in einem System aus Mensch, Technik und Organisation auch möglich, die Zusammenhänge zwischen menschlichen, technischen und organisatorischen Faktoren, der Sicherheitskultur, dem Handeln und der Sicherheit unter Einbeziehung der Handlungszuverlässigkeit zu einem Modell zu präzisieren, vom dem die Entwicklung eines Quantifizierungsansatzes bzw. deren Planung ausgehen kann. Dieses Modell wird nachfolgend formuliert und beschrieben.

Arbeitspsychologie und Zuverlässigkeitsforschung nutzen ein Modell, dem zufolge Handeln, Leistung und Zuverlässigkeit von Rahmenbedingungen abhängen, die entweder außerhalb der Person liegen oder Eigenschaften der Person selbst sind. Äußere Rahmenbedingungen sind z. B. die ergonomische Auslegung der Anlage oder das praktizierte Managementsystem. Zu den inneren Rahmenbedingungen gehören die physischen und die psychischen Leistungsvoraussetzungen wie z. B. Körperkräfte und Gesundheit bzw. Sicherheitsbewusstsein, Motivation, Wissen und Können (z. B. /APA 07/, /HAC 14/, /SWA 83/). Methoden der Zuverlässigkeitsbewertung nutzen oft auch die Begriffe der externen und internen leistungsbestimmenden oder leistungsbeeinflussenden Faktoren (“performance shaping factors“ oder „performance influencing factors“ – PSF bzw. PIF), um die äußeren und inneren Rahmenbedingungen des Handelns zusammenfassend zu bezeichnen.

Abb. 3.7 veranschaulicht die Abhängigkeit der Zuverlässigkeit der Aufgabenerfüllung vom Handeln und den Rahmenbedingungen des Handelns. Das Modell gilt auch für die probabilistisch bewertete Zuverlässigkeit.

Abb. 3.7 Allgemeines Modell zuverlässigen Handelns

Dieses Modell eignet sich auch, um den Beitrag der Sicherheitskultur zur Zuverlässigkeit in sehr allgemeiner Form zu beschreiben. Man ersieht dies aus dem Wortlaut der Begriffsbestimmung laut Regelwerk:

- Die Sicherheitskultur zeichnet sich durch die angemessene Priorisierung des Ziels der Sicherheit im Handeln der Mitarbeiter und die Gesamtheit der Eigenschaften und Verhaltensweisen im Unternehmen bzw. des Mitarbeiters aus, die dieser Ausrichtung des Handelns auf die Sicherheit dienlich bzw. förderlich sind. Diese Eigenschaften und Verhaltensweisen unterstützen ein Handeln im Dienst der Sicherheit, sie sind also Rahmenbedingungen für ein solches Handeln. Beispiele für diese Eigenschaften und Verhaltensweisen sind auf Unternehmensebene z. B. die unmissverständliche Festlegung der Unternehmensziele in Bezug auf die Sicherheit und eine Führung, die klar zum Ziel der Sicherheit steht und es nicht anderen Zielen wie dem wirtschaftlichen Erfolg unterordnet.

- Auf den einzelnen Mitarbeiter bezogen liegen Eigenschaften bzw. innere, psychologische Rahmenbedingungen des Handelns u. a. in Form der Einstellungen („Grundhaltung“) zur Sicherheit vor. Zu den Verhaltensweisen des Einzelnen gehört z. B. die Einhaltung von Regeln, Richtlinien, Vorschriften und Prozeduren bei Handlungen, die für die Sicherheit wichtig sind (Charakteristikum 3, Attribut c, /IAE 09/).

Der Begriff der Zuverlässigkeit kommt zwar im Sicherheitskulturbegriff laut Regelwerk nicht vor, lässt sich aber problemlos mit ihm verbinden, weil eine adäquate Berücksichtigung der Sicherheit auch damit einhergeht, sicherheitsbezogene Aufgaben mit hoher Zuverlässigkeit zu erfüllen. Es wäre mit dem Wesen der Sicherheitskultur einfach unvereinbar, sicherheitsbezogene Handlungen mit einer unzureichenden Zuverlässigkeit auszuführen.

Das allgemeine Modell Abb. 3.7 wurde in einem Vorhaben /GRS 15a/ weiterentwickelt wobei folgende Analyseschritte mit den Attributen der Sicherheitskultur /IAE 09/ verbunden wurden (s. Abb. 3.8):

- Die Attribute der Sicherheitskultur wurden als äußere oder innere Rahmenbedingungen des Handelns bzw. als Aktionen auf der Ebene der Führung oder des sonstigen Personals klassifiziert. Zu den Aktionen gehören auch diejenigen der Kooperation und Kommunikation innerhalb und zwischen allen Hierarchieebenen im Unternehmen bzw. den verschiedenen Organisationseinheiten des Unternehmens. „Aktion“ steht für ein näher bestimmtes Handeln wie z. B. die Erteilung einer Anweisung, die Ausführung eines Eingriffs usw.

- Beim Handeln wurden Aktionen an bzw. mit den technischen Einrichtungen der Anlage von Aktionen unterschieden, die sich der Vorbereitung, Planung, Überwachung, Koordination usw. dieser technischen Aktionen zuordnen lassen. Da die Attribute eine starke Sicherheitskultur auszeichnen bzw. fördern, können Aktionen auf Seiten der Führung und der weiteren Mitarbeiter, die Attributen der Sicherheitskultur entsprechen, auch als Aktionen zur Förderung der Sicherheitskultur bezeichnet werden.

- Da auch die Rahmenbedingungen des Handelns geplant, organisiert, geschaffen, aufrechterhalten, verbessert usw. werden müssen, hängen die Rahmenbedingungen einerseits von den einschlägigen Aktionen des Managements und der übrigen Mitarbeiter ab. Andererseits unterliegen die Aktionen diesen Rahmenbedingungen: Z. B. wirkt sich eine Stärkung sicherheitsbezogener Einstellungen aller Voraussicht nach sowohl auf die Aktionen an bzw. mit den technischen Einrichtungen, als auch auf Aktionen der Vorbereitung, Planung, Überwachung, Koordination usw. der Aktionen an bzw. mit technischen Einrichtungen aus.

- Die Sicherheitskultur ist also das jeweils erreichte Ergebnis der idealerweise im Rahmen und nach Maßgabe der Regelwerksanforderungen vorangetriebenen, aktiven Förderung, Erhaltung und Weiterentwicklung der sicherheitskulturell wichtigen Rahmenbedingungen und Aktionen durch das Unternehmen.

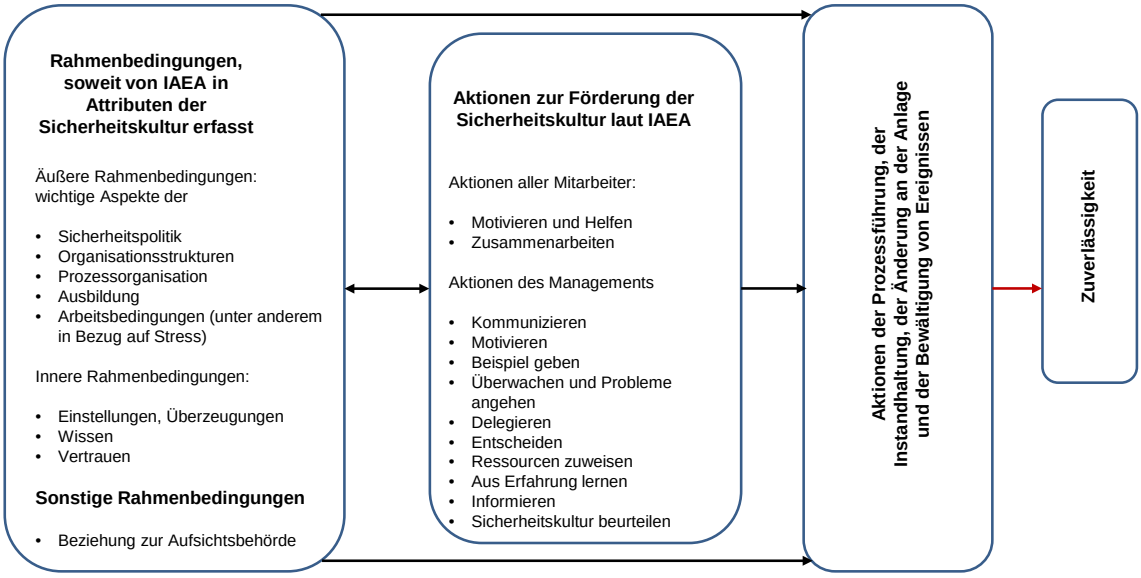

Abb. 3.8 Erweitertes Modell zuverlässigen Handelns

Ergebnis eines weiteres Projekts /GRS 16/ war, dass sich die Attribute der Sicherheitskultur /IAE 09/ problemlos als menschliche, technische oder organisatorische Faktoren klassifizieren lassen, wobei sich der Bereich der technischen Faktoren auf Attribute der menschengerechten Auslegung der Mensch-Maschine-Systeme konzentriert. Die meisten Attribute sind organisatorische und menschliche Faktoren wie z. B. die Organisationsstrukturen des Unternehmens oder die Einstellungen des Personals zur Sicherheit. Dagegen nehmen technisch-ergonomische Faktoren in Methoden für das Design und die Bewertung von Systemen aus Mensch, Technik und Organisation einen deutlich breiteren Raum ein. Auch wenn es also prinzipiell möglich ist, Attribute der Sicherheitskultur mit menschlichen, technischen und organisatorischen Faktoren zu identifizieren, bestehen doch Unterschiede in Bezug auf die Schwerpunkte und dementsprechend auf die Erkenntnisstände, die zur Sicherheitskultur bzw. zu Systemen aus Mensch, Technik und Organisation vorliegen. Man kann also die Erkenntnisse zur Sicherheitskultur mit Wissen erweitern, das zur Auslegung und Beurteilung von Systemen aus Mensch, Technik und Organisation vorliegt, ohne den Rahmen der Sicherheitskultur zu sprengen, weil deren Attribute erschöpfend mit den Kategorien „Mensch“, „Technik“ (Ergonomie) und „Organisation“ erfassbar sind. (Dementsprechend gilt auch, dass man die Sicherheitskultur in das System aus Mensch, Technik und Organisation einbeziehen kann.)

Mit den Ergebnissen früherer Untersuchungen sind zwei wichtige Erkenntnisse für den angestrebten Arbeitsplan bzw. die Entwicklung eines Ansatzes zur Quantifizierung des Beitrags sicherheitskultureller Faktoren zur Zuverlässigkeit gewonnen:

- Das System der menschlichen, technischen und organisatorischen Faktoren ist nicht nur, wie im Regelwerk festgestellt, „Grundlage“, sondern wesentlicher Teil der Sicherheitskultur.
- Man kann die Sicherheitskultur bzw. die zugehörigen Faktoren ohne Weiteres in das allgemeine Modell einfügen, das die probabilistische Zuverlässigkeit der Erfüllung sicherheitsbezogener Aufgaben auf das Handeln unter den gegebenen, äußeren und inneren Rahmenbedingungen des Handelns zurückführt (siehe Abb. 3.7).

Man braucht also “nur“ noch geeignete Daten, um sicherheitskulturelle Faktoren im Rahmen dieses Modells zu quantifizieren. Die Ermittlung solcher Daten war Zweck weiterer Recherche im Rahmen der Vorstudie unter Berücksichtigung der Kriterien, die im Fachbericht /GRS-A-3891/ ausführlich beschrieben sind. Zur besseren Übersicht sind die Erkenntnisse aus der Recherche in folgende Kategorien eingeteilt

- Lenkungsform („Corporate Governance“, Erklärung: siehe unten)
- Personalführung
- Teamarbeit
- aktive Beteiligung an der Unternehmenstätigkeit OCB („Organizational Citizenship Behavior“)
- Arbeitsmotivation und Einstellung zu Arbeit und Beruf
- Analyse und Bewertung menschlicher Zuverlässigkeit in Abhängigkeit von menschlichen, technischen und organisatorischen Faktoren

Diese Kategorien erfassen wesentliche Voraussetzungen dafür, Arbeitstätigkeiten im Einklang mit den Unternehmenszielen auszuführen:

- Lenkung und Führung decken die Aspekte der Koordination und Unterstützung dieser Arbeitstätigkeiten „von oben“, also von Seiten des Unternehmens ab,
- Kooperation, aktiver Einsatz für das Unternehmen und Motivation für die Arbeit sind dagegen die Voraussetzungen, die „von unten“, also von Seiten der Mitarbeiter und Teams, zur Erreichung der Unternehmensziele beitragen. Diese Einteilung ent-

spricht der Unterscheidung zwischen „Koordination“ und „Kooperation“ als den zwei zentralen Faktoren, die bei der „Governance“ zu beachten sind /WIE 07/.

Die Ergebnisse der Recherchen sind im Fachbericht /GRS-A-3891/. dokumentiert. Für die Entwicklung eines Quantifizierungsansatzes bzw. die Planung dieser Arbeiten sind folgende Erkenntnisse von Bedeutung:

- Nutzbar sind empirische Untersuchungen zur Abhängigkeit des Unternehmenserfolgs vom Umgang des Top Managements mit Fehlern (z. B. /DYC 05/).
- Aufgrund ihrer Themenstellung kann man bestimmte theoretische Arbeiten dem Bereich der „Corporate Governance“ zuordnen. Dabei geht es um Modelle für die mathematisch-formale Integration sicherheitskulturell wichtiger Faktoren, die man der „Corporate Governance“ zuordnen kann, in eine quantitative Sicherheits- bzw. Risikoanalyse (u. a. /ALE 12/, /MOH 12/, /MUR 96/, /PAT 96/). Einige Modellentwickler nutzen hypothetische Daten, mit denen folgende Auswirkungen simuliert werden:
  - des risikofreudigen oder risikoscheuen Entscheidungsverhalten auf der Ebene des Top-Managements /COW 04/).
  - der Anreize, Sicherheitsvorkehrungen außer Acht zu lassen, um Nachteile einer drohenden Terminüberschreitung zu vermeiden (/GAR 12/.

Solche Zusammenhänge sind auch für Expertenschätzungen interessant, weil sie zeigen, wie Sicherheit und Zuverlässigkeit von bestimmten Faktoren abhängen können. Expertenschätzungen können erforderlich sein, um Lücken des empirischen Erkenntnisstandes bis zum Vorliegen erfahrungswissenschaftlich fundierter Ergebnisse zu überbrücken. Zahlreiche empirische Untersuchungen zeigen, wie bestimmte Merkmale von Arbeitsteams und der Kooperation mehrerer Arbeitsteams dazu beitragen, Ziele zu erreichen, die das Unternehmen gesetzt hat (z. B. /GMÜ 05/):

- Erfolgsfaktoren sind z. B. Kommunikation, Koordination der einzelnen Arbeiten, Beteiligung der Teammitglieder, wechselseitige Unterstützung, individuelle Anstrengung und Zusammenhalt des Teams zur Auswirkung auf die Zielerreichung (z. B. /HÖG 01/, /HÖG 04/). Auch dazu liegen z. T. schon seit Jahrzehnten quantitative Daten vor (z. B. /LIK 61/).
- Diese Erkenntnisse sind nutzbar, weil Sicherheit und Zuverlässigkeit von der sachgerechten und guten Zusammenarbeit vieler Personen und Teams abhängt. Es be-

stehen enge Zusammenhänge mit den Charakteristika der Sicherheitskultur laut IAEA. Man kann z. B. erwarten, dass die Sicherheit nicht, wie von der IAEA gefordert (siehe oben), in allen Aktivitäten angemessen berücksichtigt werden, wenn die Mitglieder einer Arbeitsgruppe es bei der Erfüllung sicherheitstechnisch wichtiger Arbeiten an der erforderlichen, wechselseitigen Unterstützung fehlen lassen.

„Organizational Citizenship Behavior“ (OCB) beschreibt ein Mentalitätsmuster, das sich auf die subjektiv freiwillige, generalisierte Bereitschaft zum Handeln i. S. v. Organisationszielen bezieht /CON 04/. Man versteht darunter ein freiwilliges Handeln und ihre generelle aktive Mitwirkung der Mitarbeiter an der Unternehmenstätigkeit, die beide die Arbeitsleistung fördern ohne vom Unternehmen direkt belohnt zu werden /CON 04/. Es äußert sich z. B. in spontaner, freiwilliger Hilfe unter Kollegen, einer ebensolchen Unterstützung der Vorgesetzten, der Einhaltung von Regeln, geringen Fehlzeiten, keinen exzessiven Pausen, etc.. Abb. 3.9 veranschaulicht diese Zusammenhänge. Zum OCB liegen viele empirische Untersuchungen und Meta-Analysen vor:

- Arten dieses Verhaltens (unterstützendes Verhalten, generelle Willigkeit zur Mitarbeit, im Einzelnen: u. a. Arbeitszufriedenheit, Verantwortungsbewusstsein, Umsicht, Sportsgeist /LEP 02/).
- Voraussetzungen für dieses Verhalten (u. a. Unterstützung durch die Führung, Arbeitsinhalt, gerechte Behandlung usw. /SMI 83/, /WIL 91/).
- Wirkungen des OCB-Verhaltens auf die Erreichung der Unternehmensziele /POD 00/, /HOF 07/.

Die einschlägigen empirischen Erkenntnisse sind auch für die Zusammenhänge zwischen Sicherheitskultur, Handeln, Zuverlässigkeit und Sicherheit von größter Bedeutung und sollten daher so weit wie möglich genutzt werden. Man ersieht dies auch aus der Rolle der Führung, der Kooperation und der Kommunikation, die wichtige Teile des OCB sind und mit den bereits berichteten Rechercheergebnissen zu „Corporate Governance“, Führung und Teamarbeit in Einklang stehen und den Charakteristika der Sicherheitskultur laut IAEA entweder entsprechen oder zugeordnet werden können.

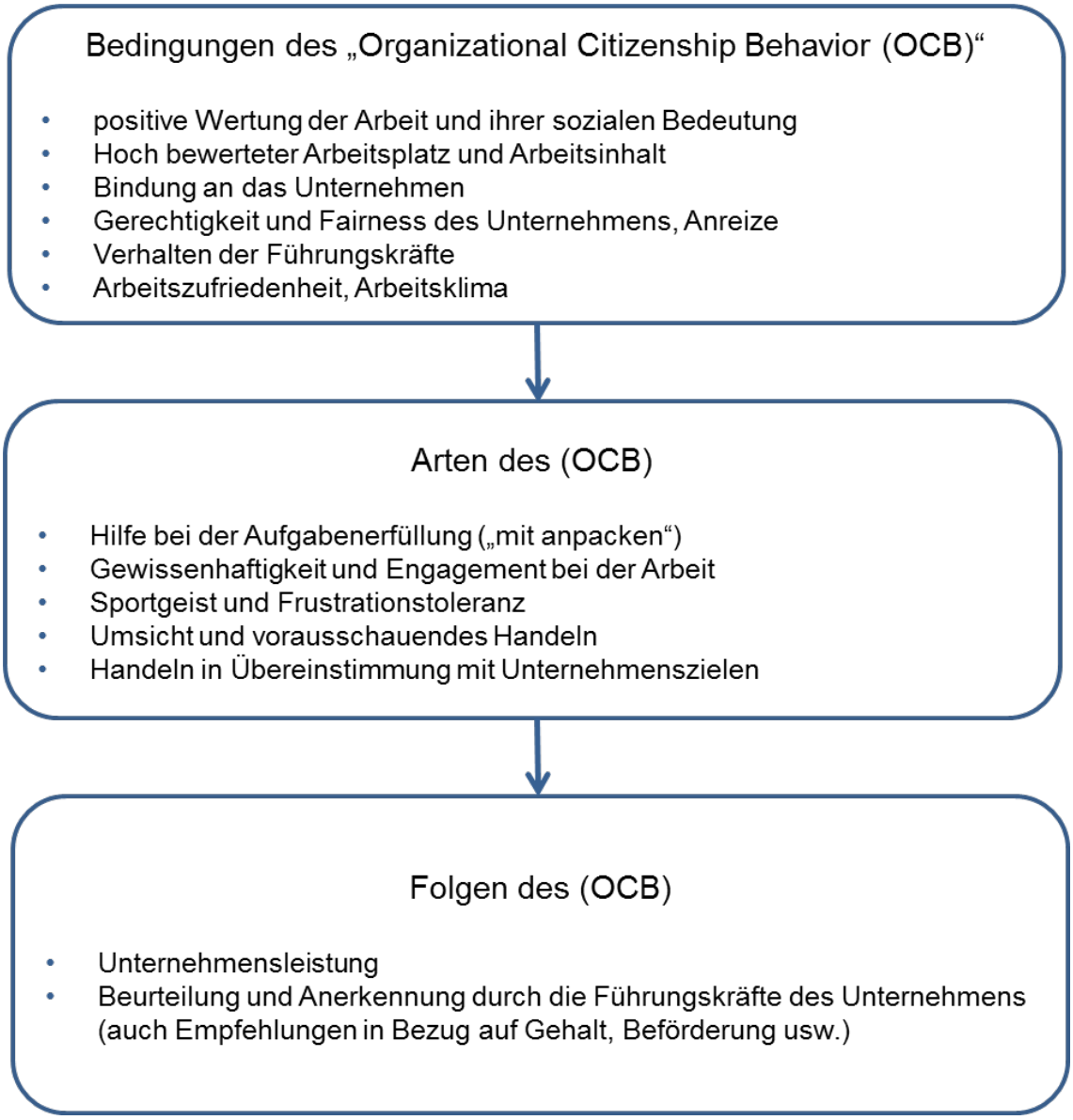

Abb. 3.9 Ursache-Wirkungszusammenhänge des Organizational Citizenship Behavior

Motivation erklärt Zielauswahl, Nachdruck und Ausdauer beim Handeln. Sie ist daher auch für sicherheitsbezogenes zuverlässiges Handeln von direkter und großer Bedeutung. Die vorliegende Recherche hat Meta-Analysen zu den Zusammenhängen zwischen Arbeitsmotivation, Handeln und Leistung berücksichtigt. Aus ihnen geht hervor, dass zahlreiche empirische Untersuchungen mit quantitativen Ergebnissen belegt werden.

Ein weiteres wesentliches Ergebnis dieses Projektes besteht darin, dass die Erkenntnisse zu „Corporate Governance“, „Führung“, „Teamarbeit“, „Organizational Citizenship Behavior“ und „Motivation“ mit den Attributen der Sicherheitskultur in Einklang stehen.

Des Weiteren hat die Vorstudie die Methoden für die Analyse und Bewertung menschlicher Zuverlässigkeit einbezogen und folgende Ergebnisse erbracht:

- Analyse und Bewertung menschlicher Zuverlässigkeit können sich auf unterschiedlichste Methoden stützen. Die Recherche konzentrierte sich auf das „Handbook for Human Reliability Analysis with Emphasis on Nuclear Power Plant Application” (/SWA 83/, auch als „Technique for Human Error Rate Prediction (THERP)“ bekannt). Dafür sprechen mehrere Gründe:

1. Die Dokumentation ist umfangreich und öffentlich zugänglich.

2. Es liegt die Empfehlung vor, sie für die probabilistische Sicherheitsanalyse deutscher Kernkraftwerke zu nutzen.

3. Die Methode berücksichtigt sowohl wesentliche Aktionen auf Seiten der Führung und des sonstigen Personals, als auch menschliche, technische und organisatorische Rahmenbedingungen dieser Aktionen.

4. Auch sind die Quantifizierungen, die diese Methode vorsieht und teils aus empirischen Quellen, teils über Expertenschätzungen gewonnen hat, mit Hilfe statistisch fundiert ausgewerteter Betriebserfahrungen in einem bestimmten Umfang empirisch überprüft worden (/PRE 13/, /PRE 16/).

Als weitere Quelle dienen in der vorliegenden Studie die Erkenntnisse eines früheren Projekts zur Analyse und quantitativen Bewertung organisatorischer Faktoren (/GRS 10/). Als nutzbar erweisen sich auch folgende Rechercheergebnisse:

- Versteht man Kultur als eine Standardisierung des Handelns, die sich durch die Kooperation zwischen Personen im Lauf der Zeit durch Lernen und der wechselseitige Anpassung herausbildet und auch die zugrunde liegenden, psychologischen Faktoren der Handlungssteuerung betrifft /HAN 11/, so folgt:

  - Planung absehbarer, immer wiederkehrender Vorgänge und Umsetzung des Geplanten spielen für die Entstehung, Erhaltung und Weiterentwicklung einer Kultur im Allgemeinen und einer Unternehmens- bzw. Sicherheitskultur im Besonderen eine Schlüsselrolle,

- Im allgemeinen Fall können Planung und Umsetzung auf Seiten der Handelnden mehr oder minder reflektiert und systematisch erfolgen. In Unternehmen dagegen handelt es sich um klar definierte Aufgabengruppen, für die wesentlich das Management zuständig ist. Auf Seiten der Geführten steht dem die mehr oder minder zuverlässige Erfüllung von Aufgaben im Rahmen der bestehenden Vorgaben, Arbeitsbedingungen und Leistungsmöglichkeiten gegenüber.

Aus diesem Blickwinkel sind für die Sicherheitskultur folgende Aktivitäten im Unternehmen wichtig:

- Ausführung erforderlicher, sicherheitsbezogener Aktionen an bzw. mit technischen Einrichtungen, also Aktionen in den Bereichen Prozessüberwachung, Prozessführung, Prüfung, Wartung, Reparatur, Änderung, Errichtung, usw.
- Anweisung, Koordination und Kontrolle dieser Aktionen einschließlich der zugehörigen Kommunikation,
- Vorbereitung und Unterstützung dieser Aktionen, Anweisungen, Koordination, Kommunikation und Kontrolle durch Planung und Realisierung der Rahmenbedingungen für ihre Ausführung. Zu dieser Vorbereitung und Unterstützung gehören auch Wissensvermittlung und Training, um die vorgesehenen Ausführenden für die Ausführung dieser Aktionen, Anweisungen, usw. zu befähigen, also eine wesentliche Rahmenbedingung sicheren und zuverlässigen Handelns auf Seiten des Menschen zu schaffen,
- Organisation dieser Vorbereitung und Unterstützung, also die Planung, Einrichtung, Lenkung und Pflege einer Prozessorganisation bzw. eines Managementsystems,
- Umsetzung einschlägiger Regelwerksanforderungen.

THERP bietet eine Reihe an Möglichkeiten, Fehler bei Aktivitäten dieser Art quantitativ zu bewerten, u. a.:

- Die Umsetzung der Anlagenpolitik wird unterlassen. Inhalt der Anlagenpolitik sind nach Swain umfassende Regelungen zum Betrieb der Anlage und Anforderungen, die für alle Mitglieder eines Fachbereichs oder einer Berufsgruppe auf der Anlage gelten /SWA 83/,
- Unter diese Begriffsbestimmung fallen auch die Regelungen der Unternehmenspolitik und Anforderungen an das Soll-Verhalten der Führungskräfte im Sinne des

kerntechnischen Regelwerks (KTA 1402, 4.1). Zur Politik des Unternehmens bzw. der Anlage hat laut kerntechnischem Regelwerk auch die Förderung der Sicherheitskultur zu gehören. Unterlässt man also im Unternehmen die Förderung der Sicherheitskultur, erfährt die Umsetzung der Anlagenpolitik Abstriche. Eine unvollständige Umsetzung läuft auf die Unterlassung der (kompletten) Umsetzung hinaus,

- THERP eröffnet damit im Prinzip die Möglichkeit, die Unterlassung der Implementierung sicherheitskultureller Faktoren sehr umfassend quantitativ zu bewerten.
- THERP unterstützt die Bewertung verschiedener regelbasierter Aktionen der Überwachung und Bedienung technischer Systeme, der Kooperation, Kommunikation und Kontrolle sowie der Erstellung und Verwendung von Prozeduren für sicherheitstechnisch wichtige Aufgaben.

Für organisatorische Faktoren wie z. B. die Aufgabenplanung liegt bereits eine Methode vor, um auch systematische Auswirkungen von Fehlern auf eine Mehrzahl von Arbeiten zu analysieren und zu bewerten /GRS 10/. Diese Methode „…basiert auf der Überlegung, dass sich Personenhandlungen in organisatorisch vorgelagerten Arbeitssystemen durch die Qualität ihrer Arbeitsergebnisse auf organisatorisch nachgeordnete Arbeitssysteme konkret auswirken und dies einen relevanten Beitrag zum Ergebnis einer probabilistischen Sicherheitsanalyse liefern könnte. Die Untersuchung und Modellierung dieser Zusammenhänge führt in mehreren Iterationsschritten zu einem sich immer weiter verzweigenden Modell der Organisation der Arbeitsabläufe im Kraftwerk“ /GRS 10/.

Meta-Analysen belegen, dass es sich zu einem erheblichen Teil um Erkenntnisse handelt, die z. T. über Jahrzehnte hinweg immer wieder reproduziert worden sind. Etablierte Bewertungsmethoden bieten Anknüpfungspunkte für die quantitative Bewertung wichtiger sicherheitskultureller Faktoren. Es liegen Informationen zu Faktoren auf Unternehmensebene (z. B. die Umsetzung der Unternehmenspolitik) und zu Faktoren auf der Ebene des Mitarbeiters (z. B. Nutzung vorhandener Prozeduren) bzw. der Mitarbeiterteams (z. B. Aktionen, mit möglichen geringen, fehlerförderlichen Abhängigkeiten) vor. Nach den Erkenntnissen aus früheren Untersuchungen der GRS, deckt der Bestand an empirischen Untersuchungen alle Bereiche der Sicherheitskultur ohne wesentliche Lücken ab /GRS 16/.

Das Konzept der Methodenentwicklung für die Quantifizierung des Beitrags der Sicherheitskultur zu Zuverlässigkeit des Handelns bei sicherheitsbezogenen Aufgaben sieht die folgenden übergeordneten Schritte vor:

- Darstellung des fachlichen Fundaments der Methode,
- Festlegung der Entwicklungsstrategie,
- Erarbeitung des Analyseteils der Methode,
- Erstellung der Teilmethode für die quantitative Bewertung.

Die Methodenentwicklung sieht vor, den Beitrag sicherheitskultureller Faktoren zur menschlichen Zuverlässigkeit wie folgt zu berücksichtigen:

- Die Förderung der Sicherheitskultur wird als Aufgabe betrachtet, die zur Umsetzung der Anlagen- und Unternehmenspolitik gehört. Zu dieser Politik rechnet die angestrebte Methode im Einklang mit THERP auch die sicherheitsbezogenen Verhaltensweisen, die ein Unternehmen, das dem Ziel der Sicherheit verpflichtet ist, z. B. von seinen Führungskräften zu erwarten hat.
- Sicherheitskultur besteht aus dem System der sicherheitskulturellen Faktoren. Folglich läuft die Förderung der Sicherheitskultur durch das Unternehmen auf die Realisierung sicherheitskultureller Faktoren oder, gleichbedeutend, die Herstellung der den sicherheitskulturellen Faktoren entsprechenden menschlichen, technischen und organisatorischen Rahmenbedingungen für die Erfüllung sicherheitsbezogener Aufgaben im Unternehmen hinaus.
- Mit den folgenden Festlegungen erfolgt sowohl die Verbindung mit der Bewertung menschlicher Zuverlässigkeit in probabilistischen Sicherheitsanalysen als auch eine erhebliche Reduktion des Aufwands für den späteren Methodenanwender:
  - Die angestrebte Methode unterstützt die quantitative Bewertung der Eingriffe (wie z. B. die Absenkung eines Druckes auf ein sicherheitstechnisch erforderliches Niveau), die eine Sicherheitsanalyse, den Ergebnissen der technischen Ereignis- und Systemanalyse zufolge, einzubeziehen hat.
  - Es werden nur regelbasierte Eingriffe betrachtet, um den Entwicklungsaufwand in Grenzen zu halten. Wissensbasierte Eingriffe und ihre sicherheitskulturell bedeutsamen Rahmenbedingungen können nach Abschluss der Entwicklung des

Quantifizierungsansatzes für regelbasiertes Handeln in einem Ausbau dieses Ansatzes angegangen werden.

- Neben dem Eingriff selbst sind alle Aktionen zu betrachten, deren Unterlassung oder fehlerhafte Ausführung die Bewertung berücksichtigen muss, weil ihre Folge, dass ein sicherheitstechnisch erforderlicher Eingriff unterbleibt oder mit unakzeptablen Fehlern durchgeführt wird, probabilistisch nicht vernachlässigt werden kann.

- Zusammenfassend heißen nachfolgend erforderliche Eingriffe und die nicht zu vernachlässigenden, fehlerträchtigen Aktionen „zu bewertende Aktionen". Sie können sehr verschiedenen Bereiche angehören: Prozessüberwachung, Prozessführung, Kommunikation und weitere Interaktionen (z. B. zur wechselseitigen Kontrolle) zwischen Personen, Aufsuchen der Arbeitsorte, Einsatz der Arbeitsmittel (einschließlich der Nutzung vorgesehener Prozeduren und des bestimmungsgemäßen Einsatzes von Checklisten), Erstellung von Unterlagen, usw.

- Die Förderung der Sicherheitskultur läuft also darauf hinaus, sicherheitskulturelle Faktoren zu implementieren, die menschliche, technische oder organisatorische Rahmenbedingungen für die Ausführung der zu bewertenden Aktionen sind. Zu diesen Rahmenbedingungen gehört auch die Festlegung und Einübung der Aktion durch Prozeduren und Training. Dieser Hinweis soll das mögliche Missverständnis beseitigen, es gehe nur um die Rahmenbedingungen der Aktion, nicht um diese selbst. Die Aktion ist in der Methode also über die Genauigkeit ihrer Beschreibung in der Prozedur und des Wissens erfasst, das durch Training und Praxis erworben und im Gedächtnis des Akteurs verankert ist.

- „Implementieren" oder „verwirklichen" kann als Vorgang und als Ergebnis dieses Vorgangs verstanden werden. Die Methode soll deshalb die quantitative Bewertung unterstützen,

  - dass die Implementierung eines sicherheitskulturellen Faktors bei der betrachteten Aktion stattgefunden hat, also nicht unterlassen worden ist.

  - welche Ausprägung der realisierte Faktor konkret aufweist. Man denke z. B. an die Umsetzung des Attributs, gute Arbeitsbedingungen u. a. durch Vermeidung von Zeitdruck, Fehlbelastung und Stress herzustellen /IAE 09/. Diese Vorkehrung kann aus Versehen unterbleiben und sich als ungünstige Rahmenbedin-

gung der Aufgabenerfüllung auf die Zuverlässigkeit betroffener Aktionen auswirken.

  - Neben der Verminderung von Abhängigkeiten stellen Kontrollen ein wichtiges Mittel dar, um Fehler zu entdecken und zu beheben. Die Entwicklung der Methode sollte daher detailliertere Schritte für die Analyse und Bewertung der Abhängigkeiten und ihrer Lockerung sowie für die Analyse und Bewertung der Kontrollen und ihrer bestmöglichen Unterstützung umfassen.

- Die unterlassene Implementierung kann Ergebnis eines zufälligen Fehlers sein oder eine systematische Ursache haben. Solche systematischen Ursachen werden dadurch berücksichtigt, dass die Implementierung des Faktors sicher unterbleibt. Der systematische Ausschluss bestimmter sicherheitskultureller Faktoren von der Implementierung erlaubt es auch, Effekte wie z. B. das systematische, absichtliche Überspringen bestimmter Sicherheitsvorkehrungen unter Zeitdruck in die Bewertung einzubeziehen.

Tab. 3.2 veranschaulicht den prinzipiellen Analyse- und Bewertungsansatz. Sie bedarf folgender Erläuterungen:

(1) Die Tabelle führt jeweils nur einen sicherheitskulturellen Faktor und einen möglichen Fehler bei der zu bewertenden Aktion auf. Mehrere Faktoren bzw. mögliche Fehler erfordern eine wiederholte Anwendung dieses Bewertungsansatzes (zur Reduktion des Aufwands durch Zusammenfassung sicherheitskultureller Faktoren: siehe unten).
(2) Sofern Fehlererkennung und Fehlerbehebung Aktionen des Menschen sind, hängen sie ebenfalls von der Implementierung relevanter sicherheitskultureller Faktoren ab. Der Bewertungsansatz ist also auch auf „recovery“-Aktionen anzuwenden.

Tab. 3.2 Prinzipieller Aufbau des Analyse- und Bewertungsansatzes

Zu bewertende Aktion				
Umsetzung eines für diese Aktion relevanten sicherheitskulturellen Faktors	ja		nein	
Wahrscheinlichkeit der Umsetzung des sicherheitskulturellen Faktors und Fehlerfaktor	$1\text{-}P_{\text{Nicht - Umsetzung des sicherheitskulturellen Faktors}}$		$P_{\text{Nicht - Umsetzung des sicherheitskulturellen Faktors}}$	
Möglicher Fehler bei der zu bewertenden Aktion (evtl. in Abhängigkeit von Fehlern bei anderen Aktionen)	trotz Umsetzung des sicherheitskulturellen Faktors		ohne Umsetzung des sicherheitskulturellen Faktors	
Ausführung der zu bewertenden Aktion	korrekt	• unterlassen oder • fehlerhaft	korrekt	• unterlassen oder • fehlerhaft
Wahrscheinlichkeit für Fehler bei der Aktion in Abhängigkeit von Umsetzung bzw. Nicht-Umsetzung (des sicherheitskulturellen Faktors) und Fehlerfaktor	$1\text{-}P_{\text{Fehler Aktion - trotz Umsetzung}}$	$P_{\text{Fehler Aktion - trotz Umsetzung}}$	$1\text{-}P_{\text{Fehler Aktion - trotz Umsetzung}}$	$P_{\text{Fehler Aktion - trotz Umsetzung}}$
Fehlererkennung, Fehlerbehebung		Welche Fehler sind erkennbar und behebbar?		Welche Fehler sind erkennbar und behebbar?

Zur Entwicklungsstrategie für die Methode gehörten auch Nutzung von Beständen zu sicherheitskulturellen Faktoren aus früheren Projekten /GRS 16/:

- Für die Methodenentwicklung soll eine Gruppierung dieser Faktoren vorgenommen werden, indem Faktoren ähnlicher Art zusammengefasst werden. Eine Gruppierung der Art „klar formulierte Sicherheitsziele“, könnte diese und weitere einschlägige Attribute zusammenführen. Der Bewertungsansatz könnte sich dann auf die Umsetzung dieses „übergeordneten Attributs“ beschränken.

- Sicherheitskulturelle Faktoren können sich der direkten Beobachtung und Implementierung entziehen. Dabei ist in erster Linie an die menschlichen Faktoren in den Bereichen der Einstellungen und der Motivation zu denken. Das Unternehmen kann nur Anreize setzen bzw. Rahmenbedingungen schaffen, die erwarten lassen, dass Personen bis hin zu den Führungskräften auf der obersten Leitungsebene so motiviert und eingestellt sind, dass sie der Sicherheit in ihren Aktionen das erforderliche Gewicht geben und ihr andere Ziele entsprechend unterordnen. Erkenntnisse zu belegbar wirksamen Anreizen sind aus den empirischen Untersuchungen zusammenzustellen.

Die Entwicklung des Bewertungsansatzes soll in zwei Stufen vor sich gehen:

- In der ersten Stufe soll ein Bewertungsansatz auf der Basis von THERP aufgebaut werden. Entwicklung und kritische Prüfung dieses „Erstansatzes“ werden zeigen, welche Grenzen etablierte Methoden für die Bewertung menschlicher Zuverlässigkeit haben.

- In einer zweiten Stufe der Entwicklung sollen die Bestände an empirischen, quantitativen Erkenntnissen genutzt werden, um Lücken und Beschränkungen im Erstansatz zu schließen. Dabei soll auch die im Erstansatz und in THERP summarisch betrachtete Umsetzung der Anlagenpolitik /SWA 83/ in detailliertere Schritte mit dem Ziel zerlegt werden, mögliche Fehler und ihre Folgen bei diesen Schritten zu bestimmen und probabilistisch zu bewerten. Hierbei sollen, analog der Methode für die Analyse und Bewertung organisatorischer Faktoren /GRS 10/, insbesondere Fehlermöglichkeiten betrachtet werden, die eine breite(re) Wirkung entfalten, also eine Mehrzahl von Aktionen betreffen können.

Im Fachbericht /GRS-A-3891/ ist die Entwicklung des Analyse- bzw. des Bewertungsteils der angestrebten Methode erläutert, wobei die Methode in ihrem Analyseteil prinzipiell dem Vorgehen, das in der Bewertung der menschlichen Zuverlässigkeit üblich ist

(z. B. /SWA 83/) entspricht. Die quantitative Bewertung stützt sich in der ersten Entwicklungsstufe auf das Zahlenwerk, das THERP enthält und das sich auf die Umsetzung sicherheitskultureller Faktoren und ihre Beiträge zur Zuverlässigkeit der Aktionen unter den gegebenen und durch Umsetzung sicherheitskultureller Faktoren geschaffenen Rahmenbedingungen des Handelns anwenden lässt. Dieses Zahlenmaterial soll in der zweiten Entwicklungsstufe anhand einer Auswertung empirischer Untersuchungen so weit wie möglich erweitert und überprüft werden.

3.3.2 Vorstudie zur Bewertung der Auswirkungen organisatorischer Einflussfaktoren

Anhand einer Vorstudie wurden ausgewählte Beispiele untersucht, ob sich bei in der Vergangenheit aufgetretenen Unfallereignissen technologieübergreifende, charakteristische organisatorische Einflussfaktoren identifizieren lassen, die einen Unfallablauf signifikant beeinflusst haben, und ob es Möglichkeiten zur Bewertung der Signifikanz solcher Einflussfaktoren gibt. Dabei wurde auch geprüft, welche organisatorischen Einflussfaktoren gegebenenfalls positive Auswirkungen auf die Beherrschung, auf Notfallmaßnahmen oder auf die Begrenzung von Umweltauswirkungen hatten.

Die aus sicherheitstechnischer Perspektive ungeeigneten Organisationsstrukturen sowie nicht geeignete Prozessorganisation beeinflussen die Ursachen für nukleare Unfälle und deren Abläufe negativ – dies zeigt die diesem Bericht zugrunde liegende Auswertung. Gleiches gilt auch für große Unfallereignisse bei nicht-nuklearen Technologien. Das betrifft sowohl die Gründe, die zu einem Unfallereignis führten, als auch Ereignisse, die beim Versuch der Beherrschung eines Unfallablaufs auftraten. Dies können organisatorische Defizite sein, die die Entstehung eines Unfalls begünstigten, die Notfallmaßnahmen zur Beherrschung eines Unfalls negativ beeinflussten oder die Umweltauswirkungen infolge des Unfalls beeinflussten.

Deshalb wurde eine Vorstudie mit dem Ziel durchgeführt, anhand ausgewählter Beispiele zu untersuchen, ob sich bei in der Vergangenheit aufgetretenen Unfallereignissen technologieübergreifende, charakteristische organisatorische Einflussfaktoren identifizieren lassen, die einen Unfallablauf signifikant beeinflusst haben, und ob es Möglichkeiten zur Bewertung der Signifikanz solcher Einflussfaktoren gibt. Dabei sollte auch geprüft werden, welche organisatorischen Einflussfaktoren gegebenenfalls positive Auswirkungen auf die Beherrschung, auf Notfallmaßnahmen oder auf die Begrenzung von Umweltauswirkungen hatten.

Im vorliegenden Bericht wird die Vorgehensweise zur Auswahl der Katastrophenereignisse dargestellt und anschließend werden die drei für eine detailliertere Analyse ausgewählten Katastrophenereignisse vorgestellt. Eine genauere Betrachtung dieser Katastrophen ist im separaten Technischen Fachbericht /GRS-A-3892/ dargestellt. Es werden die identifizierten Merkmale aufgeführt, ihre Signifikanz für Entstehung und Beherrschung der Katastrophen dargestellt und ihre Übertragbarkeit auf den Nuklearbereich sowie deren Eignung zur Bewertung von Organisationen diskutiert.

Zur Durchführung der Vorstudie wurde folgende Vorgehensweise entwickelt:

- Auswahl der zu untersuchenden Katastrophenereignisse

  a) Aufstellung einer Liste grundsätzlich für die Untersuchung geeigneter Katastrophenereignisse

  b) Grobes Screening der zu diesen Katastrophenereignissen zur Verfügung stehenden Informationen

  c) Auswahl von drei Katastrophenereignissen, wobei nukleare und nichtnukleare Katastrophenereignisse einzubeziehen sind

- Ermittlung von signifikanten technologieübergreifenden organisatorischen Einflussfaktoren

  d) Umfassende Literaturrecherche für die drei ausgewählten Katastrophenereignisse

  e) Darstellung der wesentlichen Schritte der Unfallabläufe

  f) Auswertung der Literatur in Bezug auf Informationen über die technologieübergreifenden, charakteristischen organisatorischen Einflussfaktoren, die den Ablauf signifikant beeinflusst haben

- Darstellung und Diskussion der Einflussfaktoren

- Ableitung von Schlussfolgerungen

Zunächst wurden einige nukleare und nichtnukleare Katastrophenereignisse identifiziert, die für Zielstellung der Vorstudie generell geeignet wären:

- Nuklearkatastrophe von Tschernobyl am 26.04.1986,
- Nuklearkatastrophe von Fukushima am 11.03.2011,
- Unglück der Raumfähre Challenger am 28.01.1986,
- Unglück der Raumfähre Columbia am 01.02.2003,
- Unfall der Produktionsplattform Piper Alpha am 06.07.1988,
- Explosion der Bohrplattform Deepwater Horizon am 20.04.2010,
- Havarie der Fähre Herald of Free Enterprise 06.03.1987,
- Untergang der Fähre Jan Heweliusz am 14.01.1993,
- Untergang der Fähre Estonia am 28.09.1994,
- Havarie des Kreuzfahrtschiffes Costa Concordia am 13.01.2012,
- Kollision zweier Boeing 747 auf dem Flughafen Teneriffa Nord am 27.03.1977.

Nach einem Screening der zu den genannten Ereignissen mit geringem Aufwand zugänglichen Informationsquellen, insbesondere von GRS-Berichten, im Internet verfügbaren Informationen sowie verfügbaren Tagungsbeiträgen und unter Berücksichtigung der bei den Bearbeitern bereits vorliegenden Kenntnisse, wurden für eine weitergehende Untersuchung die Katastrophenereignisse des Schiffsunglücks der Costa Concordia, der Ölförderplattform „Deepwater Horizon“ und der Reaktorkatastrophe in Fukushima ausgewählt.

Zu den drei ausgewählten Katastrophenereignissen wurden umfangreichere Literaturrecherchen durchgeführt. Dabei wurden die mit im Rahmen dieser Vorstudie zur Verfügung stehenden Ressourcen zugänglichen und auswertbaren Informationsquellen ermittelt und analysiert. Dies umfasste insbesondere bereits existierende GRS-Berichte, im Internet frei verfügbare Informationen sowie bei der GRS verfügbare Tagungsbeiträge und Tagungsnotizen insbesondere der internationalen Konferenzen ANS PSA und PSAM.

Die Recherche ergab eine Vielzahl von Quellen:

- Für die Havarie der Costa Concordia wurden folgende Quellen ausgewertet: /BRÜ 14/, /DIL 12/, /EUC 12/, /MIN 12/, /MIN 12a/, /PIC 13/ und /RUS 13/.
- Für das Unglück der Deepwater Horizon wurden /BPD 10/, /BOE 11/, /DEE 11/, /FIN 11/, /GRA 11/, /HEL 13/, /HEN 11/, /NGU 08/, /NOR 12/ und /TIN 11/ detailliert betrachtet.
- Für die Katastrophe von Fukushima wurde /ATO 04/, /ACR 57/, /CON 07/, /CON 10/, /INT 07/, /OEC 13/, /OPE 11/, /RYU 13/ und /SPE 11/ analysiert.

Hierbei wurde die Katastrophe der Costa Concordia mit größerer Tiefe und insbesondere Breite als die beiden anderen Katastrophen analysiert. Während bei der Costa Concordia versucht wurde, sowohl die organisatorischen Eigenschaften als auch die Schritte des Ereignisablaufs, anhand derer sie wirksam wurden, möglichst vollständig zu erfassen (d. h. auch wenn dasselbe Merkmal mehrfach wirksam war, wurde dies berücksichtigt), wurde bei den beiden anderen Ereignissen keine vollständige Betrachtung sämtlicher Einwirkpunkte der organisatorischen Eigenschaften angestrebt. Es wurde vielmehr untersucht, ob die bei der Costa Concordia identifizierten Eigenschaften auch hier vorlagen und ob sich weitere, bei der Costa Concordia noch nicht identifizierte Merkmale, erkennen lassen.

Insgesamt wurden folgende Merkmale identifiziert:

- Duldung von Nichtkonformitäten
- Fehlende oder unangemessene Regeln zum Umgang mit Abweichungen
- Führungskultur unterstützt die Äußerung von Sicherheitsbedenken nicht
- Kommunikationsdefizite
- Keine Priorisierung von Sicherheit bei Entscheidungen, insbesondere
  - Eingehen vermeidbarer Risiken
  - Priorisierung von Kosten oder Schnelligkeit gegenüber Sicherheit
- Unterlassen notwendiger Entscheidungen
- Fehlende oder mangelhafte Durchführung von Notfallübungen
- Ungenügende Anforderungen

Diese organisatorischen Merkmale sind nicht unabhängig, sondern miteinander verknüpft. So ist z. B. das Merkmal, dass die Führungskultur die Äußerung von Sicherheitsbedenken nicht unterstützt, eng mit mangelnder Priorisierung von Sicherheit bei Entscheidungen sowie mit Defiziten in der Kommunikation verknüpft.

Diese Merkmale und ihre Signifikanz für die katastrophalen Ereignisse werden in den folgenden Abschnitten näher diskutiert.

Es ist hier zu betonen, dass die Merkmale auf einer in Umfang und Tiefe inhomogener und eingeschränkter Auswertung weniger Ereignisse basieren. Nicht alle Merkmale konnten bei allen Katastrophen nachgewiesen werden. Weitere vertiefte Analysen sind erforderlich, bevor erwogen werden kann, sie im Rahmen von Bewertungen von organisationalen Einflüssen anzuwenden.

Duldung von Nichtkonformitäten

Beim Unfall der Costa Concordia lassen sich mehrere Regelabweichungen identifizieren, die von der Organisation geduldet wurden:

- Zum einen wurde die ursprünglich vorgesehene Route modifiziert, indem eine nahe Vorbeifahrt an der Insel Giglio vorgesehen wurde. Solche Vorbeifahrten waren eine häufig geübte Praxis (so genannter „Bückling“, italienisch „inchino“). Diese Abweichung ist eine wesentliche Ursache für die Entstehung der Katastrophe.
- Bei der Planung der abweichenden Route stand kein geeignetes, ausreichend detailliertes Kartenmaterial zur Verfügung, da die Modifikation der Route durch den Kapitän erst zu einem Zeitpunkt veranlasste wurde, als kein weiteres geeigneteres Kartenmaterial beschafft werden konnte. Der für die Routenplanung zuständige Offizier plante die neue Route dennoch. Diese Abweichung begünstigte die Entstehung der Katastrophe.

Weitere beitragende Faktoren waren:

- Der Kapitän übernahm die Führung des Schiffes ohne eine vorgeschriebene formelle Übernahme.
- Der Voyage Data Recorder (VDR) war teilweise unverfügbar. Eine Fahrt mit nicht verfügbarem VDR ist nicht zulässig.

- Auf der Kommandobrücke befanden sich regelmäßig Personen, deren Aufenthalt dort nicht vorgesehen war.

Diese Nichtkonformitäten haben die Entstehung der Katastrophe nicht oder nur sehr mittelbar beeinflusst.

Durch Fehlverhalten bei der Evakuierung von geflüchteten Besatzungsmitgliedern aus Kompartimenten, welche geflutet wurden, entstanden unzulässige Verbindungen durch Türen, die diese verschiedenen Kompartimente wasserdicht voneinander trennen sollten. Dies ist nicht vorgesehen, da dadurch die Voraussetzung für die Beherrschung eines Lecks, für welches das Schiff ausgelegt ist, nämlich die zwingend erforderliche Trennung der Kompartimente, nicht gegeben ist. Es sind deshalb überflutete Kompartimente nur über *Notausstiege* nach oben zu verlassen. Dieses Fehlverhalten hat somit potentiell hohe sicherheitstechnische Bedeutung. Bei dem Unglück der Costa Concordia waren die Auswirkungen allerdings vernachlässigbar, da die Türen in allen Fällen wieder schlossen und die Menge Wasser, die während der Öffnung der Türen durch sie durchfließen konnte, so gering war, dass die Auswirkungen auf den Unfallablauf unwesentlich waren. Darüber hinaus hatte das Leck die Auslegung in einem solchen Maß überschritten, dass selbst vollständig dichte Schotten (Kompartimente) das Kentern nicht hätten verhindern können.

Auch beim Unfall der Deepwater Horizon und der Katastrophe von Fukushima wurden Nichtkonformitäten identifiziert. Diese umfassen z. B. bei der Deepwater Horizon die Verwendung ungeeigneten Zementes und die Nichtverfügbarkeit der Blowout-Preventer-Einrichtung. In der Anlage Fukushima waren vor dem Ereignis wiederholt Prüfungen sicherheitsrelevanter Komponenten nicht durchgeführt und einige Prüfergebnisse sogar gefälscht worden.

Zusammenfassend lässt sich sagen, dass Nichtkonformitäten als unmittelbare Ereignisursache nachgewiesen worden sind. Bei allen drei betrachteten Organisationen wurden Nichtkonformitäten geduldet. Die Duldung von Nichtkonformitäten ist nicht nur bei der Entstehung von katastrophalen Ereignissen zu beobachten. Dieses Merkmal ist auch erfassbar, wenn kein katastrophales Ereignis eingetreten ist. Dieses Merkmal ist ohne Einschränkung auf den kerntechnischen Bereich übertragbar.

Fehlende oder unangemessene Regeln zum Umgang mit Abweichungen

- Auf der Costa Concordia wurde von dem geplanten Kurs abgewichen. Hierfür existierte keine beschriebene Vorgehensweise.
- Bei der Bohrung der Deepwater Horizon wurde an mehreren Stellen von der ursprünglich vorgesehenen Vorgehensweise bzw. den vorgesehenen Anforderungen abgewichen, ohne dass hierzu wohldefinierte Prozessvorschriften vorlagen.

Dies hat mittelbar zu der Entstehung der Katastrophen beigetragen. Bei der Reaktorkatastrophe in Fukushima wurde dieses Merkmal nicht gefunden.

Dieses Merkmal ist auch erfassbar, wenn keine katastrophalen Ereignisse eingetreten sind. Es ist auf den kerntechnischen Bereich übertragbar.

Führungskultur unterstützt die Äußerung von Sicherheitsbedenken nicht

Im Falle der Costa Concordia ist bekannt, dass sowohl bei der Umplanung der Route als auch bei der Navigation keine Sicherheitsbedenken von Offizieren geäußert wurden. Mehreren Dokumenten ist zu entnehmen, dass der Kapitän einen autoritären Führungsstil hatte, der der Äußerung von Bedenken oder gar Widerspruch keinen Raum gab.

In den Berichten der Deepwater Horizon gibt es Anhaltspunkte, dass Sicherheitsbedenken des Personals nicht willkommen waren und nicht angemessen berücksichtigt wurden.

Die japanische Kultur und der Unfallablauf in Fukushima lassen darauf schließen, dass Sicherheitsbedenken gegenüber Vorgesetzten zwar geäußert worden sind, aber die Umsetzung von Maßnahmen nicht erfolgte. Eigenverantwortliche Entscheidungen wurden selten getroffen.

Die Äußerung von Sicherheitsbedenken hätte bei diesen katastrophalen Ereignissen mittelbar die Katastrophe verhindern können, wenn adäquat darauf reagiert worden wäre.

Dieses Merkmal ist auf den kerntechnischen Bereich übertragbar.

Kommunikationsdefizite

An der Entstehung und den Verlauf des Unfalls der Costa Concordia waren verschiedene Defizite bei der Kommunikation beteiligt. Der Verlauf der Evakuierung wurde aufgrund von Kommunikationsdefiziten, u. a. aufgrund der unterschiedlich ausgeprägten Fähigkeiten in Bezug auf Sprach- bzw. Fremdsprachenkenntnisse der Mannschaftsmitglieder, negativ beeinflusst. Kommunikationsprobleme zwischen Kapitän und Steuermann haben zur Entstehung des Unglücks beigetragen, indem sie zu einer falschen bzw. verzögerten Ausführung von Anweisungen führten. Es ist ebenfalls davon auszugehen, dass die Entscheidung der Leitung der Reederei Costa Crociere, die sicherheitsrelevante Dokumentation ausschließlich in italienischer Sprache zu verfassen, die Kommunikation ihrer Inhalte aufgrund der unterschiedlichen Sprachkenntnisse der Mannschaft negativ beeinflusst hat.

Auch für die Entstehung der Explosion der Deepwater Horizon hatten Kommunikationsdefizite eine erhebliche Bedeutung, u. a. die Ergebnisse von Untersuchungen eines Auftragnehmers zum verwendeten Zement wurden in ungeeigneter, schwer zugänglicher Form mitgeteilt, und deshalb nicht wahrgenommen.

Aufgrund der Verflechtungen in der japanischen Aufsichts- und Gutachterstruktur gab es auch dort Kommunikationspannen, die zu Verzögerungen bei der Unfallbewältigung im Kernkraftwerk Fukushima geführt haben.

Das Phänomen, dass Kommunikationsdefizite Ereignisabläufe beeinflussen, ist auch aus Kernkraftwerken bekannt. Ein Beispiel hierfür ist das Brandereignis im Kernkraftwerk Krümmel (Meldepflichtiges Ereignis 2007/058).

Keine Priorisierung von Sicherheit bei Entscheidungen

Bei den betrachteten Katastrophen wurde von den verantwortlichen Organisationen keine eindeutige Priorisierung von Sicherheit bei Entscheidungen vorgenommen. Dies führte zum Eingehen vermeidbarer Risiken und zur Priorisierung von Kosten und/oder Schnelligkeit bei der Entscheidungsfindung gegenüber der notwendigen Sicherheit.

Bei der Costa Concordia wurde von dem geplanten Kurs zugunsten eines Kurses sehr nahe der Insel Giglio abgewichen. Dies war wesentlich für die Entstehung der Katastrophe.

Es sind weitere Vorfälle dokumentiert, die darauf hinweisen, dass seitens der Schiffsführung der Costa Concordia der Sicherheit keine klare Priorität eingeräumt wurde:

- Mehrmaliges grundloses sehr nahes Vorbeifahren an anderen Schiffen,
- Auslaufen aus dem Hafen Marseille im Dezember 2011 bei starkem Sturm trotz Verbot des Hafenmeisters.

Darüber hinaus führte die oben bereits erwähnte Wahl von Italienisch als Sprache für die sicherheitsrelevante Dokumentation zwar zu einem geringeren Aufwand bei der Erstellung und Genehmigung, jedoch ist davon auszugehen, dass dies zu Lasten der Sicherheitsaspekte ging und diese mittelbar negativ beeinflusst wurden, da die Kommunikation und das Verständnis wichtiger Inhalte aufgrund der mangelnden Italienischkenntnisse der Mannschaft erschwert wurden.

Im Fall des Unfalls der Deepwater Horizon wurden systematisch Kostenerwägungen und Zeitbedarf prioritär gegenüber der Sicherheit behandelt.

Mehrere wissenschaftliche Untersuchungen ergaben, dass bei der weit überwiegenden Zahl wesentlicher Entscheidungen im Vorlauf der Katastrophe, sicherheitstechnisch vorteilhaftere Alternativen zugunsten zeit -bzw. kostensparenden Alternativen verworfen wurden. Diese Entscheidungen haben das Entstehen des katastrophalen Ereignisses ermöglicht.

Darüber hinaus wurde der vorbeugenden Instandhaltung technischer Einrichtungen keine ausreichend hohe Priorität eingeräumt. Die vorbeugende Instandhaltung führt unmittelbar und mittelbar zu Kosten, da Einrichtungen für die Zeit der Instandhaltung nicht zur Verfügung stehen, was einen Zeitverlust verursacht. Multiples Versagen technischer Einrichtungen war für den ungünstigen Verlauf wesentlich. Die Zuverlässigkeit technischer Einrichtungen ist eng mit Intensität und Qualität vorbeugender Instandhaltung verknüpft.

Die Erkenntnisse aus dem Unfallablauf von Fukushima lassen bspw. den Schluss zu, dass die Unsicherheit des Betreibers bei der Entscheidungsfindung zur Venting-Maßnahme eine stark hierarchisch ausgeprägte Vorgehensweise als Ursache hatte und dadurch Zeitverzögerungen entstanden sind.

Dieses Merkmal ist prinzipiell auch erfassbar, wenn keine Katastrophe eingetreten ist; es ist auf den Nuklearbereich übertragbar.

Nicht-Treffen notwendiger Entscheidungen

Sowohl während der Katastrophe der Costa Concordia als auch der von Fukushima wurden notwendige Entscheidungen zur Mitigation der Ereignisfolgen nur verzögert getroffen. Beim Unglück der Costa Concordia wurde die Evakuierung des Schiffs deutlich verzögert angeordnet. Es ist davon auszugehen, dass die Anzahl der Todesopfer geringer gewesen wäre, wenn die Evakuierung unmittelbar nach Vorliegen der für diese Entscheidung notwendigen Informationen beschlossen worden wäre.

Auch bei der Deepwater Horizon lässt sich dieses Merkmal feststellen. Eine Ableitung der austretenden Stoffe ins Meer unterblieb. Dies war für den Unfallablauf wesentlich. Die Katastrophe hätte vermieden werden können, wenn anstehende Entscheidungen zeitnah getroffen worden wären.

Dieses Merkmal ist auf den kerntechnischen Bereich übertragbar.

Die Fragestellung, ob und ggf. wie Beinahe-Unfälle erfasst werden können, also kein tatsächlich katastrophales oder vom üblichen Betrieb wesentlich abweichendes Ereignis eingetreten ist, ist noch zu untersuchen. Als Informationsquelle könnte z. B. der Verlauf von Übungen betrachtet werden. Hierbei wäre allerdings zu berücksichtigen, dass der Kontext für die Entscheidungsträger in Übungen anders ist als bei tatsächlichen Katastrophen.

Durchführung von Notfallübungen

Sowohl im Vorfeld der Katastrophe der Costa Concordia, als auch der Deepwater Horizon bzw. Fukushima wurden vom Betreiber regelmäßig und erfolgreich Übungen durchgeführt. Inwieweit diese Übungen bei der Costa Concordia einen noch ungünstigeren Verlauf verhindert haben, kann den vorliegenden Dokumenten nicht entnommen werden.

Bei der Deepwater Horizon wurden auch regelmäßige Notfallübungen durchgeführt. Diese wiesen jedoch mehrere Schwächen auf:

- Es gab keine unangekündigten Übungen.
- Einige relevante Unfallszenarien wurden nicht geübt.
- Bei den durchgeführten Übungen wurden nicht alle von den jeweiligen Ereignisverläufen betroffenen Personen beteiligt.

Diese Defizite werden in der untersuchten Literatur mit Fehlhandlungen des Personals während des Unfallgeschehens in Verbindung gebracht. Die Notfallorganisation des Betreibers an Land war auf ein katastrophales Ereignis dieser Größenordnung nicht vorbereitet – entsprechende Übungen waren nicht durchgeführt worden.

Als positives Resultat praktizierter Notfallübungen wurde in Fukushima erfolgreich das Anlagenpersonal vor Eintreffen der Tsunami evakuiert. Weitere positive Auswirkungen der durchgeführten Übungen sind aus den betrachteten Unterlagen nicht nachweisbar.

Ein erheblicher Einfluss dieses Merkmals erscheint sehr plausibel; seine Signifikanz für die positive bzw. negative Beeinflussung einer Katastrophenentstehung und auch Beherrschung ist aber aus den untersuchten Dokumenten nicht eindeutig nachweisbar und muss noch vertieft untersucht werden.

Dieses Merkmal ist grundsätzlich auch erfassbar, wenn keine Katastrophe eingetreten ist. Allerdings lässt sich die Vollständigkeit und Realitätsnähe von geübten Szenarien erst abschließend beurteilen, wenn tatsächlich entsprechende Katastrophen eingetreten sind.

Dieses Merkmal ist auf den Nuklearbereich übertragbar.

Ungenügende Anforderungen

Ein weiteres bei den Katastrophen identifiziertes Merkmal sind ungenügende Anforderungen an Technik, Organisation, Nachweise usw.

Sowohl im Fall von Deepwater Horizon als auch bei Fukushima sind unzureichende Anforderungen an die technischen Systeme wesentliche Ursache der Katastrophen.

Bei der Deepwater Horizon waren die Anforderungen an die Blow Out Preventer-Einrichtung so gering, dass keine Funktion dieser Komponente mit hoher Zuverlässigkeit gesichert war. Die Abscherbacken dieser Einrichtung funktionierten nicht bei allen Positionen des Bohrgestänges. Zusätzliche Auslösemechanismen, die in anderen Ländern vorgeschrieben sind, waren nicht gefordert. Der Automatisierungsgrad sicherheitsrelevanter Maßnahmen war bei der Deepwater Horizon sehr gering, obwohl viele Maßnahmen automatisierbar wären. Dies steht im Gegensatz zu international üblichen Anforderungen an Kernkraftwerke, wo sicherheitstechnisch erforderliche Handmaßnahmen im Allgemeinen nicht zulässig sind, wenn sie kurzfristig (typischerweise binnen 30 min) erfolgen müssten.

In Fukushima waren die Anforderungen an Nachweise bezüglich Tsunami und Erdbeben nicht adäquat. So wurde zur Festlegung der Auslegung gegen Tsunami nur auf die Erfahrung ab 1896 herangezogen. Frühere, wesentlich höhere Tsunamis, wurden nicht berücksichtigt.

Für diese Defizite sind nur teilweise die Betreiberorganisationen verantwortlich. Sie liegen im Wesentlichen im Verantwortungsbereich der staatlichen Aufsicht.

Im Nachgang der Katastrophenereignisse wurden wesentliche organisatorische Änderungen der Aufsicht von kerntechnischen Anlagen in Japan bzw. der Offshore-Ölindustrie in den USA vorgenommen.

Dieses Merkmal spielte bei dem Unglück der Costa Concordia keine wesentliche Rolle. So hat zwar die Größe des Lecks die Auslegung des Schiffes überschritten. Es ist allerdings technisch unmöglich, Schiffe auf beliebig große Lecks auszulegen. Die vorliegende Auslegung wird daher nach wie vor als angemessen angesehen.

Darüber hinaus waren die wasserdichten Schotten so angeordnet, dass mehrere Türen ständig offenstehen mussten, um Arbeitsabläufe nicht erheblich zu erschweren. Dies war von der Aufsichtsbehörde genehmigt worden. Das ständige Offenstehen beinhaltet das Risiko des Versagens der Kompartimentenabtrennung im Falle eines Schließversagens der Türen. Allerdings ist dieses Risiko eher gering, so dass die Änderung entsprechender Anforderungen zu keinem wesentlichen Sicherheitszuwachs führen würde. Beim vorliegenden Unglück funktionierten die Türen auslegungsgemäß, so dass hier kein Einfluss auf den Unfallablauf gegeben war.

Die anhand der verfügbaren Informationsquellen im Rahmen der Vorstudie durchgeführte Untersuchung ergab, dass aus den zugänglichen Informationsquellen, in ihrer Signifikanz bewertbare und grundsätzlich auch auf Kernkraftwerke übertragbare organisatorische Einflussfaktoren identifiziert werden konnten, welche die Entstehung und den Verlauf der Katastrophen beeinflussten.

Die meisten Einflussfaktoren können auch erfasst werden, wenn kein katastrophales Ereignis aufgetreten ist und sind somit prinzipiell geeignet, um organisatorische Einflüsse zu bewerten.

4 Zusammenfassung und Ausblick

4.1 Methode für die Analyse und Bewertung einer fortschrittlichen Mensch-Maschine-Schnittstelle

Das Ziel der Methodenentwicklung wurde erreicht: Es liegt eine fachlich begründete Methode für die Analyse und Bewertung der Zuverlässigkeit vor, mit der das Personal in Kernkraftwerken innerhalb oder außerhalb der Leitwarte sicherheitsrelevante Prozesse über Benutzungsoberflächen überwacht und führt, die mit Hilfe moderner Computer- und Bildschirmtechnologie und den zugehörigen Bedieneinrichtungen realisiert sind. Der Anwendungsbereich der Methode ist umfassend. Sie unterliegt keinen Einschränkungen dadurch, dass die Methode auf Warten z. B. einer bestimmten Kraftwerksbaulinie zugeschnitten ist.

Der Bewertungsansatz der Methode stützt sich in einem erheblichen Umfang auf die umfassende und weltweit anerkannte Analyse- und Bewertungsmethode „Technique for Human Error Rate Prediction (THERP)“ /SWA 83/. Es wurde genau und ausführlich begründet, inwieweit die Daten aus THERP auch für die Zuverlässigkeitsbewertung nutzbar sind, wenn die Erfüllung sicherheitskritischer Aufgaben der Prozessüberwachung und Prozessführung mit den Informationen, Informations- und Bedieneinrichtungen einer rechner- und bildschirmbasierten Schnittstelle erfolgt.

Diese Methode wurde Experten des „Halden Reactor Project (HRP)“ zur kritischen Sichtung und Rückmeldung vorgelegt und hat eine sehr positive Gesamtbeurteilung erfahren. Zur Rückmeldung des HRP gehören konstruktive Anregungen, die umgesetzt worden sind, soweit dies im Rahmen der Enddokumentation noch möglich war.

Eine Weiterarbeit an der Methode sollte sich in erster Linie darauf konzentrieren, sie mit Daten aus Untersuchungen zu validieren, in denen Operateure sicherheitsrelevante Aufgaben mit Hilfe rechner- und bildschirmbasierter Benutzungsoberflächen bewältigt haben. Solche Untersuchungen können entweder an Simulatoren wie denjenigen des HRP oder, auf der Basis einschlägiger Betriebserfahrungen erfolgen, die in Kooperation mit geeigneten, auch internationalen Partnereinrichtungen gesammelt und mit geeigneten statistischen Methoden (/PRE 13/, /PRE 16/) ausgewertet werden.

4.2 CAMIC-Methode für die sicherheitstechnische Bewertung digitaler Leittechnik

Die Zielstellung des Teilvorhabens wurde erreicht, indem ein systematischer Ansatz zur sicherheitstechnischen Bewertung von PLD-basierter Leittechnik entwickelt wurde.

Die generelle Vorgehensweise der im Vorhaben entwickelten CAMIC-Methode entspricht dem zyklischen PDCA-Prozess /DIN 08/ und kann für unterschiedliche Zielstellungen (u. a. Auslegung einer Einrichtung, Bewertung des Ist-Zustandes, Implementierung neuer Funktionen) und für alle Lebenszyklusphasen einer leittechnischen Einrichtung oder eines Leittechnik-Systems eingesetzt werden.

Bei der CAMIC-Methode wird zunächst eine grobe Einschätzung der zu analysierenden oder zu bewertenden Situation (u. a. Screening der vorgelegten Dokumentation und Ermittlung des Sachstandes) vorgenommen. Anschließend werden geeignete Analyseschritte und Werkzeuge ausgewählt. Danach erfolgt die Analyse des Sachstandes und die Ermittlung möglicher unerwünschter Fehlerauswirkungen, bzw. Inkonsistenzen mit den gestellten regulatorischen und technischen Anforderungen.

Die Prozessschritte der CAMIC-Methode können abhängig von unterschiedlichen Randbedingungen maßgeschneidert gestaltet werden und somit die rasante Entwicklung der PLD-Technologie (u. a. Entwicklungswerkzeuge, Chip-Herstellungstechnologie, Erweitern des Funktionsumfangs) und die Anforderungen berücksichtigen.

Die modellbasierte Erprobung der CAMIC-Methode ermittelte einige bewertungsrelevante Aspekte die bei der Weiterentwicklung der CAMIC-Methode berücksichtigt werden sollten:

- Implementierung einer durchgehend rechnergestützten Führung der PDCA-Schritte, um die Konsistenz und Nachvollziehbarkeit der Analyseergebnisse jederzeit zu gewährleisten.
  - Hierzu müssen die Entscheidungsdiagramme, die Eingabe- und Ausgabeinformationen und Zwischenergebnisse rechnergestützt verknüpft werden,
  - Datenbankbasierte Unterstützung von Entscheidungen und deren Nachvollziehbarkeit.

- Die Schnittstellen zum Einsatz von Analysewerkzeugen sollen hinsichtlich der Spezifikation von Analysen/Analysetechniken (u. a. Analyseziele, Annahmen, zeitabhängige oder statische Abläufe) verbessert werden. Hierzu sollen auch Entscheidungskriterien entwickelt werden, um die Nachvollziehbarkeit der Analyse und die Akzeptanz durch Ergebnisse zu verbessern.
- Die bisher im Vorhaben eingesetzte modellbasierte Vorgehensweise für die Erprobung der CAMIC-Methode sollte bei der Weiterentwicklung anhand der Bewertung realer leittechnischer Einrichtungen validiert werden.

Im geplanten Nachfolgevorhaben soll für die CAMIC-Methode ein rechnergestütztes Werkzeug entwickelt werden, das die in den verschiedenen Phasen der CAMIC-Methode durchzuführenden Bewertungsschritte unterstützt.

Wesentlich bei der Bewertung von sicherheitstechnisch wichtigen Einrichtungen sind die Anforderungen der jeweils anzuwendenden Regelwerke, Standards und Normen. Diese müssen derzeit beim Einsatz der CAMIC-Methode zu jeder Fragestellung neu recherchiert und die jeweils für die Fragestellung anzuwendenden Anforderungen ermittelt werden. Im Nachfolgevorhaben soll für die auf digitale Leittechnik anzuwendenden nationalen und internationalen Regelwerke und Normen eine systematisierte Abfrage entwickelt werden, die zu verschiedenen Fragestellungen die relevanten Anforderungen automatisiert ausgibt. Hierbei werden unter anderem die in /GRS 16a/ bereits erzielten Ergebnisse zu Anforderungen an Software herangezogen.

4.3 Vorstudien zur Weiterentwicklung von Methoden zu Bewertung personell-organisatorischer Einflüsse

4.3.1 Teilvorhaben „Vorstudie zu Methoden für die qualitative und quantitative Bewertung des Beitrags einer Sicherheitskultur zum sicheren Betrieb“

Die Zielstellung der Vorstudie zur Bewertung personell-organisatorischer Einflüsse wurde erreicht, wobei ein Konzept und ein Arbeitsplan für die Entwicklung einer Methode zur quantitativen Bewertung personell-organisatorischer Einflüsse entwickelt wurde. Aus den Entwicklungsarbeiten soll ein Quantifizierungsansatz hervorgehen, der mit dem nationalen und internationalen Regelwerk zur kerntechnischen Sicherheitskultur in Einklang steht und die Beiträge erfasst, die sicherheitskulturelle Faktoren nach

dem heutigen fachwissenschaftlichen Erkenntnisstand zur Zuverlässigkeit sicherheitstechnisch bedeutsamer Aktionen leisten. Die wesentlichen Quellen dieser Beiträge werden die (realisierte oder unterlassene) Umsetzung sicherheitskultureller Faktoren (siehe Tab. 3.2), die mögliche Lockerung fehlerträchtiger Abhängigkeiten zwischen Aktionen und die Intensivierung der sicherheitskulturell gebotenen Führungs- und Kontrollaufgaben bei den betrachteten Aktionen sein.

Zum Erfolg der zukünftigen Methodenentwicklung kann die Erkenntnis beitragen, dass im ersten Arbeitsschritt die bereits vorliegenden Daten für die Zuverlässigkeitsbewertung (THERP) verwendet werden können und dass der im Vorhaben entwickelte Ansatz einer systematischen begründeten Übertragung dieser Daten auf sicherheitskulturelle Faktoren beruht.

Fachliche Grundlagen, Entwicklungsschritte und erwartetes Ergebnis der im Konzept vorgesehenen Arbeiten wurden im Technischen Bericht /GRS-A-3891/ erläutert und im Detail dokumentiert.

Teilvorhaben „Vorstudie zur Bewertung der Auswirkungen organisatorischer Einflussfaktoren“

Die im Rahmen der Vorstudie zur Bewertung der Auswirkungen organisatorischer Einflussfaktoren durchgeführte Untersuchung ergab, dass aus den zugänglichen Informationsquellen in ihrer Signifikanz bewertbare organisatorische Einflussfaktoren identifiziert werden konnten, die die Entstehung und den Verlauf einer Katastrophe beeinflussten. Ihr signifikanter Einfluss auf den Katastrophenverlauf konnte hier anhand der verfügbaren Informationsquellen belegt werden. Alle gefundenen Einflussfaktoren sind grundsätzlich auf die Kerntechnik übertragbar. Die meisten Einflussfaktoren können auch erfasst werden, wenn kein katastrophales Ereignis aufgetreten ist und sind somit prinzipiell geeignet, um organisatorische Einflüsse in Kernkraftwerken zu bewerten.

Die gewonnenen Erkenntnisse legten es nahe, in einer weiterführenden Studie umfassend und vertieft solche Einflussfaktoren zu ermitteln, zu charakterisieren und in Bezug auf ihre mögliche Sicherheitsrelevanz für den Betrieb kerntechnischer Anlagen zu diskutieren und zu bewerten. Es soll insbesondere untersucht werden, wie eine Menge von möglichst unabhängigen („orthogonalen“) Merkmalen definiert werden kann, deren

Ausprägung nach einem wohldefinierten Prozess erfassbar und bewertbar ist und in späterer Folge einen nachweisbaren Einfluss auf die Zuverlässigkeit hat.

Ein Projekt für eine solche Studie ist bereits konzipiert, beantragt und bewilligt. Daher ist bereits eine Untersuchung begonnen worden, wie eine Menge solcher möglichst unabhängiger („orthogonaler“) Merkmalen definiert werden kann, deren Ausprägung nach einem wohldefinierten Prozess erfassbar und bewertbar ist und in weiterer Folge einen nachweisbaren Einfluss auf die Zuverlässigkeit hat. Im Rahmen der Vorstudie wurde darüber hinaus erkennbar, dass Externe (behördliche Aufsicht, sonstige Stakeholder) erheblichen Einfluss auf die Ausbildung solcher Faktoren in Organisationen haben können. Auch dieser Aspekt soll in dem bereits begonnenen Projekt vertieft untersucht werden.

Referenzen

Die folgenden Berichte zu den Arbeitspaketen AP1, AP 2, AP 3.1 und AP 3.2 wurden als Technische Fachberichte innerhalb des Vorhabens RS1525 erstellt und stellen umfangreiche und detaillierte Teilberichte zu diesem Abschlussbericht für die entsprechenden Arbeitspakete dar:

AP 1:

GRS-A-3889 Fassmann, W., Petermeier, B., Beck, J. Preischl, W.
Technischer Fachbericht, Methode für die Analyse und Bewertung fortschrittlicher Mensch-Maschine-Schnittstellen, Gesellschaft für Anlagen und Reaktorsicherheit (GRS) gGmbH, Fertigstellung im 4. Quartal 2017.

AP 2:

GRS-A-3890 Jopen, M., Quester, C., Piljugin, E., Mbonjo, H., Sommer, D.,
Technischer Fachbericht, Zuverlässigkeitsbewertung digitaler leittechnischer Einrichtungen, Gesellschaft für Anlagen und Reaktorsicherheit (GRS) gGmbH, Fertigstellung im 4. Quartal 2017.

AP 3.1:

GRS-A-3891 Fassmann, W., Preischl, W.
Technischer Fachbericht, Vorstudie zu Methoden für die qualitative und quantitative Analyse des Beitrags der Sicherheitskultur zum sicheren Betrieb eines Kernkraftwerks, Gesellschaft für Anlagen und Reaktorsicherheit (GRS) gGmbH, Fertigstellung im 4. Quartal 2017.

AP 3.2:

GRS-A-3892 Forner, J., Stiller, J.C., Holtschmidt, H., Kreuser, A., Kull, H.,
Technischer Fachbericht, Vorstudie zur Analyse der Auswirkungen organisatorischer Einflussfaktoren auf die Auslösung und Beherrschung von Katastrophenereignissen, Gesellschaft für Anlagen und Reaktorsicherheit (GRS) gGmbH, Fertigstellung im 4. Quartal 2017.

Literaturverzeichnis

/ACR 57/ Act on Regulation of Nuclear Source Material, Nuclear Fuel Material and Reactors, (Act No. 166 of June 10, 1957).

/ALE 12/ Ale, B., et al: Modelling Risk in High Hazard Operations: Integrating Technical, Organizational and Cultural Factors, PSAM11-Esrel 2013, Helsinki, 25-28.06.2012.

/APA 07/ American Psychological Association (APA): Dictionary of Psychology, Washington: APA, 2007.

/ATO 04/ Atomic Energy Basic Act (Act No.186 of 1955), Latest revision: Act No. 155 of December 3, 2004.

/BMU 15/ Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit (BMUB): Sicherheitsanforderungen an Kernkraftwerke, Be-kannt¬machung vom 3. März 2015, BAnz AT 30.02.2015 B2

/BOE 11/ BOEMRY, N.N. Report regarding the causes of the April 20, 2010 Macondo well blowout. The Bureau of Ocean Energy Management, Regulation and Enforcement (BOEMRY), September 2011, Internet: http://docs.lib.noaa.gov/noaa_documents/DWH_IR/reports/dwhfinal.pdf

/BPD 10/ BP, Deepwater Horizon Accident Investigation Report, 09/2010.

/BRÜ 14/ Brühwiler, B., Rode, C., Risk NET Studie, Ursachenanalyse und Risiko-analyse der Humanfaktoren, Die Havarie der Costa Concordia, 2014, https://www.risknet.de/themen/risknews/die-havarie-der-costa-concordia/c3c8a918a39e8c65ccae4083a6c347b3/.

/CON 04/ Conrad, P. Organizational Citzienship Behavior, in: Schreyögg, G, Wender, A. von (Eds.) Handwörterbuch Unternehmensführung und Or-ganisation, 4. Auflage, Stuttgart: Schäffer-Poeschel Verlag, 2004, Spal-ten 1101-1107.

/CON 07/ Convention on Nuclear Safety – National Report of Japan for the Forth Review Meeting, 09/2007.

/CON 10/ Convention on Nuclear Safety – National Report of Japan for the Fifth Review Meeting, 09/2010.

/COW 04/ Cowing, M.M., et al.: Dynamic Modelling of the Tradeoff between Productivity and Safety in Critical Engineering Systems, Reliability Engineering and System Safety 86, 2004, 269-284.

/DEE 11/ Deepwater Horizon Study Group, Final Report on the Investigation of the Macondo Well Blowout, 03/2011.

/DIL 12/ Di Lieto, A., Costa Concordia, Anatomy of an organizational accident, Australian Maritime College, University of Tasmania, 2012Z http://www.enav-international.com/wosmedia/273/costaconcordiaanatomyofanorganisationalaccident.pdf.

/DIN 81/ Deutsches Institut für Normung (DIN) e. V.: Fehlerbaumanalyse – Teil 1: Methode und Bildzeichen. DIN 25424, September 1981.

/DIN 87/ Psychische Belastung und Beanspruchung, DIN 33405 Februar 1987.

/DIN 05/ Deutsches Institut für Normung (DIN) e. V.: Zuverlässigkeitsmanagement – Teil 3-1: Anwendungsleitfaden – Verfahren zur Analyse der Zuverlässigkeit – Leitfaden zur Methodik, DIN EN 60300-3-1:2005-05, Mai 2005.

/DIN 06/ Deutsches Institut für Normung (DIN) e. V.: Analysetechniken für die Funktionsfähigkeit von Systemen – Verfahren für die Fehlzustandsart- und -auswirkungsanalyse (FMEA); DIN IEC 60812:2006; November 2006.

/DIN 07/ Deutsches Institut für Normung (DIN) e. V.: Fehlzustandsbaumanalyse DIN IEC 61025:2006; August 2007.

/DIN 08/ Deutsches Institut für Normung (DIN) e. V.: Qualitätsmanagementsysteme – Anforderungen; DIN EN ISO 9001, Dezember 2008.

/DIN 11/ Deutsches Institut für Normung (DIN) e. V.: Funktionale Sicherheit sicherheitsbezogener elektrischer / elektronischer / programmierbarer elektronischer Systeme – Teil 1: Allgemeine Anforderungen. DIN EN 61508-1:2011-02. Februar 2011.

/DIN 13/ Deutsches Institut für Normung (DIN) e.V.: Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen; DIN EN 61513, September 2013.

/DIN 15/ Deutsches Institut für Normung (DIN) e. V.: Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Entwicklung HDL-programmierter integrierter Schaltkreise für Systeme, die Funktionen der Kategorie A ausführen. DIN EN 62566:2015-02. Februar 2015.

/DIN 15a/ Deutsches Institut für Normung (DIN) e. V.: Fehlerzustandsart- und –auswirkungsanalyse (FMEA), DIN EN 60812, Entwurf, August 2015.

/DYC 05/ Dyck, C. van, et al.: Organizational Error Management Culture and Its Impact on Performance: A Two Study Replication, Journal of Applied Psychology 90, 2005, 1228-1240.

/EUC 12/ European Union Civil Protection Team Report, Observation Mission Costa Concordia, Giglio Island, 2012, https://www.msb.se/Upload/Insats_och_beredskap/Brand_raddning/RITS/Concordia_ Mission_final_report.pdf.

/FAA 96/ Harrison, L., Landell, B.: Design, Test, and Certification Issues for Complex Integrated Circuits. US Federal Aviation Administration (FAA) DOT/FAA/AR-95/31. 1996.

/FIN 11/ Final Government Response to the Report of the Montara Commission of Inquiry, Commonwealth of Australia, ISBN 978-1-92-1812-37-8, Canberra, 2011.

/GAR 12/ Garber, R., Paté-Cormnell, E.: Shortcuts in Complex Engineering Systems: A Principal-Agent Approach to Risk Management, Risk Analysis 32, 2012, 836-854.

/GAS 02/ Habinc, S.: Lessons Learned from FPGA Developments. European Space Agency Contract Report, Gaisler Research. September 2002.

/GAS 09/ Gassino, J.: Introduction of Programmable Electronic Devices in nuclear safety systems: a new challenge in assessment. IRSN, EUROSAFE 2009, November 2009.

/GRA 11/ Graham, B., Reilly, W.K., Beinecke, F., Boesch, D.F., Garcia, T.D., Murray, C.A., Ulmer, F., Deepwater.- The Gulf Oil Disaster and the Future of Offshore Drilling. Report to the President. National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, January 2011, Internet: http://www.gpo.gov/fdsys/pkg/GPO-OILCOMMISSION/pdf/GPO-OILCOMMISSION.pdf

/GRS 10/ Faßmann, W., Hartung, J., Preischl, W.: Weiterentwicklung und Erprobung von Methoden und Werkzeugen für probabilistische Sicherheitsanalysen, GRS-A-3560, Köln: GRS, 2010.

/GRS 15/ GRS, Aufstellung von Kriterien und Kenngrößen zur deterministischen Prüfung der Eignung von Redesign-Komponenten für den Einsatz in der Sicherheitsleittechnik von Kernkraftwerken (3611R01355), März 2015.

/GRS 15a/ Faßmann, W., Beck. J.: Stand von Wissenschaft und Technik zur Erfassung und Beurteilung wesentlicher Merkmale der Sicherheitskultur, GRS-A-3795, Köln: GRS, 2015.

/GRS 15b/ Faßmann, W., Beck. J.: Leitfaden für die Erfassung und Beurteilung wesentlicher Merkmale der Sicherheitskultur deutscher Kernkraftwerke durch die Genehmigungs- und Aufsichtsbehörden, GRS-A-3792, Köln: GRS, 2015.

/GRS 16/ Faßmann, W., Beck, J., Preischl, W.: Erhaltung und Weiterentwicklung der Sicherheitskultur in Kernkraftwerken unter Berücksichtigung der aktuellen Randbedingungen der Kernenergienutzung in Deutschland, GRS-A-3862, Köln: GRS, 2016.

/GRS 16a/ Jopen, M., Quester, C., Römer, S., Sommer, D., Stiller, J.C., Ulrich, B. Zuverlässigkeitsbewertung unter neuen Anforderungen an Sicherheitsleittechnik in Kernkraftwerken: Analysen der Anwendungspraxis, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH GRS-441, Oktober 2016.

/HAC 14/ Hacker, W.: Allgemeine Arbeitspsychologie, 3. Aufl., Göttingen: Hogrefe Verlag, 2014.

/HAN 11/ Hansen, K. P.: Kultur und Kulturwissenschaft, 4. Aufl., Tübingen, Basel: A. Francke Verlag, 2011

/HEL 13/ Hellmann, M., Rempe, S., Schlüter, J., Die Katastrophe der Deepwater Horizont. – Eine Ursachenforschung im Kontext der Theorie der High Reliability Organisations.- Soziologisches Arbeitspapier Nr.34/2013, Technische Universität Dortmund, Hrgb. Hirsch- Kreisen/Weyer TU Dortmund, 10/2013, ISSN 1612-5355.

/HEN 11/ Henneke, D., Warner, Nichols, Nuclear PRA and Defense-in-Depth Insights into the Deepwater Horizon Accident, Proceedings of the ANS PSA 2011 International Topical Meeting on Probabilistic Safety Assessment and Analysis, Wilmington, NC, 03/2011.

/HOF 07/ Hoffman, B.J.et al.: Expanding the Criterion Domain? A Quantitative Review of the OCB Literature, Journal of Applied Psychology 92, 2007, 555-566.

/HÖG 01/ Högl, M., Gemuenden, H.G.: Teamwork Quality and the Success of Innovative Projects: A Theoretical Concept and Empirical Evidence, Organization Science 12, 2001, 435-449.

/HÖG 04/ Högl, M. et al.: Inter-team Coordination, Project Commitment and Teamwork in Multi-team R&D-Projects: A Longitudinal Study, Organization Science 15, 2004, 38-55.

/HRP 17/ Halden Reactor Project Hildebrandt, Mail an W. Fassmann vom 08.07.2017.

/IAE 07/ IAEA: Safety Glossary, Wien: IAEA, 2007.

/IAE 09/ IAEA; The Management System for Nuclear Installations, Safety Guide No. GS-G-3.5, Wien, 2009.

/IAE 16/ International Atomic Energy Agency (IAEA): Application of Field Programmable Gate Arrays in Instrumentation and Control Systems of Nuclear Power Plants; IAEA Nuclear Energy Series, No. NP-T-3.17, Vienna 2016.

/IAE 91/ 75-INSAG 4, Safety Culture, Wien: IAEA, 1991.

/IEE 01/ IEEE: IEEE Standard Verilog Hardware Description Language. IEEE Computer Society. IEEE Std 1364-2001. 28.09.2001.

/IEE 08/ IEEE: IEEE Standard VHDL Language Reference Manual. IEEE Computer Society. IEEE Std 1076- 2008. 26.01.2009.

/INT 07/ Integrated Regulatory Review Service (IRRS) to Japan, Tokyo, 06/2007, http://www.nisa.meti.go.jp/genshiryoku/files/report.pdf

/KAT 13/ Kattermann, W.: In weniger Schritten zur Zertifizierung. elektroniknet.de, WEKA FACHMEDIEN GmbH. 03.07.2013.

/KES 13/ Kesel, F., Bartholomä, R.: Entwurf von digitalen Schaltungen und Systemen mit HDLs und FPGAs: Einführung mit VHDL und SystemC. ISBN-13: 978-3486589764. 12.06.2013.

/LEP 02/ LePine, J.A. et al.: The Nature and Dimensionality of Organizational Citizenship Behavior: A Critical Review and Meta-Analysis, Journal of Applied Psychology 87, 2002, 52-65.

/LIK 61/ Likert, R.: New Patterns of Management, New York (u. a): McGraw Hill, 1961.

/MIN 12/ Ministry of Infrastructure and Transport, Italian Maritime Investigative Body on Marine Accidents Marine Accident Investigation C/S Costa Concordia 13th January 2012, MSC90 London, 2012, http://www.ifsma.org/tempannounce/CostaConcordia.pdf

/MIN 12a/ Ministry of Infrastructures and Transports, Marine Casualties Investigative Body, Cruise Ship Costa Concordia, Marine casualties on 01/2012, Report on the safety technical investigation http://www.safety4sea.com/images/media/pdf/ Costa_Concordia_Full_Investigation_Report.pdf.

/MOH 12/ Mohaghegh, Z., et al.: Hybrid Incorporation of Social and Technical Failure Mechanisms in Probabilistic Risk Assessment, PSAM11-Esrel 2013, Helsinki, 25-28.06.2012.

/MUR 96/ Murphy, D.M., Paté-Cornell, E.: The SAM Framework: Modelling the Effects of Management Systems on Human Behavior in Risk Analysis, Risk Analysis 16, 1996, 501-515.

/NEA 15/ Nuclear Energy Agency: Failure modes taxonomy for reliability assessment of digital I&C systems for PRA. Committee on the safety of nuclear installations, NEA/CSNI/R(2014)16. 16.02.2015

/NGU 08/ Nguyen, T. Handbuch der wert- und risikoorientierten Steuerung von Versicherungsunternehmen.-529 S., Verl. Versicherungswirtschaft GmbH, Karlsruhe 2008, ISBN 13: 978-3-89952-344-7.

/NOR 12/ Norwegian Oil Industry Association (OLF), Deepwater Horizon accident, lessons learned and follow-up, summary report, 06/2012.

/NRC 10/ Bobrek, M., Bouldin, D., Holcomb, D., Killough, S., Smith, S., Ward, C., Wood. R.T.: Review Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems. U.S. NRC, Office of Nuclear Regulatory Research, NUREG/CR-7006. Februar 2010.

/OEC 13/ OECD/NEA, The Fukushima Daiichi Nuclear Power Plant Accident: OECD/NEA Nuclear Safety Response and Lessons Learnt, OECD, NEA No. 7161, Paris, 2013.

/OPE 11/ Operational Status of Nuclear Facilities in Japan, 2011 Edition, Japan Nuclear Energy Safety Organization (JNES), ISSN 1347-0493.

/ORN 07/ Bobrek, M., Bouldin, D., Holcomb, D., Killough, S., Smith, S., Ward, C.: Survey of Field Programmable Gate Array Design Guides and Experience Relevant to Nuclear Power Plant Applications. ORNL/NRC/LTR-07/06, Oakridge. Juli 2007.

/PAR 14/ Park, J.: Investigating the TACOM measure as a general tool for quantifying the complexity of procedure guided tasks. Reliability Engineering & System Safety, 129, 66-75, 2014.

/PAT 96/ Paté-Cornell, E., Murphy, D.M. Human and Management Factors in Probabilistic Risk Analysis: The SAM Approach and Observations from Recent Applications, Reliability Engineering and System Safety 53, 1996, 115-126.

/PET 16/ Petermeier, B., Faßmann, W., Beck J.:
Method for analyzing operator interactions with computerized interfaces and their impact on process safety, PSAM 13, Seoul, 2.-7. October 2016.

/PIC 13/ Piccinelli, M., Gubian, P., Modern ships Voyage Data Recorders:
A forensics perspective on the Costa Concordia shipwreck,
Digital Investigation 10, 2013.

/POD 00/ Podsakoff, Ph., M. et al.: Organizational Citizenship Behavior: Critical Review of the Theoretical and Empirical Literature and Suggestions for Future Research, Journal of Management 26, 2000, 513-563.

/PRE 13/ Preischl, W., Hellmich, M.: Human error probabilities from operational experience of German nuclear power plants, Reliability Engineering and System Safety 10ß, 2013, 150-1598.

/PRE 16/ Preischl, W., Hellmich, M.: Human error probabilities from operational experience of German nuclear power plants, Part II, Reliability Engineering and System Safety 148, 2016, 44-58.

/REA 99/ Reason, J. Managing the Risks of Organizational Accidents, Aldershot (u. a.): Ashgate, 1999.

/RIC 14/ Richter, P., Hacker, W.: Belastung und Beanspruchung, 4. Aufl., Kroning: Asanger Verlag 2014.

/RUS 13/ Russell, P., The Sinking Sequence of M.V. Costa Concordia, Schriftenreihe Schiffbau A-44, Technische Universität Hamburg-Harburg, 2013.

/RYU 13/ Ryuji Kubota, JNES, International Experts' Meeting on Human and Organizational Factors in Nuclear Safety in the Light of the Accident at the Fukushima Daiichi NPP, IAEA, Wien, 2013.

/SAL 12/ Salvendy, G.: Handbook of human factors and ergonomics, 4. Aufl.. John Wiley & Sons, 2012.

/SMI 83/ Smith, C.A., et al.: Organizational Citizenship Behavior: Its Nature and Antecedents, Journal of Applied Psychology 68, 1983, 653-663.

/SPE 11/ Special Report on the Nuclear Accident at the Fukushima Daiichi Nuclear Power Station, INPO 11-005, Revision 0, 2011.

/STR 09/ Strohschneider, S., Heimann, R.: Kultur und sicheres Handeln, Verlag für Polizeiwissenschaft, Frankfurt, 2009.

/SUT 01/ Sutherland, S.: Using the new Verilog-2001 Standard, Part One: Modeling Designs. Sutherland HDL Inc. 2001.

/SWA 83/ Swain, A. D., Guttmann, H. E.: Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, Washington, (DC): U.S. NRC, 1983.

/TIN 11/ Tinmannsvilk, R.K., Bratveit, E., Carlson, M., Fylling, I., Hauge, S., Haugen, S. Hynne, H., Lundteigen, M.A., Moen, B.E., Okstad, E., Onshus, T., Sandvik, P.C., Oien, K., The Deepwater Horizon accident. Causes, lessons learned and recommendations for the Norwegian petroleum activity. Executive summary, SINTEF A19148-Apen, May 2011.

/ULl 11/ Ulich, E.: Arbeitspsychologie, 7. Aufl., Zürich, Stuttgart: vdf Verlag, Schaffer-Poeschel Verlag, 2011.

/WIE 07/ Wieland, J.: Die Ethik der Governance, Marburg: Metropolis Verlag, 2997

/WIL 91/ Williams, L.J., Anderson, S.E.: Job Satisfaction and Organizational Commitment as Predictors of Organizational Citizenship Behavior, Journal of Management 17, 1991, 601-617

Abkürzungsverzeichnis

ASIC	Application Specific Integrated Circuit
CAMIC	Cyclic Analytic Methodology for Instrumentation and Control
CCF	Common cause failure (Gemeinsam verursachter Ausfall)
CPLD	Complex Programmable Logic Device
FMEA	Failure mode and effect analysis (Fehlzustandsart- und -auswirkungsanalyse)
FPGA	Field Programmable Gate Array
FTA	Fault tree analysis (Fehlzustandsbaumanalyse)
GVA	Gemeinsam verursachter Ausfall
HAZOP	Hazard and Operability
HDL	Hardware Description Language
HRP	Halden Reactor Project
IC	Integrated Circuit
LT	Leittechnik
LTE	Leittechnische Einrichtung
OCB	Organizational Citizenship Behavior
PAAG	Prognose, Auffinden der Ursache, Abschätzen der Auswirkungen, Gegenmaßnahmen
PDCA	Plan, Do, Check, Act, Vorgehensweise
PIF	Performance Influencing Factors
PLD	Programmable Logic Device
PSF	Performance Shaping Factors
SoC	System-of-the-Chip
VDR	Voyage Data Recorder
Verilog	Verifying Logic
VHDL	VHSIC Hardware Description Language
VHSIC	Very High Speed Integrated Circuit

Abbildungsverzeichnis

Tabellenverzeichnis

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH

Schwertnergasse 1
50667 Köln
Telefon +49 221 2068-0
Telefax +49 221 2068-888

Boltzmannstraße 14
85748 Garching b. München
Telefon +49 89 32004-0
Telefax +49 89 32004-300

Kurfürstendamm 200
10719 Berlin
Telefon +49 30 88589-0
Telefax +49 30 88589-111

Theodor-Heuss-Straße 4
38122 Braunschweig
Telefon +49 531 8012-0
Telefax +49 531 8012-200

www.grs.de

ISBN 978-3-946607-43-4