Entwicklung einer Methode zur Bewertung von Vorkehrungen gegen potentielle Fehler bei Softwareänderungen sicherheitsrelevanter Leittechnik

GRS - 674

Gesellschaft für Anlagen-
und Reaktorsicherheit
(GRS) gGmbH

Entwicklung einer Methode zur Bewertung von Vorkehrungen gegen potentielle Fehler bei Softwareänderungen sicherheitsrelevanter Leittechnik

Felix Gärner
Henriette Gatz
Patrick Gebhardt
Hervé Mbonjo
Jaroslaw Shvab
Dagmar Sommer

März 2022

Anmerkung:

Das diesem Bericht zugrunde liegende Forschungsvorhaben wurde mit Mitteln des Bundesministeriums für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV) unter dem Förderkennzeichen 4719R01374 durchgeführt.

Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei der GRS.

Der Bericht gibt die Auffassung und Meinung der GRS wieder und muss nicht mit der Meinung des BMUV übereinstimmen.

GRS - 674
ISBN 978-3-949088-65-0

Deskriptoren

digitale Leittechniksysteme, ergonomische Auslegung, Interrelationsmodell,
Mensch-Maschine-Schnittstelle, Mensch-Maschine-System, Personalfehlhandlungen

Kurzfassung

Der vorliegende Bericht umfasst Ergebnisse, die im Rahmen des vom BMUV geförderten Forschungsvorhabens „Entwicklung einer Methode zur Bewertung von Vorkehrungen gegen potentielle Fehler bei Softwareänderungen sicherheitsrelevanter Leittechnik“ (Förderkennzeichen 4719R01374) erarbeitet wurden. Die Zielsetzung dieses Vorhabens lag darin, Ursachen für potenzielle Mängel von technischen Vorkehrungen gegen Personalfehlhandlungen an typischen Mensch-Maschine-Schnittstellen (MMS) digitaler Leittechniksysteme zu identifizieren und zu analysieren.

Hierfür wurde im Rahmen dieses Vorhabens eine Bewertungsmethode entwickelt, nachfolgend MEDIC (Method for Evaluation of HMI of Digital I&C Systems) genannt. Grundlage für die Bewertung von technischen Vorkehrungen an MMS mit MEDIC ist ein Interaktionsmodell, welches die Beziehungen zwischen den Komponenten des Mensch-Maschine-Systems, in dem die Mensch-Maschine-Schnittstelle eingebettet ist, berücksichtigt. Im Rahmen der MEDIC-Bewertung wird angenommen, dass die Eigenschaften dieser Beziehungen die Minimierung bzw. die Vermeidung von Personalfehlhandlungen an MMS maßgeblich mitbestimmen. Es wurden daher im Rahmen von MEDIC Attribute wie zum Beispiel Konsistenz oder Korrektheit, etc. zur Charakterisierung dieser Beziehungen eingeführt. Diese Attribute betreffen die allgemeine Ergonomie und Verständlichkeit der Mensch-Maschine-Schnittstelle. Gemäß der MEDIC-Bewertungsmethode sollen diese Attribute erfüllt werden, um Personalfehlhandlungen an MMS zu vermeiden bzw. zu minimieren.

Bei der Bewertung von technischen Vorkehrungen gegen Fehlhandlungen an MMS mit MEDIC wird anhand von Kriterien aus relevanten Regelwerken, Normen und Richtlinien wie zum Beispiel NUREG 0700 oder KTA überprüft, inwieweit die eingeführten Attribute zur Charakterisierung der Beziehungen zwischen den Komponenten des zugrunde liegenden Mensch-Maschine-Systems erfüllt sind.

Zur softwaregestützten Anwendung von MEDIC wurde im Rahmen des Vorhabens das aus mehreren eigenständigen Softwaretools bestehende MEDIC-Analysewerkzeug entwickelt.

Abstract

This report contains the results of a BMUV-funded research project (Promotion code 4719R01374). The goal of this project was to identify and to analyze potential deficiencies of technical precautions against human errors at typical human-machine interfaces (HMIs) of digital I&C systems.

For this purpose, a method was developed within the framework of this project, hereinafter referred to as MEDIC (Method for Evaluation of HMI of Digital I&C Systems). The basis for the evaluation of technical precautions at HMIs with MEDIC is an interrelation model that considers the interrelations between the components of the human-machine system in which the human-machine interface is embedded. Within the framework of the evaluation of HMIs with MEDIC, it is assumed that the characteristics of these interrelations are relevant to minimize or avoid personnel errors at HMIs. Therefore, attributes for the characterization of these interactions like consistency or correctness etc. have been introduced within the framework of MEDIC. These attributes concern the general ergonomics and comprehensibility of the human-machine interface. According to the MEDIC assessment, these attributes should apply to avoid or minimize personnel errors at HMIs.

For the evaluation of technical precautions against personnel errors at HMIs with MEDIC, criteria from relevant regulations, standards and guidelines like NUREG 0700 or KTA are used to check to what extent the attributes introduced for characterizing the interactions between the components of the underlying human-machine system apply.

For the software-supported application of MEDIC, the MEDIC analysis tool, consisting of several independent software tools, was developed within the framework of the project.

Inhaltsverzeichnis

1 Einleitung und Zielsetzung

Beim Betrieb und im Rahmen der Instandhaltung von softwarebasierten leittechnischen Einrichtungen kann es wiederholt erforderlich sein, Änderungen an ihren Komponenten vorzunehmen. Diese Änderungen betreffen sowohl die Hardware (z. B. Baugruppen für die Signalverarbeitung) als auch die Software (z. B. Anwendersoftware für die Realisierung der leittechnischen Funktionen) der softwarebasierten leittechnischen Einrichtungen. Sie ergeben sich beispielsweise aus Änderungen oder Ergänzungen der Aufgabenstellung der realisierten leittechnischen Funktionen, die zur Neugenerierung von Anwendersoftware führen, aus erforderlichen Änderungen von Anlagenparametern und/oder aus dem notwendigen Austausch von Baugruppen im Rahmen von Störungsbehebungen.

Die hierfür notwendigen Eingriffe in der Software- bzw. in der Hardware softwarebasierter leittechnischer Einrichtungen werden vom Wartungspersonal bzw. Bedienpersonal über sogenannte Mensch-Maschine-Schnittstellen (MMS), engl. Human-Machine-Interface (HMI), durchgeführt. Die Mensch-Maschine-Schnittstellen stellen demnach die Zugriffsmöglichkeiten des Bedienpersonals auf die leittechnischen Einrichtungen und Komponenten dar. Sie ermöglichen es einerseits den verfahrenstechnischen Prozess zu überwachen, zu beobachten und zu steuern und andererseits beim Betrieb und/oder im Rahmen von Instandhaltungen den Zustand softwarebasierter leittechnischer Einrichtungen über entsprechende Software- und/oder Hardwaremodifikationen zu verändern.

In Kernkraftwerken befinden sich die MMS zur Prozessüberwachung und -steuerung u. a. auf der Warte und/oder auf der Notsteuerstelle oder an den örtlichen Leitständen. Die MMS zur Systeminstandhaltung und -modifizierung sind in der Regel in den Leittechnikschränken (LT-Schränke) in den Schaltanlagenräumen, im Wartennebenraum oder an den Feldgeräten wie z. B. Messumformern, Schutzgeräten zwecks Parametrisierung installiert. Sie schließen auch die MMS mobiler Diagnosegeräte ein, welche über Stecker an die LT-Schränke angeschlossen werden.

Die MMS unterscheiden sich abhängig von der jeweils durchzuführenden Aufgabe (Prozessüberwachung, Prozesssteuerung, Systeminstandhaltung, Systemmodifizierung) in ihrer Art (Hardwarelösungen wie z. B. Einstellschalter an den Baugruppen oder Softwarelösungen wie z. B. die Entwicklungssoftware mit Anbindung an das softwarebasierte Leittechniksystem) und Ausführung (z. B. Bedien-/Anzeigetafel mit Eingabemöglichkeiten, graphische Bedienoberflächen, Servicerechner, Schlüsselschalter, Diagnosestecker). In den MMS softwarebasierter Leittechniksysteme können auch verschiedene technische Vorkehrungen (z. B. Alarme, Autokorrekturen, Blockierungen usw.) gegen mögliche Fehlhandlungen des Personals realisiert werden.

In den letzten Jahren wurden viele Forschungsaktivitäten initiiert, die sich mit sicherheitsrelevanten Wechselwirkungen zwischen softwarebasierter Leittechnik und der Zuverlässigkeit von Personalhandlungen an MMS beschäftigen /NUR 02/ /OEC 07/. Der Fokus dieser Aktivitäten liegt insbesondere im Bereich der MMS zur Bedienung softwarebasierter Leittechniksysteme auf der Warte und der Notsteuerstelle (digitale Warte). Die Ergebnisse aus diesen Forschungsarbeiten sind in verschiedene Richtlinien und Normen für die sicherheitstechnische Auslegung von Mensch-Maschine-Schnittstellen softwarebasierter Leittechniksysteme eingeflossen. Zum Beispiel werden in /NUR 02/ Aspekte des menschlichen Faktors bei der Auslegung von MMS digitaler Leittechniksysteme behandelt. Im Rahmen der kontinuierlichen Auswertung der Betriebserfahrung wurden Fälle identifiziert, in denen es zu Fehlbedienungen bzw. Fehlhandlungen von Bedienpersonal an MMS softwarebasierter Leittechniksystemen in Kernkraftwerken kam. Hierbei liefern Fehlbedienungen an den MMS bei der Durchführung von Änderungen an softwarebasierten Leittechniksystemen, z. B. im Rahmen von Instandhaltung und Systemmodifizierung/-änderung, ebenfalls einen Beitrag zu den beobachteten Ausfällen. Die beobachteten Fehlhandlungen bzw. Fehlbedienungen waren u. a. auf Mängel in der Auslegung der MMS (z. B. Fehler in der Ergonomie der MMS) zurückzuführen. In einigen Fällen kam es aufgrund der Fehlbedienungen des Personals zu Ausfällen der betroffenen softwarebasierten leittechnischen Einrichtungen. Abhängig von der sicherheitstechnischen Bedeutung der betroffenen Systeme können solche Fehlhandlungen an MMS softwarebasierter Leittechniksysteme die Sicherheit der Anlage beeinträchtigen. Das vorliegende Vorhaben zielt daher darauf ab, potenzielle Mängel technischer Vorkehrungen gegen Fehlhandlungen des Personals an typischen MMS digitaler Leittechniksysteme zu identifizieren und zu analysieren. Dazu werden folgende Punkte betrachtet:

- Ermittlung von technischen Vorkehrungen im Lebenszyklus eines typischen softwarebasierten Leittechniksystems gegen unzulässige, sicherheitsrelevante Auswirkungen von Bedienfehlern (Arbeitspaket 1),
- Konzeptentwicklung zur Analyse von Ursachen und Auswirkungen von potentiellen Fehlern an den MMS softwarebasierter Leittechniksysteme (Arbeitspaket 2),
- Entwicklung eines Analysewerkzeuges zur Bewertung von technischen Vorkehrungen in softwarebasierten Leittechniksystemen gegen potentielle Fehler an den MMS (Arbeitspaket 3).

Die drei Arbeitspakete (AP) dieses Vorhabens werden nachfolgend beschrieben.

1.1 Ermittlung von technischen Vorkehrungen in softwarebasierter Leittechnik gegen Fehler durch Personalhandlungen an MMS (AP 1)

Gegenstand des AP 1 ist die Ermittlung von technischen Vorkehrungen gegen Fehler durch Personalhandlungen an MMS softwarebasierter Leittechniksysteme. Hierzu wurde zunächst nach Normen und Richtlinien recherchiert, welche Anforderungen zur Vermeidung von Fehlern durch Personalhandlungen an MMS enthalten. Anschließend wurden die regulatorischen Anforderungen aus den identifizierten relevanten Normen und Richtlinien hinsichtlich technischer Vorkehrungen gegen Fehler durch Personalhandlungen an MMS softwarebasierter Leittechniksysteme ausgewertet. Betrachtet wurden hierbei insbesondere MMS zur Prozessüberwachung und -steuerung sowie MMS für Systeminstandhaltung und -modifizierung (z. B. im Rahmen von Änderungen).

Die in diesem AP 1 durchgeführten Arbeiten orientierten sich u. a. an folgenden Leitfragen:

- Welche technischen Vorkehrungen gegen Fehler durch Personalhandlungen sind in softwarebasierter Leittechnik insbesondere bei der Prozessüberwachung und -steuerung sowie im Rahmen von Systemänderungen laut regulatorischer Anforderungen umzusetzen?
- Welche Annahmen bezüglich der Fehlermöglichkeiten des Personals sind bei diesen technischen Vorkehrungen zugrunde gelegt?

Die Ergebnisse dieses Arbeitspakets sind im Kapitel 2 dokumentiert.

1.2 Konzeptentwicklung für ein Modell zur Analyse der Ursachen und Auswirkungen von potenziellen Fehlern durch Personalhandlungen an MMS softwarebasierter Leittechniksysteme (AP 2)

Ziel des Arbeitspaketes 2 ist es, ein Konzept für die Entwicklung eines Modells für eine Analyse der Ursachen und Auswirkungen von potenziellen Fehlern durch Personalhandlungen an MMS softwarebasierter Leittechniksysteme insbesondere für die Prozessüberwachung und -steuerung sowie im Rahmen von Systemänderungen (z. B. Instandhaltung, Änderung der Software, Reparatur/Austausch von Komponenten) zu erarbeiten. Auf Basis dieses Konzeptes sollen u. a. die Wechselwirkungen an den MMS softwarebasierter Leittechniksysteme im Hinblick auf die Bewertung von technischen Vorkehrungen gegen Fehler durch Personalhandlungen analysiert werden. Die Konzeption des Untersuchungsmodells orientiert sich an einem Arbeitssystem für die Modellierung der menschlichen Tätigkeit, wie es beispielsweise in /HAR 10/ beschrieben ist. Im Kapitel 2 wird das Arbeitssystem näher beschrieben.

Bei der Konzeptentwicklung für ein Modell zur Analyse der Ursachen und Auswirkungen von potentiellen Fehlern an MMS softwarebasierter Leittechniksysteme für die Prozessüberwachung und -steuerung sowie im Rahmen von Systemänderungen werden u. a. folgende Punkte betrachtet:

a) Identifizierung relevanter Tätigkeiten an den MMS des zu untersuchenden softwarebasierten Leittechniksystems mit zugehörigen Handlungsszenarien. Dies orientiert sich u. a. an den folgenden Leitfragen:

   - Welche Tätigkeiten sind im Rahmen der Prozessüberwachung und -steuerung sowie Systemänderungen (u. a. Update/Upgrade von Firmware im Rahmen von Instandhaltungsmaßnahmen, Betriebsartwechsel, Kalibrierung der Eingangssignale durch Korrekturwerte, Änderung von Einstellwerten in der Anwendersoftware, z. B. Grenzwerteinstellung) des zu untersuchenden softwarebasierten Leittechniksystems vorgesehen?

   - An welchen MMS werden diese Tätigkeiten durchgeführt?

   - Welche Handlungen und Anweisungen (Arbeitsanweisungen, Vorschriften und sonstige Unterlagen (Systembeschreibungen)) sind mit diesen Tätigkeiten verknüpft bzw. sind zu berücksichtigen?

b) Identifizierung des Fehlerpotentials durch Personalhandlungen an MMS softwarebasierter Leittechniksysteme:

   - Welche Fehlhandlungen durch das Personal sind bei der Durchführung der unter a) identifizierten Tätigkeiten zu unterstellen?
   - Welche im AP 1 identifizierten technischen Vorkehrungen gegen Fehlhandlungen durch das Personal sind zu berücksichtigen?

c) Spezifizierung des Konzepts für ein Modell zur Analyse der Ursachen und Auswirkungen von potentiellen Fehlern:

   Auf Basis der Erkenntnisse aus a) und b) wird eine Vorgehensweise zur Modellierung eines Arbeitssystems für eine Analyse der Ursachen und Auswirkungen von potentiellen Fehlern durch Personalhandlungen an MMS softwarebasierter Leittechniksysteme für die Prozessüberwachung und -steuerung sowie im Rahmen von Systemänderungen spezifiziert.

Die gewonnenen Erkenntnisse aus diesem Arbeitspaket wurden aufbereitet und sind im Kapitel 3 dieses Abschlussberichtes dokumentiert.

1.3 Entwicklung eines Analysewerkzeugs zur Bewertung von technischen Vorkehrungen in softwarebasierten Leittechniksystemen gegen Fehler durch Personalhandlungen an MMS (AP 3)

Ziel des AP 3 ist es, ein Analysewerkzeug zur Bewertung von technischen Vorkehrungen in softwarebasierten Leittechniksystemen gegen Fehler durch Personalhandlungen insbesondere für die Prozessüberwachung und -steuerung sowie im Rahmen von Systemänderungen zu entwickeln. Das Analysewerkzeug basiert auf der in AP 2 entwickelten Methode (siehe Kapitel 4), wobei Aspekte eines Arbeitssystems hinsichtlich Wechselwirkungen an MMS berücksichtigt werden. In einem ersten Schritt wird zunächst anhand von Fallbeispielen, z. B. für Änderungen an der Hard- und/oder Software eines softwarebasierten Leittechniksystems sowie für die Prozessüberwachung und -steuerung, ein Arbeitssystem als Grundlage für die Analyse entwickelt. Dies erfolgt durch Umsetzung des Konzepts aus AP 2. Bei der Festlegung der Fallbeispiele wird u. a. auf Erkenntnisse aus der Auswertung generischer Betriebserfahrung mit softwarebasierten Leittechniksystemen zurückgegriffen. Anschließend wird das Analysewerkzeug zur Bewertung von technischen Vorkehrungen in softwarebasierter Leittechnik gegen Fehler durch

Personalhandlungen an MMS schrittweise spezifiziert und realisiert. Es werden Bewertungskriterien zur Analyse der Wirksamkeit der relevanten technischen Vorkehrungen (z. B. Fehlererkennung, Barrieren gegen Fehlerausbreitung im System) für die ausgewählten Fallbeispiele entwickelt.

Hierbei werden u. a. Erkenntnisse aus AP 1 in Bezug auf technische Vorkehrungen gegen Fehler, z. B. regulatorische Anforderungen, berücksichtigt. Modellvarianten des Arbeitssystems werden entwickelt und als Bewertungsgrundlage herangezogen, um zu untersuchen, inwieweit die fehlervermeidenden und fehlerbeherrschenden Maßnahmen (z. B. Plausibilitätsprüfung von Eingaben, Signalvalidierung in der Anwendersoftware, Gestaltung der Eingabemasken) gegen die an MMS induzierten Fehler, z. B. für die Prozessüberwachung und -steuerung sowie im Rahmen von Systemänderungen, greifen. Die Modellvarianten des Arbeitssystems ergeben sich beispielsweise aus Modifikationen der MMS (u. a. Gestaltung der Eingabemasken, Rückmeldungen, durchzuführende Aufgabe an der MMS) und werden u. a. mittels der verfügbaren Entwicklungsumgebung von AnTeS[1] realisiert. Die Validierung des so entwickelten Arbeitssystems bestehend aus MMS, Arbeitsanweisungen für die durchzuführenden Tätigkeiten an der MMS mit zugehörigen Leittechnikfunktionen und Handlungsszenarien erfolgt hierbei iterativ, wobei in jedem Schritt die Bewertungskriterien hinsichtlich Wirksamkeit der zugrunde gelegten technischen Vorkehrungen gegen Fehler evaluiert werden.

Als Ergebnis von AP 3 steht das entwickelte Analysewerkzeug als ein Softwaretool zur Verfügung, welches vom Anwender bei der Bewertung der Wirksamkeit von technischen Vorkehrungen gegen Fehler durch Personalhandlungen an MMS gemäß der in AP 2 entwickelten Methode, z. B. im Rahmen von HF-Analysen, herangezogen werden kann.

Die Ergebnisse dieses Arbeitspunktes wurden aufbereitet und sind im Kapitel 4 dieses Abschlussberichtes dokumentiert.

[1] Analyse und Testsystem der GRS /GRS 21/

2 Ermittlung und Aufbereitung des für das Vorhaben relevanten Standes von Wissenschaft und Technik

In diesem Kapitel werden die Ergebnisse der Arbeiten zum Arbeitspaket 1 „Ermittlung von technischen Vorkehrungen in softwarebasierter Leittechnik gegen Fehler durch Personalhandlungen an Mensch-Maschine-Schnittstellen“ dargestellt.

Hierzu werden zunächst für das Vorhaben relevante Begriffe beschrieben (Abschnitt 2.1). Anschließend werden im Abschnitt 2.2 für das Vorhaben relevante Aspekte der Analyse der menschlichen Zuverlässigkeit bei der Durchführung einer Aufgabe z. B. an einer Mensch-Maschine-Schnittstelle präsentiert. Im Abschnitt 2.3 finden sich die Ergebnisse der Auswertung von Regelwerksanforderungen hinsichtlich technischer Vorkehrungen gegen Personalfehlhandlungen an Mensch-Maschine-Schnittstellen zur Steuerung, Bedienung und Instandhaltung softwarebasierter Leittechniksysteme.

2.1 Für das Vorhaben relevante Begriffe

2.1.1 Arbeitssystem/Mensch-Maschine-System

Für die Analyse und Bewertung der menschlichen Zuverlässigkeit bei der Durchführung einer Aufgabe oder Tätigkeit wird in der Arbeitswissenschaft das Modell des „Mensch-Maschine-Systems“ oder des „Arbeitssystems“ verwendet.

Unter einem „Mensch-Maschine-System“ oder „Arbeitssystem“ versteht man eine oder mehrere als Team organisierte Personen mit einer bestimmten fachlichen Qualifikation, die in einer bestimmten Arbeitsumgebung mit festgelegten Arbeitsmitteln („Maschine“) und -methoden Aufgaben erfüllen, die von einer übergeordneten Arbeitsorganisation festgesetzt worden sind und nach bestimmten Maßstäben bewertet werden. Diese Maßstäbe bestehen in der Schnelligkeit, Genauigkeit und Zuverlässigkeit der Aufgabendurchführung sowie der Art, Qualität und Menge des erzielten Arbeitsergebnisses. /FAS 94/

Aus dieser Definition geht hervor, dass ein Arbeitssystem aus mehreren Teilelementen/Teilsystemen besteht:

- Arbeitsaufgabe(n),
- Arbeitsmittel (Maschine) und –methoden,
- Arbeitsumgebung (z. B. Beleuchtung, Klima),
- Arbeitsperson(en) (mit bestimmten Qualifikationen),
- Arbeitsorganisation und
- Arbeitsergebnis mit zugehörigen Bewertungsmaßstäben und -kriterien.

In der Literatur finden sich weitere Definitionen für ein Arbeitssystem, die sich je nach Anwendungsbereich und angestrebtem Ziel bei der Analyse bzw. Bewertung der menschlichen Zuverlässigkeit u. a. im Detaillierungsgrad der zu berücksichtigenden Teilsysteme (z. B. Bezeichnungen der Teilsysteme, Anzahl der Teilsysteme) voneinander unterscheiden. Die wesentlichen Bestandteile eines Arbeitssystems (Arbeitsperson, Arbeitsmittel, Arbeitsaufgabe) sind jedoch allen Arbeitssystemmodellen gemeinsam.

In /VDI 02/ und in /BAD 22/ wird beispielsweise bei der Definition eines Arbeitssystems der Fokus auf das Zusammenwirken bzw. auf die Wechselwirkungen zwischen der Arbeitsperson (Mensch) und den Arbeitsmitteln (Maschine) gelegt. Das Arbeitssystem wird in /VDI 02/ als das Zusammenwirken und die Gesamtheit der Wechselwirkungen zwischen Mensch und Betriebsmitteln bei der Arbeit definiert. Gemäß /BAD 22/ beschreibt das Arbeitssystem das Zusammenwirken und die Wechselwirkung von Mensch und Arbeitsmittel im Arbeitsablauf, um die Arbeitsaufgabe am Arbeitsplatz bzw. in der Arbeitsstätte unter Arbeitsumgebungseinflüssen zu erfüllen. Entsprechend dieser Definition wird in /BAD 22/ bei der Beschreibung des Arbeitssystems zusätzlich zu den zuvor genannten Teilsystemen das Teilsystem „Arbeitsablauf“ betrachtet, um das Zusammenwirken zwischen der Arbeitsperson und den Arbeitsmitteln bei der Erledigung der Arbeitsaufgabe zu analysieren. Dies kann beispielsweise der Optimierung des Arbeitsablaufs dienen, um die menschliche Zuverlässigkeit bei der Durchführung der Arbeitsaufgabe zu erhöhen.

Das im Rahmen dieses Vorhabens verwendete Modell eines Arbeitssystems ist in Kapitel 3 beschrieben.

2.1.2 Mensch-Maschine-Schnittstelle

Die Mensch-Maschine-Schnittstelle, nachfolgend als MMS bezeichnet, ist gemäß /DIN 03/ der Teil einer Einrichtung, welcher als direktes Kommunikationsmittel zwischen Bedienperson und Einrichtung vorgesehen ist, und die Steuerung und Überwachung des Betriebs der Einrichtung ermöglicht. Mensch-Maschine-Schnittstellen schließen handbetätigte Bedienteile, Anzeigen und Bildschirme ein. Die Steuerung und Überwachung des Betriebs einer Einrichtung kann gemäß der Definition eines Arbeitssystems (siehe Abschnitt 2.1.1) als Arbeitsaufgabe betrachtet werden. Die Mensch-Maschine-Schnittstelle entspricht demnach einem Arbeitsmittel-/Betriebsmittel zur Durchführung einer Arbeitsaufgabe. Sie ist demzufolge ein Teilsystem eines Arbeitssystems.

In /DIN 06/ wird für die Mensch-Maschine-Schnittstelle der Begriff Benutzungsschnittstelle verwendet. Als Benutzungsschnittstelle werden alle Bestandteile eines interaktiven Systems (Software oder Hardware) bezeichnet, die Informationen und Steuerelemente zur Verfügung stellen, welche für den Benutzer notwendig sind, um eine bestimmte Arbeitsaufgabe mit dem interaktiven System zu erledigen. Diese Definition der Mensch-Maschine-Schnittstelle verdeutlicht, dass die Mensch-Maschine-Schnittstelle als Bestandteil eines Arbeitssystems zu betrachten ist.

Im Rahmen dieses Vorhabens werden Mensch-Maschine-Schnittstellen softwarebasierter Leittechniksysteme, wie sie beispielsweise in Kernkraftwerken eingesetzt werden, betrachtet. Auf Grundlage von /HAR 10/ ist in eine Übersicht typischer Mensch-Maschine-Schnittstellen eines softwarebasierten Leittechniksystems für die Prozessüberwachung und -steuerung, für die Systeminstandhaltung und -modifizierung sowie für die Systementwicklung dargestellt.

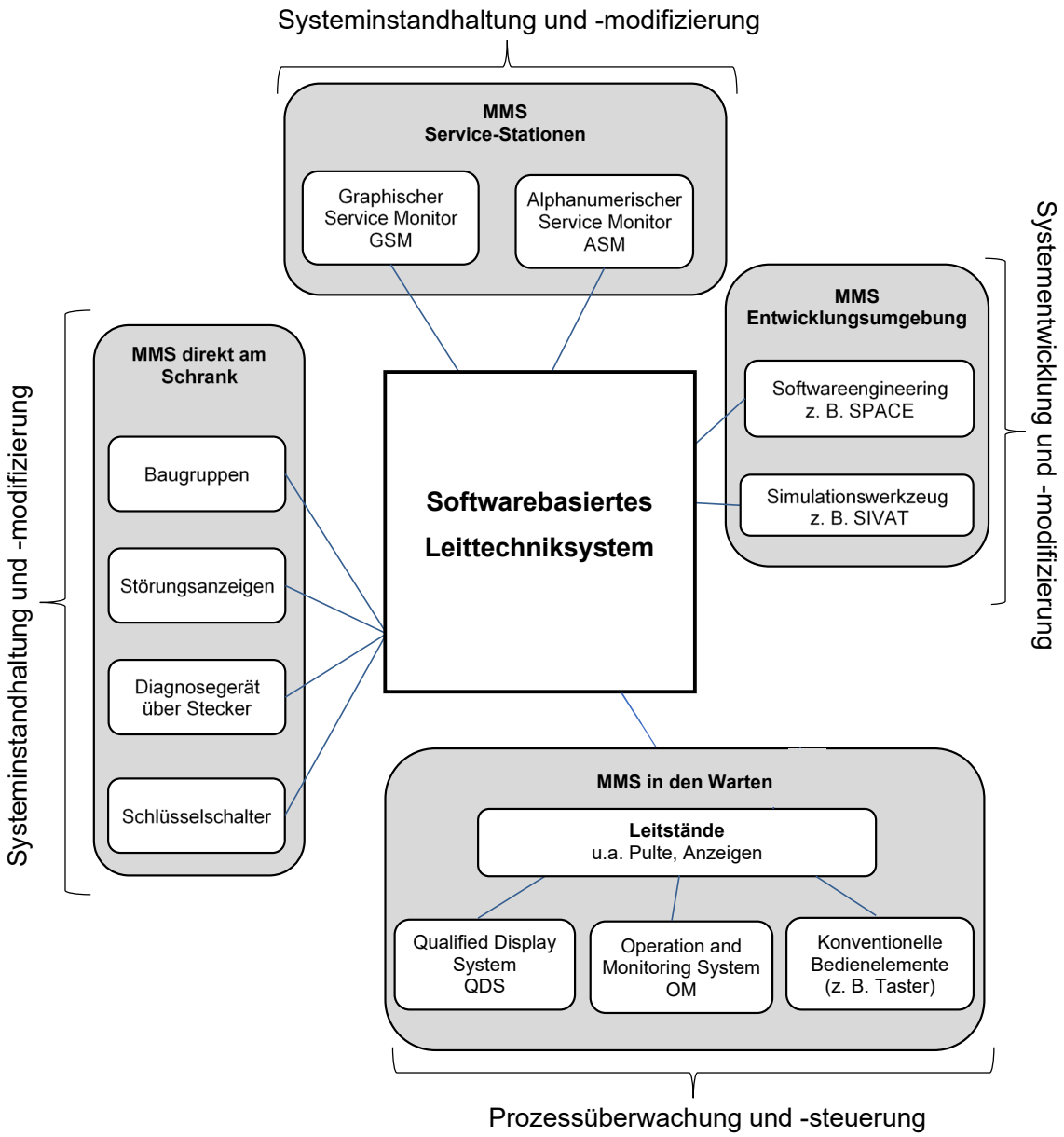

Abb. 2.1: Übersicht typischer Mensch-Maschine-Schnittstellen (MMS)

Hier MMS eines softwarebasierten Leittechniksystems für die Prozessüberwachung und -steuerung, für die Systeminstandhaltung und -modifizierung sowie für die Systementwicklung in einem Kernkraftwerk nach /HAR 10/

In Kernkraftwerken befinden sich die MMS zur Prozessüberwachung und -steuerung u. a. auf der Warte und/oder auf der Notsteuerstelle oder an den örtlichen Leitständen. Die MMS zur Systeminstandhaltung und -modifizierung sind in der Regel in den Leittechnikschränken (LT-Schränke) in den Schaltanlagenräumen, im Wartennebenraum oder an den Feldgeräten wie z. B. Messumformern, Schutzgeräten zwecks Parametrisierung installiert.

Sie schließen auch die MMS mobiler Diagnosegeräte ein, welche über Stecker an die LT-Schränke angeschlossen werden. Die MMS unterscheiden sich abhängig von der jeweils durchzuführenden Aufgabe (Prozessüberwachung, Prozesssteuerung, Systeminstandhaltung, Systemmodifizierung, Systementwicklung) in ihrer Art (Hardwarelösungen wie z. B. Einstellschalter an den Baugruppen oder Softwarelösungen wie z. B. Entwicklungssoftware in der Entwicklungsumgebung und/oder in Servicestationen/-rechner mit Anbindung an das softwarebasierte Leittechniksystem) und Ausführung (z. B. Bedien-/Anzeigetafel mit Eingabemöglichkeiten, Servicerechner, Schlüsselschalter, Diagnosestecker).

Die in Abb. 2.1 dargestellten typischen Mensch-Maschine-Schnittstellen softwarebasierter Leittechniksysteme zur Informationsanzeige (z. B. das Qualified Display System in TXS) oder zur Prozessüberwachung und -steuerung (z. B. das Operation and Monitoring System in Teleperm XP) werden überwiegend als bildschirmgestützte Benutzeroberflächen (graphische Benutzeroberflächen) realisiert. Die Informationen liegen in solchen graphischen Benutzeroberflächen in Graphiken vor, die u. U. auf mehreren zusammenhängenden Bildschirmen angezeigt werden. Die graphischen Darstellungsmöglichkeiten umfassen beispielsweise Fließbilder, Zeitkurven, Histogramme, Balkendiagramme oder auch Bilanzen von Massen- und Energieströmen. Bilder verschiedener Systeme können in Bezug zueinander gebracht werden, indem beispielsweise eine Übersichtsdarstellung mehrerer Systeme durch Detailbilder der Einzelsysteme ergänzt wird /FAS 94/. Es besteht ebenfalls die Möglichkeit Komponenten über „Soft Controls“ (z. B. Mausklicks, Tasten und Schieberegler auf Touchscreens) von der bildschirmgestützten Benutzeroberfläche aus direkt anzusteuern.

Für die Systeminstandhaltung, die Systemmodifizierung und das Systemengineering werden in der Regel menügeführte graphische Benutzeroberflächen mit Auswahl- und Dialogfenstern der eingesetzten Entwicklungswerkzeuge als MMS, z. B. in der Entwicklungsumgebung und in den Servicestationen, eingesetzt. Mensch-Maschine-Schnittstellen in den Leittechnikschränken enthalten neben graphischen Benutzeroberflächen (z. B. Bedientafel mit Eingabemöglichkeiten) auch konventionelle Bedienelemente wie z. B. Schlüsselschalter und Diagnosestecker.

2.1.3 Ergonomie

Gemäß DIN EN 62508 /DIN 11/ ist Ergonomie eine wissenschaftliche Disziplin, die sich mit dem Verständnis der Wechselwirkungen zwischen menschlichen und anderen

Elementen eines Systems befasst und anhand derer Theorie, Grundsätze, Daten und Verfahren auf die Gestaltung von Arbeitssystemen mit dem Ziel angewendet werden, das Wohlbefinden des Menschen und die Leistung des Gesamtsystems zu optimieren.

2.1.4 Menschliche Fehlhandlungen

Gemäß DIN EN 62508 /DIN 11/ spricht man von menschlichen Fehlhandlungen, wenn eine Abfolge mentaler oder physischer Tätigkeiten durch Menschen nach deren Ausführung das beabsichtigte Ergebnis nicht erbringt. Der Grund hierfür könnte sein, dass der Plan ungeeignet war oder dass die Tätigkeiten nicht wie geplant verliefen. Diese Unterscheidung führt zu einer Klassifizierung von Fehlhandlungen in Fehlverhalten, Fehltritte und Verfehlungen /DIN 11/. Fehlverhalten und Fehltritte beziehen sich hierbei auf Fehler bei der Ausführung und Verfehlungen auf Fehler bei der Planung der Tätigkeiten.

Fehlverhalten wird minimiert, wenn die inhärenten menschlichen Eigenschaften bei der Gestaltung berücksichtigt werden und sichergestellt wird, dass die handelnden Personen das nötige Wissen und die nötige Fähigkeit für die Erfüllung der Aufgabe und ausreichend Zeit für die nötigen Überlegungen haben. Klare Anweisungen, intuitive Anzeigen, Stellglieder und Gedächtnisstützen helfen dabei, Fehlverhalten zu minimieren. /DIN 11/

Fehltritte und Verfehlungen sind schwieriger zu minimieren, da die Intention der handelnden Person richtig ist und die Fehlhandlungen häufig dann entstehen, wenn Tätigkeiten automatisch ausgeübt werden und die Person sich der Konsequenzen ihrer Handlung nicht voll gewärtig ist. Maschinen, die so gestaltet sind, dass sie das Situationsbewusstsein der Bedienperson erhalten und überprüfen, stellen sich unbewussten mentalen Erwartungen entgegen und liefern eine frühzeitige Rückmeldung über eine eingetretene Fehlhandlung. Auf diese Art kann sichergestellt werden, dass Fehltritte und Verfehlungen korrigiert werden, bevor die Gesamtzuverlässigkeit gefährdet wird. /DIN 11/

2.1.5 Menschliche Aspekte/Faktoren

Gemäß /DIN 11/ versteht man unter menschlichen Aspekten bzw. Faktoren die menschlichen Eigenschaften wie z. B. Fähigkeiten, welche die Gestaltung, den Betrieb und die Instandhaltung von Systemen und deren Bestandteile betreffen und die sich auf die Leistung des Gesamtsystems auswirken.

2.2 Analyse und Bewertung der menschlichen Zuverlässigkeit

Die Analyse und Bewertung der menschlichen Zuverlässigkeit in Zusammenwirken mit einem technischen System wird als Human Reliability Assessment (HRA) bezeichnet. Die HRA schließt u. a. folgende Schritte ein /VDI 02/:

- Schritt 1: Identifikation und Festlegung der durchzuführenden Aufgabe(n)
- Schritt 2: Qualitative Analyse der Aufgabe(n) (auch qualitative HRA genannt)
- Schritt 3: Quantifizierung der menschlichen Fehlerwahrscheinlichkeit(en) bei der Durchführung der Aufgabe(n) (auch quantitative HRA genannt)

Als Kenngröße zur Quantifizierung der menschlichen Zuverlässigkeit wird im Rahmen der HRA die Fehlhandlungswahrscheinlichkeit (engl. Human Error Probability, HEP) herangezogen. Zur Ermittlung der HEP sind verschiedene HRA-Methoden/Ansätze in der Literatur vorhanden, z. B. in /VDI 02/. Alle diese HRA-Methoden/Ansätze basieren u. a. auf der Ermittlung und der Analyse von Faktoren, welche die menschliche Fehlerwahrscheinlichkeit bei der Durchführung einer bestimmten Aufgabe bzw. Tätigkeit beeinflussen können. Diese Faktoren werden leistungsbeeinflussende Faktoren genannt. Die für eine definierte Aufgabe relevanten leistungsbeeinflussenden Faktoren werden ausgehend von der Aufgabenanalyse und auf Basis der daraus identifizierten potenziellen menschlichen Fehlhandlungen im Rahmen der qualitativen HRA analysiert /INL 16/.

Bei den leistungsbeeinflussenden Faktoren wird gemäß /VDI 02/ und /DIN 11/ zwischen externen, so genannten sachlichen, und internen, so genannten menschlichen leistungsbeeinflussenden Faktoren unterschieden. Die externen leistungsbeeinflussenden Faktoren resultieren aus organisatorischen und technischen Gegebenheiten und Vorbedingungen, in denen der Mensch die ihm übertragene Aufgabe erledigen soll. Die organisatorischen Vorbedingungen betreffen Aspekte der Aufbauorganisation wie z. B. die Hierarchieebenen, Informations-, Kommunikations- und Entscheidungswege und Aspekte der Ablauforganisation wie z. B. Arbeitsabläufe, Arbeitsanweisungen, Arbeitsplanung und die Arbeitszeit. Die technischen Gegebenheiten beziehen sich auf technische Aspekte der Arbeitsumgebung wie z. B. die Arbeitsplatzgestaltung, die technische Gestaltung der Betriebsmittel, die ergonomische Gestaltung des Arbeitsplatzes und die Umgebungsbedingungen des Arbeitsplatzes. Die menschlichen leistungsbeeinflussenden Faktoren sind die Leistungsfähigkeit und die Leistungsbereitschaft. Sie stellen individuelle Faktoren dar, die durch physiologische und psychologische Möglichkeiten und

Bereitschaften des Menschen wie z. B. Motivation, Qualifikation, Fähigkeiten, Erfahrungen bestimmt werden.

Bei der Analyse und Bewertung der menschlichen Zuverlässigkeit werden u. a. zunächst mögliche Ursachen für menschliche Fehlhandlungen ermittelt. Die ermittelten Ursachen werden anschließend dahingehend analysiert, ob geeignete Gegenmaßnahmen zur Minimierung bzw. Vermeidung der mit ihnen verknüpften Fehlhandlungen festgelegt werden können.

Gemäß /DIN 11/ führt die Kombination aus sachlichen und menschlichen leistungsbeeinflussenden Faktoren in unterschiedlicher Weise zu physiologischer und psychologischer Beanspruchung des Operateurs bei der Durchführung einer Aufgabe. Das erzielte Arbeitsergebnis hängt davon ab, wie der einzelne Operateur in der Lage ist, die entsprechende Kombination zu bewältigen /VDI 02/.

Demzufolge ist das erzielte Arbeitsergebnis eines Menschen bei der Durchführung einer ihm übertragenen Aufgabe durch die vorliegenden sachlichen und menschlichen leistungsbeeinflussenden Faktoren bestimmt. Ursachen für menschliche Fehlhandlungen, d. h. Nichtübereinstimmung zwischen dem tatsächlich erzielten und dem beabsichtigten Arbeitsergebnis, sind daher mit den vorliegenden sachlichen und menschlichen leistungsbeeinflussenden Faktoren bei der Durchführung einer Aufgabe verknüpft. Eine optimale Gestaltung der sachlichen leistungsbeeinflussenden Faktoren (z. B. ergonomische Gestaltung des Arbeitsplatzes, klare Arbeitsanweisungen) kann sich positiv auf die menschliche Leistung bei der Durchführung einer Aufgabe auswirken /DIN 11/.

2.3 Ermittlung von technischen Vorkehrungen in softwarebasierter Leittechnik gegen Personalfehlhandlungen an Mensch-Maschine-Schnittstellen aus Regelwerksanforderungen

Die Mensch-Maschine-Schnittstellen softwarebasierter Leittechniksysteme enthalten in der Regel verschiedene technische Präventivmaßnahmen gegen mögliche Fehlhandlungen des Personals (z. B. Alarme, Autokorrekturen, Blockierungen usw.). Diese technischen Präventivmaßnahmen leiten sich u. a. aus Regelwerksanforderungen zur Vermeidung bzw. Minimierung von menschlichen Fehlhandlungen an Mensch-Maschine-Schnittstellen ab. Es existieren zahlreiche Normen und Regelwerke mit Bezug auf die Auslegung von Mensch-Maschine-Schnittstellen zur Vermeidung bzw. Minimierung von Fehlhandlungen von Personal. In diesem Vorhaben wurden relevante kerntechnische

Normen, Regelwerke und Richtlinien ausgewertet, in denen entsprechende Anforderungen an Mensch-Maschine-Schnittstellen zur Vermeidung bzw. Minimierung von Personalfehlhandlungen enthalten sind. Nachfolgend werden diese Normen, Regelwerke und Richtlinien inhaltlich kurz dargestellt.

2.3.1 Ausgewertete Regelwerke, Normen und Richtlinien

Das deutsche kerntechnische Regelwerk wurde hinsichtlich relevanter Vorgaben durchsucht und die einschlägigen Anforderungen aus den Sicherheitsanforderungen an Kernkraftwerke /BMU 15/ und aus den KTA-Regeln 3904 „Warte, Notsteuerstelle und örtliche Leitstände“ /KTA 17b/, 1201 „Anforderungen an das Betriebshandbuch“, /KTA 15/ 1202 „Anforderungen an das Prüfhandbuch“ /KTA 17a/ und 1203 „Anforderungen an das Notfallhandbuch“ /KTA 09/ detailliert betrachtet.

Internationale kerntechnische Normen und Richtlinien wurden ebenfalls betrachtet und die DIN IEC 62241 „Kernkraftwerke- Warte – Alarmfunktionen und ihre Darstellung“ /DIN 15/, der IAEA-Guide NR-T-2.12 „Human Factors Engineering Aspects of Instrumentation and Control System Design“ /IAE 21/ und die NUREG 0700-Norm „Human-System Interface Design Guidelines“ /NUR 02/ detailliert ausgewertet. Des Weiteren wurde der Leitfaden EPRI 1008122-Guide „Human Factors Guidance for Control Room and Digital Human-System Interface Design and Modification“ /EPR 04/ als weiteres relevantes Dokument ausgewertet.

Die genannten Regelwerke, Normen und Richtlinien wurden zunächst nach übergeordneten Anforderungen an MMS zur Vermeidung bzw. Minimierung von menschlichen Fehlhandlungen ausgewertet. Wie bereits im Abschnitt 2.1.2 erwähnt, ist der Einsatz von bildschirmgestützten Benutzeroberflächen (graphische Benutzeroberflächen) als Mensch-Maschine-Schnittstellen charakteristisch für softwarebasierte Leittechniksysteme. Aus diesem Grund wurden die genannten Regelwerke, Normen und Richtlinien nach spezifischen Anforderungen an die Auslegung/Gestaltung von graphischen Benutzeroberflächen als MMS für softwarebasierte Leittechniksysteme zwecks Minimierung von menschlichen Fehlhandlungen ausgewertet. Des Weiteren wurden in den Regelwerken, Normen und Richtlinien nach entsprechenden spezifischen Anforderungen an Mensch-Maschine-Schnittstellen für die Systementwicklung, -instandhaltung und -modifizierung recherchiert.

2.3.2 Identifizierte Anforderungen aus den ausgewerteten Normen, Regelwerke und Richtlinien

2.3.2.1 Sicherheitsanforderungen an Kernkraftwerke (SiAnf)

Im Abschnitt 3.8 „Anforderungen an Warten“ der SiAnf /BMU 15/ wird u. a. gefordert, dass die Warte und die Notsteuerstelle unter Berücksichtigung ergonomischer Gesichtspunkte so zu gestalten sind, dass die Voraussetzungen für das sicherheitstechnisch erforderliche Verhalten der Beschäftigten gegeben sind.

Des Weiteren wird in /BMU 15/ bezüglich aller Betriebsphasen gefordert, sicherheitsfördernde Auslegungs-, Fertigungs- und Betriebsgrundsätze auf Maßnahmen und Einrichtungen der Sicherheitsebenen 1 bis 4a sowie die Maßnahmen und Einrichtungen, die für Einwirkungen von innen und außen sowie bei Notstandsfällen erforderlich sind, anzuwenden. Darunter zählt u. a. eine ergonomische Gestaltung der Arbeitsplätze.

Ebenfalls in /BMU 15/ sind Anforderungen an die ergonomische Gestaltung der Voraussetzungen für zuverlässiges Handeln des Personals enthalten. Hierzu zählen gemäß /BMU 15/ alle absehbaren Tätigkeiten und Maßnahmen mit sicherheitstechnischer Bedeutung in der Anlage auf den Sicherheitsebenen 1 bis 4 sowie Tätigkeiten, die in Bezug auf Einwirkungen von innen oder von außen sowie bei Notstandsfällen durchzuführen sind. Die entsprechenden Arbeitssysteme sind gemäß /BMU 15/ unter Berücksichtigung ergonomischer Gesichtspunkte so zu gestalten, dass die Voraussetzungen für das sicherheitstechnisch erforderliche Verhalten der in der Anlage tätigen Personen gegeben sind. Das Erfordernis der ergonomischen Auslegung dieser Tätigkeiten bezieht sich nach /BMU 15/ auch auf die Gestaltung aller Arbeitsplätze, an denen diese Tätigkeiten ausgeführt werden, und aller Arbeitsmittel, deren Einsatz für diese Tätigkeiten vorgesehen ist, sowie auf die Gestaltung der Arbeitsabläufe, der Aufgabenverteilung zwischen Mensch und Technik sowie der Arbeitsteilung zwischen den ausführenden Personen.

Zusammenfassend ist festzuhalten, dass in /BMU 15/ übergeordnete Anforderungen zur Sicherstellung des sicherheitstechnisch erforderlichen Verhaltens des Personals enthalten sind. Diese Anforderungen beziehen sich auf eine ergonomische Gestaltung der Arbeitsplätze, der Arbeitsmittel, der Arbeitsläufe, der Aufgabenverteilung zwischen Mensch und Technik sowie der Arbeitsteilung zwischen den ausführenden Personen.

2.3.2.2 KTA 3904 „Warte, Notsteuerstelle und örtliche Leitstände“

Die KTA-Regel 3904 /KTA 17b/ befasst sich mit der Planung, der Ausführung und dem Betrieb der Warte, der Notsteuerstelle und der örtlichen Leitstände für Einrichtungen mit sicherheitstechnischer Bedeutung in Kernkraftwerken.

Hinsichtlich der allgemeinen Anforderungen an Leitstände in der Warte, in der Notsteuerstelle und an örtliche Leitstände wird in /KTA 17b/ ähnlich wie in /BMU 15/ gefordert, dass Arbeitsplätze, Arbeitsmittel, Arbeitsabläufe und Arbeitsumgebung unter Berücksichtigung ergonomischer Gesichtspunkte so zu gestalten und die Aufgaben auf Personal und leittechnische Einrichtungen so aufzuteilen sind, dass die Voraussetzungen für das sicherheitstechnisch erforderliche Verhalten der Beschäftigten gegeben sind. Weiterhin wird in /KTA 17b/ gefordert, dass bei der Auslegung der Leitstände Maßnahmen gegen unbeabsichtigte menschliche Fehlhandlungen zu treffen sind. Gemäß /KTA 17b/ zählen hierzu Maßnahmen wie z. B. eine ergonomische Gestaltung sowie die Automatisierung.

In Bezug auf die ergonomische Gestaltung der Mensch-Maschine-Schnittstelle wird in /KTA 17b/ aufgeführt, dass optische Anzeigen so auszulegen und anzuordnen sind, dass sowohl die Überwachung aller Einzelsysteme als auch die Überwachung des Zusammenwirkens von Einzelsystemen mit anderen Systemen ermöglicht werden. Zudem sind gemäß /KTA 17b/ die für rechnergestützte Prozessinformationssysteme vorgesehenen Melde- und Anlagenbilder sowie Grafiken entsprechend ihrer sicherheitstechnischen Bedeutung für den anlagenspezifischen Einsatz zu qualifizieren. Hierbei sind die sicherheitstechnischen und ergonomischen Aspekte der Bildgestaltung zu berücksichtigen.

Gemäß /KTA 17b/ sind die Anforderungen an ergonomische Gestaltung der Mensch-Maschine-Schnittstellen in der Warte, Notsteuerstelle und an den örtlichen Leitständen bereits bei der Planung, Errichtung und Probephase zu berücksichtigen. Es wird in diesem Zusammenhang in /KTA 17b/ gefordert, dass bei der Gestaltung von Warte, Notsteuerstelle und örtlichen Leitständen ergonomische Erkenntnisse, Daten und Methoden von den Anfängen der Planung an systematisch für das Arbeitssystem berücksichtigt werden. Dabei soll gemäß /KTA 17b/ das zu betrachtende Arbeitssystem das Schichtpersonal (z. B. Anzahl, Qualifikation und Organisation), die Arbeitsmittel (z. B. Informations-, Betätigungs- und Kommunikationseinrichtungen), die Arbeitsaufgaben des Leitstandpersonals und die Arbeitsumgebung (z. B. Beleuchtung und Klima) umfassen.

Dem Erfordernis nach ergonomischer Gestaltung ist nach /KTA 17b/ in der Planungsphase gerecht zu werden, indem u. a. verschiedene Lösungskonzepte hinsichtlich der Bemessung von menschlichen Leistungsmöglichkeiten und Leistungsgrenzen zu analysieren und zu bewerten sind. Bei dieser Analyse und Bewertung sind die späteren Benutzer sowie Fachleute der verschiedenen Ingenieurdisziplinen, der Ergonomie und der Arbeitspsychologie zu beteiligen. Im Rahmen der Errichtungs- und Probephase sind gemäß /KTA 17b/ u. a. die resultierenden Aufgaben des Schichtpersonals zu bewerten. Hierbei ist nachzuweisen, dass die Prozessführungsaufgaben insgesamt unter Berücksichtigung ergonomischer Gesichtspunkte so erfüllt werden, dass die Voraussetzungen für ein sicherheitstechnisch optimales Verhalten der Beschäftigten gegeben sind.

Zusammenfassend ist festzuhalten, dass in der /KTA 17b/ übergeordnete Anforderungen hinsichtlich der Auslegung der Mensch-Maschine-Schnittstelle gegen Personalfehlhandlungen enthalten sind. Die genannten Anforderungen betreffen u. a. Aspekte der ergonomischen Gestaltung der Leitstände in der Warte und in der Notsteuerstelle sowie der örtlichen Leitstände z. B. in Bezug auf die Auslegung und Anordnung optischer Anzeigen und auf die Gestaltung von Melde- und Anlagenbildern sowie Grafiken für rechnergestützte Prozessinformationssysteme. Darüber hinaus wird in /KTA 17b/ gefordert, dass Anforderungen an die ergonomische Gestaltung der Mensch-Maschine-Schnittstellen in der Warte, in der Notsteuerstelle und an den örtlichen Leitständen bereits bei der Planung zu berücksichtigen sind und dass die Erfüllung dieser Anforderungen im Rahmen der Errichtungs- und Probephase nachgewiesen wird. Dies hebt die Bedeutung ergonomischer Gestaltung von Mensch-Maschine-Schnittstellen zur Vermeidung von Personalfehlhandlungen hervor.

2.3.2.3 KTA 1201 „Anforderungen an das Betriebshandbuch“

Die in der KTA-Regel 1201 /KTA 15/ enthaltenen Anforderungen sind auf den Inhalt und die Gestaltung des Betriebshandbuchs eines Kernkraftwerks anzuwenden. Das Betriebshandbuch enthält alle betriebstechnischen und sicherheitstechnischen Regelungen, darunter auch Sicherheitsspezifikationen, die für den bestimmungsgemäßen Betrieb der Anlage und zur Beseitigung von Störungen und Beherrschung von Störfällen erforderlich sind. In einem Anhang des Betriebshandbuchs sind Auflistungen, Unterlagen und ergänzende Regelungen enthalten. Das Betriebshandbuch ist deshalb eine verbindliche Unterlage für die Personalhandlungen in einem Kernkraftwerk und enthält u. a. Handlungsanweisungen zur Durchführung von Schalthandlungen an Mensch-Maschine-Schnittstellen in der Warte.

Der Gestaltung des Betriebshandbuchs insbesondere der Handlungsanweisungen, kommt daher eine hohe Bedeutung bei der Vermeidung bzw. der Minimierung von Fehlhandlungen an Mensch-Maschine-Schnittstellen zu.

Abschnitt 4 von /KTA 15/ enthält allgemeine Anforderungen an die Gestaltung des Betriebshandbuchs, insbesondere hinsichtlich der Berücksichtigung ergonomischer Aspekte zur Vermeidung bzw. Minimierung von Fehlhandlungen. Diese betreffen u. a. den Aufbau, die Schriftart und den Schriftgrad, die Textstrukturierung und -gestaltung, die verwendeten Kennzeichnungen, Hervorhebungen, Bezeichnungen und Abkürzungen sowie den Aufbau von Handlungsanweisungen und Hinweisen. Beispielsweise wird in /KTA 15/ eine einheitliche Gestaltung der Kapitel, die Verwendung einer gut lesbaren Schriftart mit ausreichendem Schriftgrad, eine sparsame Verwendung und eine verständliche Gestaltung von Fließtexten gefordert. Hinsichtlich der Gestaltung der Handlungsanweisungen wird beispielsweise auf die Formulierung von Handlungsanweisungen in imperativer Form, die Verwendung graphischer und typographischer Mittel zur Darstellung von Schrittprogrammen, die Eintragung von Erledigungsvermerken für als Checklisten verwendeten Teilen des Betriebshandbuchs und auf die Verwendung von Hinweisen bei Handlungsanweisungen hingewiesen.

2.3.2.4 KTA 1202 „Anforderungen an das Prüfhandbuch“

Die KTA-Regel 1202 /KTA 17a/ ist auf Inhalt, Aufbau, Gestaltung und Erstellung der Prüfliste und der darin aufgeführten Prüfanweisungen eines ortsfesten Kernkraftwerks anzuwenden. Sie gilt für alle im atomrechtlichen Genehmigungsverfahren festgelegten wiederkehrenden Prüfungen an sicherheitstechnisch wichtigen Systemen und deren Komponenten sowie Einrichtungen. Eine Prüfanweisung enthält die Festlegung der Arbeitsschritte für die Durchführung und für die Protokollierung einer Prüfung unter Angabe von Voraussetzungen und Randbedingungen. Für die Durchführung von Prüfungen gemäß den Prüfanweisungen im Prüfhandbuch sind Schalthandlungen an Mensch-Maschine-Schnittstellen erforderlich. Die Gestaltung des Prüfhandbuchs ist daher ähnlich wie beim Betriebshandbuch von hoher Bedeutung bei der Vermeidung bzw. zur Minimierung von Fehlhandlungen an Mensch-Maschine-Schnittstellen. Hinsichtlich der Gestaltung des Prüfhandbuchs wird auf die sinngemäße Anwendung der Anforderungen der KTA-Regel 1201, Abschnitt 4 /KTA 15/ verwiesen.

2.3.2.5 KTA 1203 „Anforderungen an das Notfallhandbuch“

Die KTA-Regel 1203 /KTA 09/ ist auf den Inhalt und die Gestaltung des Notfallhandbuchs von Kernkraftwerken anzuwenden. Das Notfallhandbuch ist als eigenständiges Handbuch Teil der Betriebsdokumentation. Es enthält die organisatorischen Regelungen und Handlungsanweisungen zum anlageninternen Notfallschutz. Die Durchführung der Maßnahmen des anlageninternen Notfallschutzes erfolgt gemäß den im Notfallhandbuch enthaltenen Handlungsanweisungen für das Anlagenpersonal. Die Gestaltung des Notfallhandbuchs ist daher von hoher Bedeutung zur Vermeidung bzw. zur Minimierung von Fehlhandlungen. Bezüglich der Gestaltung des Notfallhandbuchs wird auf eine sinngemäße Anwendung der Anforderungen Abschnitt 4 der KTA-Regel 1201 /KTA 15/ hingewiesen. Zusätzliche Anforderungen betreffen Entnahmeexemplare aus dem Notfallhandbuch. Entnahmeexemplare sind gemäß /KTA 09/ Handlungsanweisungen mit der Möglichkeit der Protokollierung durchgeführter Handlungen für Tätigkeiten vor Ort. In /KTA 09/ heißt es diesbezüglich: „Zusätzlich ist für das Entnahmeexemplar die Informationsstrukturierung und -gestaltung so zu wählen, dass die vorgeschriebenen Maßnahmen auch unter den besonderen Bedingungen von Notfallsituationen durchgeführt werden können.“ Detaillierte Angaben zu der Gestaltung des Entnahmeexemplars sind nicht angegeben.

2.3.2.6 DIN IEC 62241 „Kernkraftwerke- Warte – Alarmfunktionen und ihre Darstellung“

In der DIN IEC 62241 /DIN 15/ sind funktionale Anforderungen an Systeme zur Meldung von Störungen in der Warte von Kernkraftwerken zusammengestellt. Neben den Definitionen für die Begriffe, die im Zusammenhang mit dem Melden von Störungen verwendet werden, enthält die Norm Auslegungsrichtlinien für die Ausgabe von Störungsmeldungen in der Warte von Kernkraftwerken. In diesen Auslegungsrichtlinien sind gemäß den Ausführungen in /DIN 15/ menschliche Aspekte zu berücksichtigen. Hierzu wird in /DIN 15/ erläutert, dass insbesondere unter anomalen oder transienten Anlagenbedingungen im Kernkraftwerk viele Störungsmeldungen gleichzeitig auftreten. Daher sind für Störungsmeldungen in der Hauptwarte spezielle Überlegungen zum „Human-Factors-Engineering” und zur Systemanordnung erforderlich, um Missverständnisse des Operateurs zu vermeiden und ihn mit geeigneten Informationen zu versorgen /DIN 15/. Mit der Berücksichtigung von menschlichen Aspekten bei der Auslegung der Störungsmeldeanlage soll laut /DIN 15/ sichergestellt werden, dass die Auslegung der Anlage, der Systeme und Geräte, die Aufgaben des Menschen und die Umgebungsbedingungen mit den

Sinnes-, Wahrnehmungs-, kognitiven und physikalischen Merkmalen des Personals, welches Anlagen, Systeme und Geräte betreibt und wartet, kompatibel sind. Es wird in /DIN 15/ u. a. hierzu gefordert, dass die Auslegung der Meldeanlage mit Normen und Konventionen anderer Mensch-Maschine-Schnittstellen konsistent sein muss. Sie muss gemäß /DIN 15/ auch mit den relevanten Betriebsanweisungen übereinstimmen. Daher sollen laut /DIN 15/ die Störungsmeldungen nicht isoliert definiert werden, sondern als integraler Teil des gesamten Informationssystems unter Berücksichtigung von Betriebsbelangen und HF-Gesichtspunkten. Besonders zu beachten sind gemäß /DIN 15/ u. a. folgende Punkte:

- Informationsinhalt und –abdeckung,
- Terminologie und Abkürzungen, z. B. Klarheit und Konsistenz der Informationsdarstellung bei Sichtgeräten und Meldefeldern und
- Kodierung und andere einschlägige Normen und Konventionen in Bezug auf die Gestaltung und Darstellung von Informationen, z. B. Konsistenz der Kodierung für Darstellungen auf Sichtgeräten und auf Meldefeldern

Weiterhin wird in /DIN 15/ gefordert, dass bei der Auslegung der Meldeanlage eine ausreichende Abdeckung von HF-Fragen und eine genaue Betrachtung der Sicherheitsaspekte sichergestellt werden muss. Kriterien für die ergonomische Auslegung der Meldeanlage müssen festgelegt sein und systematisch angewendet werden. /DIN 15/

Im Zuge der Auslegung der Meldeanlage soll laut /DIN 15/ eine Methode ausgewählt werden, die die Aufmerksamkeit der Operateure auf die Meldungen lenkt und die auf die Notwendigkeit des Quittierens hinweist. Dies sollte üblicherweise die Liste der Meldungen sein, um eine eindeutige Identifikation und Aufzeichnung sicherzustellen. Dieselben Symbole und Konventionen sollen sowohl für die Meldungslisten als auch für Prozess- und Anlagenbilder verwendet werden. /DIN 15/

Es ist festzuhalten, dass übergeordnete Aspekte hinsichtlich der Berücksichtigung von menschlichen Faktoren bei der Auslegung von Meldeanlagen in Warten von Kernkraftwerken in /DIN 15/ enthalten sind. Dies betrifft u. a. die Klarheit und die Konsistenz der Informationsdarstellung bei Sichtgeräten und Meldefeldern, die Terminologie und die verwendeten Abkürzungen sowie die Konsistenz der Kodierung für Darstellungen auf Sichtgeräten und auf Meldefeldern. Da abhängig von den auflaufenden Meldungen das Personal darauf angewiesen ist, Handlungen an entsprechenden Mensch-Maschine-

Schnittstellen durchzuführen, trägt dies zur Vermeidung bzw. Minimierung von Fehlhandlungen an Mensch-Maschine-Schnittstellen bei.

2.3.2.7 IAEA-Guide NR-T-2.12 „Human Factors Engineering Aspects of Instrumentation and Control System Design“

Das Ziel dieses Leitfadens /IAE 21/ ist es, Entwicklungsteams praktische Umsetzungsstrategien und Methoden für die Auslegung und Entwicklung leittechnischer Systeme an die Hand zu geben. Diese zielen darauf ab, die Funktionen und Aufgaben des Anlagenpersonals durch Verbesserung der Mensch-Maschine-Schnittstellen zu unterstützen. Im Leitfaden wird hierzu insbesondere auf die Bedeutung menschlicher Faktoren bei der Auslegung und Entwicklung von Mensch-Maschine-Schnittstellen von Leittechniksystemen abgehoben.

Die genannten Umsetzungsstrategien und Methoden in /IAE 21/ beziehen sich auf jede Phase des Lebenszyklus eines Leittechniksystems, d. h. für den Entwurf eines neuen Leittechniksystems, den Betrieb und die Wartung, die Modernisierung und die Stilllegung des Leittechniksystems. Die Mensch-Maschine-Schnittstelle wird hierbei als integraler Bestandteil des Leittechniksystems betrachtet. Darüber hinaus ist anzumerken, dass die in /IAE 21/ betrachteten Konzepte insbesondere auf die Planung von Warten in Kernkraftwerken ausgerichtet sind. Diese Konzepte können jedoch in einem abgestuften Ansatz auch auf Mensch-Maschine-Schnittstellen außerhalb der Warte, z. B. auf Steuerstellen vor Ort, angewendet werden.

Zu den in /IAE 21/ betrachteten Methoden zur Einbeziehung menschlicher Faktoren bei der Auslegung und Entwicklung von Leittechniksystemen im Hinblick auf eine Verbesserung der Mensch-Maschine-Schnittstelle zählen u. a. die Berücksichtigung von relevanten Erkenntnissen aus der Betriebserfahrung, die Analyse der vorgesehenen Leittechnikfunktionen und deren Realisierungen (als Hand- und/oder Automatikfunktionen) sowie die Analyse der Interaktionen zwischen Personal und Leittechniksystem bei der Durchführung von Aufgaben. Die Identifizierung von sicherheitstechnisch wichtigen Aufgaben des Personals wird in /IAE 21/ als ein weiterer bedeutsamer Baustein bei der Berücksichtigung menschlicher Faktoren betrachtet.

Die Berücksichtigung von relevanten Erkenntnissen aus der Betriebserfahrung soll gemäß /IAE 21/ darauf abzielen, bereits bekannt gewordene Mängel des zu realisierenden Leittechniksystems zu identifizieren und unter Beibehaltung betriebsbewährter

Eigenschaften dieses Leittechniksystems durch entsprechende Maßnahmen zu beseitigen. Dies beinhaltet u. a. die Auswertung von Erfahrungen aus Anlagen, in denen die gleichen oder ähnliche Systeme, Komponenten und Mensch-Maschine-Schnittstellen eingesetzt werden. Hierzu können beispielsweise in Bezug auf Mensch-Maschine-Schnittstellen Ereignisdatenbanken und vorhandene Dokumentation (z. B. Berichte, Gutachten) gesichtet und wenn möglich das Personal zur Bedienung und Wartung des Leittechniksystems befragt werden. Die daraus gewonnenen Erkenntnisse können dann in die Planung des Leittechniksystems einfließen. Bei der Berücksichtigung der Betriebserfahrung ist gemäß /IAE 21/ sicherzustellen, dass der Einfluss von menschlichen Faktoren an Mensch-Maschine-Schnittstellen bei den identifizierten Mängeln ebenfalls betrachtet wird.

Die Analyse der Leittechnikfunktionen und deren Realisierung dient gemäß /IAE 21/ zum einen der Festlegung der zur Realisierung der leittechnischen Aufgabe erforderlichen Leittechnikfunktionen. Zum anderen wird abhängig von den zugrundeliegenden leittechnischen Anforderungen (Komplexität, Auswirkungen bei Ausfall, geforderte Genauigkeit etc..) zugeordnet, ob die identifizierten Leittechnikfunktionen als Hand- und/oder Automatikfunktionen realisiert werden. Hieraus werden der erforderliche Automatisierungsgrad für die Leittechnikfunktionen sowie die Rolle und der notwendige Informationsbedarf des Personals zur Ausführung der ihm zugrundliegenden Aufgaben an entsprechenden Mensch-Maschine-Schnittstellen festgelegt.

Die Analyse der Interaktionen zwischen Personal und Leittechniksystem bei der Durchführung von Aufgaben soll gemäß /IAE 21/ u. a. dazu verwendet werden, die notwendige Schrittabfolge bei der Durchführung einer Aufgabe an einer Mensch-Maschine-Schnittstelle zu bestimmen. Dies ermöglicht es, potenziell fehleranfällige Aufgaben bzw. Schritte und somit auch das Potenzial für Fehlhandlungen von Personal zu identifizieren.

Mit der Identifizierung sicherheitstechnisch wichtiger Aufgaben des Personals soll gemäß /IAE 21/ sichergestellt werden, dass die Wahrscheinlichkeit menschlicher Fehlhandlungen an die geplanten Mensch-Maschine-Schnittstellen zur Ausführung dieser Tätigkeiten oder die Auswirkungen eines auftretenden Fehlers an diesen Mensch-Maschine-Schnittstellen minimiert wird. In Bezug auf konkrete Designvorgaben für die Gestaltung der Mensch-Maschine-Schnittstelle zur Vermeidung von Fehlhandlungen vom Personal wird in /IAE 21/ auf andere Normen und Richtlinien z. B. /NUR 02/ verwiesen.

Im Leitfaden sind ebenfalls Empfehlungen in Bezug auf die Behandlung von potenziellen menschlichen Fehlhandlungen an den Mensch-Maschine-Schnittstellen enthalten, die im Rahmen der Analyse der Interaktionen zwischen Personal und Leittechniksystem erkannt wurden. Hierzu wird ein abgestuftes Vorgehen vorgeschlagen. Dieses besteht darin, zunächst die identifizierte Fehlermöglichkeit durch Ausschließen der fehleranfälligen Aufgabe zu beseitigen. Falls dies nicht möglich ist, wird empfohlen, das Fehlerrisiko zu minimieren, z. B. durch eine entsprechende Gestaltung des Systems, der Komponente oder der Aufgabe. Eine weitere Möglichkeit, Fehlhandlungen an Mensch-Maschine-Schnittstellen zu vermeiden bzw. zu reduzieren, besteht darin, das Personal auf Fehler und auf ggfs. vorhandene Fehlerbehebungsmöglichkeiten hinzuweisen. Durch gezieltes Training des Personals kann ebenfalls eine Reduzierung oder Minimierung von Fehlhandlungen an Mensch-Maschine-Schnittstellen erreicht werden.

Zusammenfassend ist festzuhalten, dass in /IAE 21/ übergeordnete Empfehlungen zu relevanten Aspekten zur Fehlerminimierung bzw. -vermeidung an Mensch-Maschine-Schnittstellen enthalten sind. Diese betreffen u. a. die Berücksichtigung von relevanten Erkenntnissen aus der Betriebserfahrung, die Analyse der vorgesehenen Leittechnikfunktionen und deren Realisierungen (als Hand- und/oder Automatikfunktionen), die Analyse der Interaktionen zwischen Personal und Leittechniksystem bei der Durchführung von Aufgaben, die Identifizierung von sicherheitstechnisch wichtigen Aufgaben des Personals sowie Möglichkeiten der Fehlererkennung und -behebung durch das Bedienpersonal. Für konkrete Angaben zur Gestaltung von Mensch-Maschine-Schnittstellen zwecks Vermeidung bzw. Minimierung von Fehlern durch Personalhandlungen wird auf andere Normen wie z. B. /NUR 02/ verwiesen.

2.3.2.8 NUREG 0700 „Human-System Interface Design Review Guidelines“

Die in /NUR 02/ enthaltenen Richtlinien wurden von der US-amerikanischen Aufsichtsbehörde Nuclear Regulatory Commission (NRC) entwickelt, um zu bewerten, ob menschliche Aspekte und Faktoren bei der Auslegung von Mensch-Maschine-Schnittstellen für die Steuerung und den Betrieb leittechnischer Systeme in Kernkraftwerken entsprechend den Anforderungen des geltenden US-amerikanischen Regelwerkes berücksichtigt wurden. Die /NUR 02/ ist in vier Abschnitte und einen Anhang gegliedert, die nachfolgend beschrieben werden.

2.3.2.8.1 Part I- Basic HSI Elements

Dieser Abschnitt enthält Richtlinien für die Auslegung von grundlegenden Elementen von Mensch-Maschine-Schnittstellen. Diese Elemente werden gemäß /NUR 02/ als Bausteine verwendet, um Mensch-Maschine-Schnittstellen-Systeme[2] zu entwickeln. Zu den grundlegenden Elementen zählen gemäß /NUR 02/ Informationsdarstellungselemente (Diagramme, Fließbilder, Anzeigegeräte, usw.), Benutzerinteraktionselemente (Menüs, Auswahlfenster, Popups, usw.) sowie Steuerelemente bzw. Eingabeelemente (Tastatur, Funktionstasten, Touchscreens, Computermaus, konventionelle Betätigungselemente wie z. B. Taster etc.). Die Richtlinien zur Bewertung der genannten Elemente insbesondere hinsichtlich der Berücksichtigung menschlicher Aspekte sind in entsprechenden Unterabschnitten dieses Abschnitts der Richtlinie angegeben. Beispielsweise sind Anforderungen an die Informationsdarstellungselemente betreffend Format, Schriftgröße, Schriftart, Zeichenabstand, Beschriftung der Diagramme usw. angegeben. Hinsichtlich der Auslegung der Benutzerinteraktionselemente sind beispielsweise Anforderungen an die Anordnung der Dialogmenus auf der Benutzeroberfläche, an die zu verwendende Schrift und Schreibweise in Dialogfenstern sowie an die Systemrückmeldungen an die Bedienperson (z. B. Fehlermeldungen, Fortschrittsanzeige, Blinkanzeige) enthalten. Für die Bedien- und Steuerelemente sind in /NUR 02/ beispielsweise Anforderungen für die Ausgestaltung rechnerbasierter Eingabegeräte (Tastatur, Touchscreens, Computermaus etc.) und konventioneller Eingabegeräte (Taster, Schalter), für die Anordnung der Eingabegeräte an den Leitständen sowie für Systemrückmeldungen nach Betätigung von Eingabeelementen enthalten.

2.3.2.8.2 Part II- HSI Systems

Im diesem Abschnitt sind Richtlinien für die Bewertung von sieben Mensch-Maschine-Schnittstellen-Systemen enthalten, die in softwarebasierten Leittechniksystemen verwendet werden: Alarmsystem, Gruppenansicht-Anzeigesystem, Überwachungssystem für sicherheitstechnisch wichtige Funktionen und Anlagenparameter, Steuerungssysteme mit rechnerbasierten Eingabegeräten (z. B. Touchscreens), System für

[2] Zusammenhängende Gruppe von Mensch-Maschine-Schnittstellen zur Realisierung bestimmter Funktionen z. B. Alarmfunktionen, Anzeigefunktionen, Steuerungsfunktionen, Benutzerunterstützungsfunktionen

rechnerunterstützte Prozeduren[3], computergestütztes Bedienerunterstützungssystem[4] und Systeme für die Kommunikation zwischen dem Betriebspersonal wie z. B. Einrichtungen für Sprachkommunikation. In /NUR 02/ wird angenommen, dass die Mensch-Maschine-Schnittstellen-Systeme aus den grundlegenden Elementen von Mensch-Maschine-Schnittstellen entwickelt werden. Es gelten demnach für die Mensch-Maschine-Schnittstellen-Systeme die an die grundlegenden Elemente gestellten Anforderungen. Je nach betrachtetem Mensch-Maschine-Schnittstellen-System werden in /NUR 02/ zusätzliche spezifische Anforderungen an Mensch-Maschine-Schnittstellen-Systeme gestellt. Diese zusätzlichen Anforderungen an Mensch-Maschine-Schnittstellen-Systemen sind in entsprechenden Unterabschnitten dieses Abschnittes angegeben und werden nachfolgend beschrieben.

Der Begriff Alarm wird in /NUR 02/ in einem erweiterten Sinne verwendet. Gemäß /NUR 02/ liegt ein Alarm vor, wenn ein Anlagenparameter, eine Komponente, ein System oder eine Funktion sich in einem für den vorliegenden Anlagenzustand nicht vorgesehenen Bereich befindet, sodass Handlungen des Anlagenpersonals erforderlich sind. Das Alarmsystem als Mensch-Maschine-Schnittstellen-System umfasst gemäß /NUR 02/ neben den Sensoren zur Erfassung der Anlagenparameter u. a. auch die Mensch-Maschine-Schnittstellen zur Anzeige von auflaufenden Meldungen mit den zugehörigen überwachten Anlagenparametern (z. B. wenn ein überwachter Anlagenparameter einen vorgegebenen Grenzwert überschreitet) und die Mensch-Maschine-Schnittstellen zur Durchführung von entsprechenden Personalhandlungen bei Vorliegen von Meldungen (Quittieren von Meldungen, Eingabe von Steuerbefehlen für die betroffenen verfahrenstechnischen Komponenten). Anforderungen an das Alarmsystem betreffen beispielsweise die Anzeige von Meldungen, die Priorisierung von Meldungen, die Auslegung von Steuerelementen zur Bearbeitung von Meldungen und die Wartung und Prüfung von Meldesystemen.

Das Gruppenansicht-Anzeigesystem dient dazu, dem Personal einen Gesamtüberblick über den Anlagenzustand zu vermitteln.

---

[3] interaktive Rechneranwendung zur Präsentation einer prozeduralen Anleitung für Anlagenoperateure, die zusätzlich dynamische Prozessinformation einschließlich Zugang zu Operateur-Steuerungen umfassen kann /IEC 20/.

[4] Systeme, die Computertechnologie zur Unterstützung von Bedienern oder Wartungspersonal bei der Situationsbewertung und Reaktionsplanung unterstützen. Sie können den Anlagenstatus überwachen und Empfehlungen oder Warnungen geben. /NUR 02/

Auf diese Weise verfügen z. B. alle Mitglieder einer Schichtmannschaft gleichzeitig über dieselben Informationen. Für die Gruppenansicht-Anzeigesysteme werden i.d.R. Großbildschirme verwendet, die beispielsweise zentral in der Warte platziert sind. Die Anforderungen an das Gruppenansicht-Anzeigesystem beziehen sich beispielsweise auf die Darstellung von Informationen (Schriftart, Schriftgröße) auf dem Anzeigegerät.

Das Überwachungssystem für sicherheitstechnisch wichtige Funktionen und Anlagenparameter dient dazu, dem Personal notwendige Informationen bei Störungen, anomalen Bedingungen und Störfällen zur Verfügung zu stellen, um den Anlagenzustand zwecks Einleitung entsprechender Gegenmaßnahmen bewerten zu können. Spezifische Anforderungen werden in /NUR 02/ an die Informationsdarstellung und an die Benutzerinteraktionselemente im Überwachungssystem für sicherheitstechnisch wichtige Funktionen und Anlagenparameter gestellt. Diese betreffen beispielsweise die Aktualisierungsrate der dargestellten Informationen, die Darstellung der Alarmmeldungen (akustisch und optisch) und die Handhabbarkeit der Benutzerinteraktionselemente.

Steuerungssysteme mit rechnerbasierten Eingabegeräten sind in der Regel als bildschirmgestützte Oberflächen realisiert. Die Steuerbefehle an die Komponenten werden im Gegensatz zu konventionellen Bedienelementen (Taster, Schalter etc.) durch Berühren (Touchscreens) oder durch Anklicken (über Mauszeiger auf Monitore) der entsprechenden Symbole auf der graphischen Oberfläche softwarebasiert aktiviert und an die zu steuernden Komponenten weitergeleitet. Spezifische Anforderungen für Steuerungssysteme mit rechnerbasierten Eingabegeräten in /NUR 02/ betreffen beispielsweise die Auswahl der zu steuernden Komponenten, die Anzeigebereiche, in denen Eingaben vorgenommen werden, und die Formate, die für die Dateneingabe sowie die Systemrückmeldungen nach einer Eingabe verwendet werden. Zudem wird in /NUR 02/ empfohlen, Backup-Systeme mit konventionellen Bedienelementen vorzusehen, um bei Ausfall oder Nichtverfügbarkeit der Steuerungssysteme mit rechnerbasierten Eingabegeräten die Durchführung von sicherheitstechnisch wichtigen Aufgaben durch das Bedienpersonal sicherzustellen.

Das System für rechnerunterstützte Prozeduren ist eine interaktive Rechneranwendung zur Präsentation einer prozeduralen Anleitung (z. B. Schaltanweisungen) für Anlagenoperateure. Es kann zusätzlich dynamische Prozessinformationen einschließlich Zugang zu Operateur-Steuerungen umfassen /IEC 20/. In /NUR 02/ sind spezifische Anforderungen an Systeme für rechnerunterstützte Prozeduren beispielsweise in Bezug auf die Darstellung der Informationen, die Interaktionselemente des Bedienpersonals und

die Kompatibilität des Systems mit anderen Mensch-Maschine-Schnittstellen-Systemen wie z. B. andere Informationsanzeigesysteme (Gruppen-Ansichtsanzeigesystem), enthalten. Für Systeme für rechnergestützte Prozeduren wird ebenfalls empfohlen, Backup-Prozeduren für sicherheitstechnisch wichtige Aufgaben des Personals vorzuhalten, falls das System nicht verfügbar ist.

Als rechnergestützte Bedienerunterstützungssysteme (sogenannte COSS[5]-Systeme) werden rechnerbasierte Mensch-Maschine-Schnittstellen-Systeme bezeichnet, welche das Bedienpersonal bei der Überwachung von Anlagenprozessen, der Erkennung von anomalen Betriebszuständen und der Analyse des Anlagenzustands unterstützen /INL 19/. Rechnergestützte Bedienerunterstützungssysteme können Trends der Anlagenparameter vorhersagen, geeignete Abhilfemaßnahmen auswählen und dem Bedienpersonal Empfehlungen für durchzuführende Abhilfemaßnahmen geben /INL 19/ /NUR 02/. In /NUR 02/ werden übergeordnete Anforderungen an rechnergestützte Bedienerunterstützungssysteme zur Minimierung von Fehlhandlungen des Bedienpersonals gestellt. Diese betreffen beispielsweise die Darstellungsform und den Detaillierungsgrad der angezeigten Informationen, die Kompatibilität des COSS-Systems mit anderen Mensch-Maschine-Schnittstellen-Systemen und die Interaktionsmöglichkeiten mit der Bedienperson. Zudem wird in /NUR 02/ empfohlen, dass die vom COSS-System bereitgestellte Unterstützung in Inhalt und Format möglichst den mentalen Modellen des Benutzers entsprechen sollen, um das Verständnis der vom COSS-System verwendeten Analyselogik beim Nutzer zu fördern.

In /NUR 02/ sind weiterhin Anforderungen an konventionelle Kommunikationseinrichtungen (Telefone, Headsets, Lautsprecheranlagen, Notrufanlagen) sowie an rechnergestützte Kommunikationseinrichtungen für die Kommunikation zwischen dem Betriebspersonal enthalten. Diese betreffen beispielsweise die Auslegung der Mensch-Maschine-Schnittstellen zur Informationsdarstellung an diesen Kommunikationseinrichtungen und zur Steuerung bzw. Bedienung der genannten Kommunikationseinrichtungen sowie die Umgebungsbedingungen der verwendeten Einrichtungen. Hinsichtlich der Informationsdarstellung wird auf die Anforderungen der grundlegenden Elemente von Mensch-Maschine-Schnittstellen verwiesen.

[5] COSS: Computerized Operator Support System

Bezüglich der Bedienung bzw. Steuerung der in Frage stehenden Kommunikationseinrichtungen wird u. a. auf das Bereitstellen von Interaktionsmöglichkeiten zwischen dem Kommunikationsgerät und dem Benutzer und auch zwischen kommunizierenden Partnern mit gleichen Kommunikationsgeräten hingewiesen. Hinsichtlich des Einsatzortes wird gefordert, dass die Funktionalität der eingesetzten Einrichtungen an die Umgebungsbedingungen (z. B. Lärmpegel am Einsatzort) anzupassen ist.

2.3.2.8.3 Part III- Workstation and Workplace Design

In diesem Abschnitt sind Anforderungen an die Bewertung der ergonomischen Aspekte von Leitständen enthalten. Die Anforderungen beziehen sich auf die Konfiguration der Leitstände als Steh-, Sitz- oder Sitz-Steh-Arbeitsplätze für das Schichtpersonal und auf die Anordnung der Bedien- und Anzeigeräte auf der Warte. Diese Aspekte wirken sich auf das Wohlbefinden des Bedienpersonals aus und können demzufolge dessen Leistungsfähigkeit beeinflussen. Bezüglich der Konfiguration der Arbeitsplätze finden sich in /NUR 02/ detaillierte Anforderungen beispielsweise zu der Höhe des Arbeitsplatzes, zu der Neigung und Tiefe der Tischplatte bei Arbeitsplätzen, zu der Anordnung der Bedienelemente und der Anzeigegeräte auf den Arbeitsplätzen und zu den Freiräumen für Beine und Füße. Zur ergonomischen Gestaltung des Arbeitsplatzes gehören gemäß /NUR 02/ auch die Sitzgelegenheiten für das Personal an den Arbeitsplätzen, an die ebenfalls Anforderungen gestellt werden. Hinsichtlich der Anordnung der Anzeigeräte und Bedienelemente wird beispielsweise auf das Erfordernis der Gruppierung zusammengehöriger Bedienelemente oder Anzeigen (z. B. nach Verwendungsreihenfolge, Häufigkeit der Verwendung und Wichtigkeit), die zur Erfüllung einer Aufgabe gemeinsam verwendet werden, hingewiesen. Es wird weiterhin der Einsatz von Beschriftungen und Abgrenzungen empfohlen, um das Bedienpersonal bei der Nutzung von Bedienelemente, Anzeigen und andere Geräte zu unterstützen.

2.3.2.8.4 Part IV- HSI Support

In diesem vierten Abschnitt sind Anforderungen an die Bewertung der HF-relevanten Designaspekte von Mensch-Maschine-Schnittstellen für Wartungs- und Instandhaltungsarbeiten an digitalen Leittechniksystemen enthalten. Der Schwerpunkt liegt insbesondere bei ergonomischen Designaspekten für konventionelle Schnittstellen, z. B. Taster, Stecker, Schalter. Designaspekte zur Minimierung bzw. Vermeidung von Fehlern des Personals, die hierbei betrachtet werden, betreffen beispielsweise die Gestaltung der Leittechnikschränke (z. B. Umfang der Bestückung mit Baugruppen und der

elektrischen Verdrahtung und der vorhandenen Schutzvorrichtungen) und deren Umgebungsbedingungen (z. B. Beleuchtung, physischer und visueller Zugang), die Kennzeichnung der Baugruppen in den Leittechnikschränken, die Anordnung der Baugruppen in Leittechnikschränken, die Anordnung von Betätigungselementen (Taster, Schlüsselschalter), die Störungsanzeigen z. B. zur Kennzeichnung von defekten Baugruppen sowie Rückmeldeanzeigen an den Baugruppen.

2.3.2.8.5 Anhang

Zusätzliche Leitlinien zur Bewertung von Mensch-Maschine-Schnittstellen sind im Anhang der Richtlinie enthalten. Es sind zum einen übergeordnete Leitlinien für die Bewertung von Mensch-Maschine-Schnittstellen angegeben. Diese Leitlinien beziehen sich auf allgemeine Merkmale von Mensch-Maschine-Schnittstellen zur Unterstützung eines möglichst fehlerfreien Handelns des Personals an Mensch-Maschine-Schnittstellen. Sie wurden für die Entwicklung der in /NUR 02/ enthaltenen Anforderungen an Mensch-Maschine-Schnittstellen herangezogen. Aufgrund ihres übergeordneten Charakters können sie zum Beispiel auch für die Bewertung neuartiger Mensch-Maschine-Schnittstellen-Systeme, die nicht in der /NUR 02/ aufgeführt sind, herangezogen werden. Zum anderen sind einige zusätzliche Leitlinien für ausgewählte Themen in Zusammenhang mit Mensch-Maschine-Schnittstellen im Anhang enthalten, beispielsweise zur Überprüfung der Berücksichtigung menschlicher Faktoren beim Entwurf von Mensch-Maschine-Schnittstellen als Informationsanzeigen, Benutzerschnittstelleninteraktion und -management sowie Systemen für rechnerunterstützte Prozeduren.

Zusammenfassend ist festzuhalten, dass sich die NUREG 0700-Richtlinie /NUR 02/ sehr ausführlich und detailliert mit der Auslegung von Mensch-Maschine-Schnittstellen leittechnischer Systeme unter Berücksichtigung menschlicher Faktoren befasst. Betrachtet werden sowohl konventionelle als auch rechnerbasierte Mensch-Maschine-Schnittstellen. Weiterhin sind Anforderungen zur ergonomischen Gestaltung von Leitständen in der Warte und von Leittechnikschränken leittechnischer Systeme in /NUR 02/ enthalten.

2.3.2.9 EPRI 1008122-Guide „Human Factors Guidance for Control Room and Digital Human-System Interface Design and Modification“

Die EPRI-Richtlinie 1008122 /EPR 04/ enthält Leitlinien für die Planung, Spezifizierung, Gestaltung, Implementierung, den Betrieb, die Wartung und die Schulungsmaßnahmen für modernisierte Leitwarten und digitale Mensch-Maschine-Schnittstellen.

Hierbei liegt der Schwerpunkt auf der Berücksichtigung von HF-relevanten Aspekten. Ein Großteil der in der Richtlinie behandelten Aspekte ist auch für Anlagen mit neuartigen Leitwarten mit rechnerbasierten Informationssystemen geeignet. Die Richtlinie enthält detaillierte Informationen und Anforderungen zu spezifischen Mensch-Maschine-Schnittstellen-Systemen wie Informationsanzeigesysteme, Soft Controls, Alarmsysteme und rechnergestützten Systeme zur Berücksichtigung menschlicher Aspekte. Diese Anforderungen entsprechen den Anforderungen aus /NUR 02/ (siehe Abschnitt 2.3.2.8). Aus diesem Grund wird an dieser Stelle auf die in /EPR 04/ diesbezüglich enthaltenen Anforderungen nicht näher eingegangen.

In Bezug auf Mensch-Maschine-Schnittstellen für die Durchführung von Wartungs- und Instandhaltungsarbeiten an softwarebasierten Leittechniksystemen wird in der EPRI-Richtlinie darauf hingewiesen, dass HF-relevante Designaspekte für bildschirmgestützte MMS für Wartungs- und Instandhaltungsarbeiten den Designaspekten für Mensch-Maschine-Schnittstellen zur Steuerung und Bedienung entsprechen und demzufolge den gleichen Anforderungen unterliegen. HF-relevante Designaspekte für konventionelle Mensch-Maschine-Schnittstellen digitaler Leittechniksysteme (Taster, Stecker, Layout der Leittechnikschränke und der Baugruppen etc.) bei der Durchführung von Wartungs- und Instandhaltungsarbeiten, welche der Vermeidung bzw. Minimierung von Fehlhandlungen dienen, werden ebenfalls in /EPR 04/ behandelt. Diesbezüglich enthaltene Anforderungen entsprechen im Wesentlichen den Anforderungen aus /NUR 02/.

Spezifisch für die EPRI-Richtlinie ist, dass diese sich mit HF-relevanten Aspekten des Konfigurationsmanagements[6] befasst, welche mit Handlungen des Personals an Mensch-Maschine-Schnittstellen digitaler Leittechniksysteme zusammenhängen und potenziell fehlerverursachend sein können, wie z. B. im Rahmen von Wartungs- und Instandhaltungsarbeiten. Die EPRI-Richtlinie enthält diesbezüglich übergeordnete Anforderungen, z. B. hinsichtlich des Informationsaustausches an den Mensch-Maschine-Schnittstellen. Beispielsweise heißt es in /EPR 04/: „Wenn der Betrieb oder die Wartung

[6] Konfigurationsmanagement: Identifizierung und Dokumentation der Merkmale von Strukturen, Systemen und Komponenten einer Einrichtung (einschließlich Leittechniksysteme) und die Sicherstellung, dass Änderungen an diesen Merkmalen ordnungsgemäß entwickelt, bewertet, genehmigt, herausgegeben, implementiert, verifiziert, aufgezeichnet und in die Dokumentation der Einrichtung aufgenommen werden. /EPR 04/. Zusätzlich zu den Konfigurationsinformationen gibt es in der Regel weitere Informationen oder Daten, die bei den Aufgaben an den Mensch-Maschinen-Schnittstellen verwendet werden, um die Anlage zu betreiben oder zu warten. Diese Informationen können sich periodisch ändern oder hängen von bestimmten Anlagenbedingungen ab, die variabel sind. Hierzu gehören z. B. betriebsbedingte Änderungen von Einstellwerten, Parametern und Grenzwerten in Leittechniksystemen. /EPR 04/

digitaler Leittechniksysteme zu Aufgaben an Mensch-Maschine-Schnittstellen führt, welche Informationen aus dem Konfigurationsmanagementsystem und ähnlichen Datenquellen erfordern, sollten diese Aufgaben im Entwurfsprozess identifiziert werden und eine entsprechende Überprüfung der menschlichen Faktoren vorgesehen werden.“ Weiterhin heißt es in /EPR 04/: „Wenn Aufgaben an MMS das Abfragen von Konfigurationsinformationen beinhalten, sollte eine Möglichkeit bereitgestellt werden, um die Aktualität der angeforderten Informationen zu verifizieren.“

2.3.3 Zusammenfassung und Schlussfolgerung für das Vorhaben

Es sind zahlreiche Regelwerke, Normen und Richtlinien mit Anforderungen zur Vermeidung bzw. Minimierung von Personalfehlhandlungen an Mensch-Maschine-Schnittstellen für die Steuerung, Bedienung und Instandhaltung leittechnischer Systeme in Kernkraftwerken vorhanden. Im Rahmen dieses Vorhabens wurden relevante kerntechnische Normen, Regelwerke und Richtlinien ausgewertet. Hierbei wurde das deutsche und das internationale kerntechnische Regelwerk betrachtet. Die in diesen Regelwerken identifizierten Anforderungen hinsichtlich technischer Vorkehrungen gegen Personalfehlhandlungen an Mensch-Maschine-Schnittstellen unterscheiden sich in dem Detaillierungsgrad und in den berücksichtigten Aspekten. Allen ausgewerteten Regelwerken ist gemeinsam, dass ergonomische Aspekte eine hohe Bedeutung bei der Vermeidung bzw. Minimierung von Personalfehlhandlungen zukommt.

Übergeordnete Anforderungen zur ergonomischen Gestaltung der Arbeitsplätze, der Arbeitsmittel und der Arbeitsläufe sind beispielsweise in den /BMU 15/ enthalten.

Die KTA-Regel 3904 /KTA 17b/ enthält übergeordnete Anforderungen hinsichtlich der Auslegung der Mensch-Maschine-Schnittstelle gegen Personalfehlhandlungen, u. a. hinsichtlich der ergonomischen Gestaltung der Leitstände in der Warte und in der Notsteuerstelle sowie er örtlichen Leitstände. Die KTA-Regeln 1201 /KTA 15/, 1202 /KTA 17a/ und 1203 /KTA 09/ enthalten allgemeine Anforderungen an die Gestaltung des Betriebshandbuchs, des Prüfhandbuchs und des Notfallhandbuchs insbesondere hinsichtlich der Berücksichtigung ergonomischer Aspekte zur Vermeidung bzw. Minimierung von Fehlhandlungen. Die in diesen Handbüchern enthaltenen Handlungsanweisungen werden an Mensch-Maschine-Schnittstellen angewendet und sind daher von hoher Bedeutung zur Vermeidung bzw. zur Minimierung von Fehlhandlungen an Mensch-Maschine-Schnittstellen. In /IAE 21/ wird insbesondere auf die Bedeutung menschlicher Faktoren bei der Auslegung und Entwicklung von Mensch-Maschine-Schnittstellen von

Leittechniksystemen abgehoben. Der Leitfaden /IAE 21/ enthält praktische Umsetzungsstrategien und Methoden für Entwicklungsteams für die Auslegung und Entwicklung leittechnischer Systeme zur Berücksichtigung menschlicher Faktoren in jeder Phase des Lebenszyklus eines Leittechniksystems, z. B. für den Entwurf eines neuen Leittechniksystems, den Betrieb und die Wartung, die Modernisierung und die Stilllegung eines Leittechniksystems.

In /DIN 15/ sind übergeordnete Anforderungen hinsichtlich der Berücksichtigung von menschlichen Faktoren bei der Auslegung von Meldeanlagen in Warten von Kernkraftwerken enthalten. Diese betreffen u. a. die Klarheit und die Konsistenz der Informationsdarstellung bei Sichtgeräten und Meldefeldern, die Terminologie und die verwendeten Abkürzungen sowie die Konsistenz der Kodierung für Darstellungen auf Sichtgeräten und auf Meldefeldern.

Die Richtlinien /NUR 02/ und /EPR 04/ befassen sich sehr detailliert mit menschlichen Aspekten bei der Entwicklung und Auslegung von Leittechniksystemen zur Vermeidung bzw. Minimierung von Personalfehlhandlungen an Mensch-Maschine-Schnittstellen. Sie enthalten insbesondere sehr detaillierte Anforderungen zur Gestaltung von bildschirmgestützten Benutzeroberflächen wie sie typischerweise als Mensch-Maschine-Schnittstelle für die Steuerung, Bedienung und Wartung von softwarebasierten Leittechniksystemen eingesetzt werden. Die Anforderungen betreffen beispielsweise die Ausgestaltung der verwendeten Informationsdarstellungselemente (Diagramme, Fließbilder, Anzeigegeräte…), die Anordnung von Benutzerinteraktionselementen (Menüs, Auswahlfenster, Popups usw..) sowie der Steuerelemente bzw. Eingabeelemente. Die in /NUR 02/ und in /EPR 04/ behandelten HF-relevanten Designaspekte für konventionelle Mensch-Maschine-Schnittstellen digitaler Leittechniksysteme (Taster, Stecker, Layout der Leittechnikschränke und der Baugruppen etc..) bei der Durchführung von Wartungs- und Instandhaltungsarbeiten, welche der Vermeidung bzw. Minimierung von Fehlhandlungen dienen, betreffen beispielsweise die Gestaltung der Leittechnikschränke (z. B. Umfang der Bestückung mit Baugruppen und der elektrischen Verdrahtung und der vorhandenen Schutzvorrichtungen) und deren Umgebungsbedingungen (z. B. Beleuchtung, physischer und visueller Zugang).

Die gewonnenen Erkenntnisse aus der Auswertung der Regelwerke, Normen und Richtlinien mit Anforderungen zur Vermeidung bzw. Minimierung von Personalfehlhandlungen an Mensch-Maschine-Schnittstellen, sind in das im Rahmen dieses Vorhabens

entwickelte MEDIC[7]-Modell und das entsprechende Analysewerkzeug zur Bewertung von technischen Vorkehrungen in softwarebasierten Leittechniksystemen gegen Fehler durch Personalhandlungen, eingeflossen. Das entwickelte MEDIC-Modell ist im Kapitel 3 und das auf das MEDIC-Modell aufbauende Analysewerkzeug zur Bewertung von technischen Vorkehrungen in softwarebasierten Leittechniksystemen gegen Fehler durch Personalhandlungen im Kapitel 4 beschrieben.

[7] MEDIC: Method for Evaluation of HMI of Digital I&C

3 Entwicklung eines Modells zur Bewertung von technischen Vorkehrungen gegen Fehler durch Personalhandlungen an Mensch-Maschine-Schnittstellen eines softwarebasierten Leittechniksystems

3.1 Einleitung

In diesem Kapitel werden die im Rahmen der Bearbeitung des Arbeitspakets 2 erzielten Ergebnisse dargestellt.

Im Rahmen der Bearbeitung des Arbeitspakets 2 dieses Vorhabens wurde eine Methode - nachfolgend als MEDIC-Bewertungsmethode bezeichnet - zur qualitativen Bewertung von technischen Präventivmaßnahmen gegen Fehler durch Personalhandlungen an Mensch-Maschine-Schnittstellen entwickelt. Das Ziel der entwickelten MEDIC-Bewertungsmethode ist es, potenzielle Mängel technischer Vorkehrungen gegen Fehlhandlungen des Personals an typischen Mensch-Maschine-Schnittstellen digitaler Leittechniksysteme zu identifizieren und zu analysieren.

Wie im Abschnitt 2.1 bereits dargestellt wurde, ist eine Mensch-Maschine-Schnittstelle als Teilsystem eines Arbeitssystems anzusehen. Für die Entwicklung der MEDIC-Bewertungsmethode wurde daher in einem ersten Schritt das zugrunde zulegende Arbeitssystem entwickelt. Hierfür wurde zunächst anhand einer Literaturrecherche der für das Vorhaben relevante Stand von Wissenschaft und Technik zur Modellierung von Arbeitssystemen zur Bewertung von Mensch-Maschine-Schnittstellen ermittelt. Die Ergebnisse dieses Arbeitsschrittes sind in Kapitel 3.2 zusammengestellt. Darauf aufbauend wurden das Modell des Arbeitssystems für die MEDIC-Bewertungsmethode und die MEDIC-Bewertungsmethode selbst entwickelt. Die erzielten Ergebnisse dieser Arbeitsschritte sind im Abschnitt 3.3 dargestellt. Im Abschnitt 3.4 finden sich einige Anwendungsbeispiele der entwickelten MEDIC-Bewertungsmethode.

3.2 Stand von Wissenschaft und Technik zur Modellierung von Arbeitssystemen und Bewertung von Mensch-Maschine-Schnittstellen

Zur Beschreibung und Bewertung von in Arbeitssystemen eingebetteten Benutzerschnittstellen bzw. Mensch-Maschine-Schnittstellen existiert eine Vielzahl von abstrakten Modellen und Methoden in der Literatur. Einige dieser Modelle und Methoden werden nachfolgend beschrieben.

3.2.1 Das IFIP-Modell

Das von der „International Federation for Information Processing“[8] (IFIP) entwickelte „IFIP-Modell“ dient als Grundlage für Anforderungen in verschiedenen Normen, wie beispielsweise ISO 9241 „Ergonomie der Mensch-System-Interaktion“ (und deren Vorgängernormen), und DIN 66234 „Bildschirmarbeitsplätze“ /HER 18/.

Gemäß dem IFIP-Modell setzt sich die Benutzerschnittstelle eines interaktiven Rechnersystems aus vier verschiedenen (Teil-) Schnittstellen zusammen /KOC 91/ /TRI 02/ /OPP92a/ /HER 18/:

- **Ein-/Ausgabeschnittstelle (E/A-Schnittstelle)**
  In dieser Schnittstelle werden die Regeln für die Eingabe des Benutzers und die Ausgabe des Rechners definiert. Die Benutzereingabe umfasst beispielsweise die Eingabe von Zeichen und Befehlen (z.B. über eine Tastatur, Spracheingabe, ...) und die Eingabe der Bewegung des Cursors (z.B. über eine Maus, Cursortasten, ...). Zur Ausgabe des Rechners zählen unter anderem Meldungen, Daten und Softwarewerkzeuge (z.B. Funktionen, Anwendungen), die dem Benutzer mittels eines Bildschirms, Druckers, Lautsprechers oder ähnlichem angezeigt werden.

- **Dialogschnittstelle**
  Die Dialogschnittstelle bestimmt die Regeln für den Dialog zwischen Benutzer und Rechner. Der Dialog beschreibt dabei den Ablauf der Arbeit des Benutzers mit dem Rechner. Hierzu zählt beispielsweise, ob der Nutzer in einem oder mehreren Dialogschritten vorgehen oder den Verarbeitungsprozess unterbrechen möchte. Der Benutzer entscheidet im Dialog über das Ausmaß an Erläuterungen und Unterstützungen, die er vom Computer über eine Ausgabe erhalten möchte.

- **Werkzeugschnittstelle**
  Die Regeln für den Zugriff des Benutzers auf Daten und Softwarewerkzeuge[9] werden in dieser Schnittstelle festgelegt. Die Regeln für den Zugriff sind u. a. durch das Anwendungsspektrum der Softwarewerkzeuge bestimmt.

---

[8] Internationalen Dachorganisation für nationale Gesellschaften und Akademien der Wissenschaften im Bereich der Informations- und Kommunikationstechnologie

[9] Ein Softwarewerkzeug ist ein Programm zur Unterstützung der Softwareentwicklung. Es ermöglicht die computergestützte Anwendung einer Methode im Dialogbetrieb (einem direkten Austausch von Daten zwischen einem System und dem Benutzer in Form eines Dialogs). /GAB 20/

Ein Werkzeug kann spezifische „funktionale Gegebenheiten“ haben, also beispielsweise nur für einen bestimmten Einsatzzweck geeignet sein. Es kann aber auch als sogenanntes „generisches Werkzeug“ allgemeine „funktionale Gegebenheiten“ aufweisen und somit für viele verschiedene Einsatzzwecke wie beispielsweise „Löschen“ und „Einfügen“ genutzt werden.

- **Organisationsschnittstelle**

  Die Organisationsschnittstelle ist die Schnittstelle zur Arbeitsumgebung und zum Betrieb. Die Regeln der Entstehung, Festlegung und Verteilung von Arbeitsaufgaben und des Zusammenhangs zwischen den Arbeitsaufgaben verschiedener Benutzer werden über die Organisationsschnittstelle definiert. Es lässt sich zwischen technischer und nicht-technischer Organisationsschnittstelle unterscheiden. Über die technische Organisationsschnittstelle ist geregelt, wie der Benutzer mithilfe seiner Arbeitsmittel (Rechner) in die Organisation integriert wird (Mensch-Rechner-Funktionsverteilung). Zudem ist die Zusammenarbeit verschiedener Benutzer mittels Rechner hier geregelt (z. B. Kommunikation mittels E-Mail). Die Integration des Benutzers in die Organisation erfolgt mittels der nicht-technischen Organisationsschnittstelle durch entsprechende Organisationskonzepte (Mensch-Mensch-Funktionsverteilung, Gestaltung der Arbeitsabläufe).

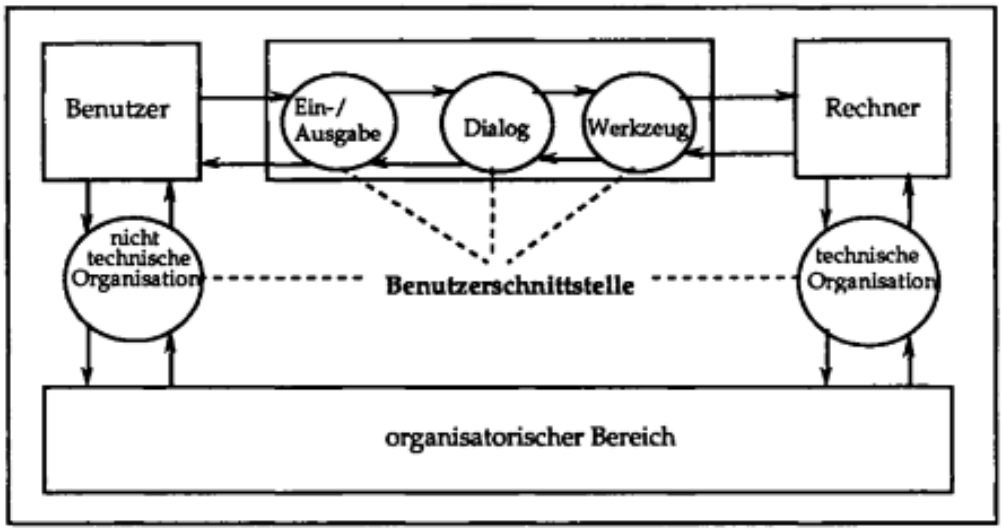

Abb. 3.1 Grafische Darstellung des IFIP-Modells, nach /OPP 92a/.

Die verschiedenen (Teil)-Schnittstellen sind durch Ovale repräsentiert.

Abb. 3.1 stellt den Zusammenhang zwischen den verschiedenen Komponenten und (Teil)-Schnittstellen des IFIP-Modells dar.

Der organisatorische Bereich umfasst dabei die Mensch-Mensch-Funktionsverteilung, die Gestaltung der Arbeitsabläufe und die Mensch-Rechner-Funktionsverteilung /KOC 91/.

Die Teilschnittstellen des IFIP-Modells verweisen auf verschiedene Aspekte einer Benutzerschnittstelle. Den Teilschnittstellen „Ein-/Ausgabe“, „Dialog“ und „Werkzeug“ lassen sich verschiedene Kriterien bezüglich zu bewertender Aspekte der Teilschnittstellen zuordnen: /HER 18/

- Ein-/Ausgabe-Schnittstelle:
    - Wahrnehmbarkeit,
    - Handhabbarkeit,
    - Lesbarkeit,
    - Unterscheidbarkeit,
    - Orientierungsförderlichkeit,
    - Lenkbarkeit der Aufmerksamkeit,
    - u.a.m.
- Dialogschnittstelle:
    - Aufgabenangemessenheit,
    - Selbstbeschreibungsfähigkeit,
    - Steuerbarkeit,
    - Erwartungskonformität,
    - Fehlerrobustheit,
    - Individualisierbarkeit,
    - Lernförderlichkeit,
    - u.a.m.
- Werkzeugschnittstelle:
    - Wiederverwendbarkeit,
    - Zuverlässigkeit,
    - Erweiterbarkeit,

- Verfügbarkeit,
- Kombinierbarkeit,
- u.a.m.

Diese Zuordnungen und Gruppierungen der Kriterien sind nicht als vollständig anzusehen, andere Zuordnungen und Gruppierungen sind auch möglich und begründbar. Dennoch können die Gruppierungen als hilfreiche Struktur für eine differenzierte Untersuchung und Bewertung von Benutzerschnittstellen bzw. von einzelnen Aspekten eines interaktiven Rechnersystems genutzt werden. /HER 18/

3.2.2 Das VDI-Modell

In /VDI 02/ wird das in Abb. 3.2 dargestellte Modell eines Arbeitssystems zur Analyse der menschlichen Zuverlässigkeit bei der Durchführung einer Aufgabe an einer Mensch-Maschine-Schnittstelle, nachfolgend als VDI[10]-Modell bezeichnet, verwendet.

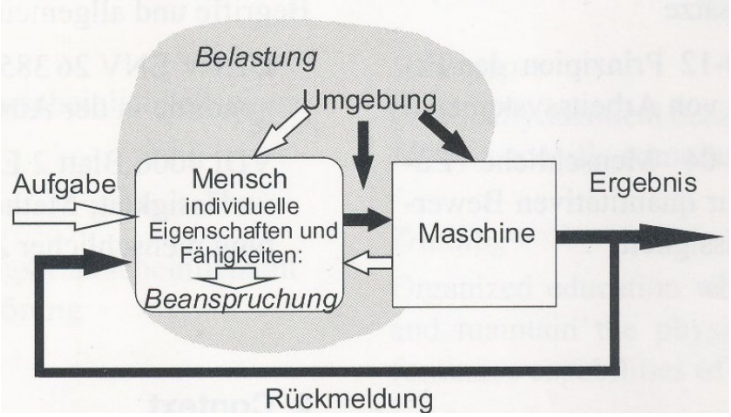

Abb. 3.2 Modell eines Arbeitssystems zur Beschreibung der menschlichen Zuverlässigkeit an Mensch-Maschine-Schnittstellen nach /VDI 02/

Bei dem VDI-Modell umfasst das Arbeitssystem die Elemente Mensch und Maschine. Der Eingang des Systems ist die Aufgabe, welche durch das System erfüllt werden soll, der Ausgang des Systems ist das Ergebnis. Die Rückmeldung ist die von der Maschine abgegebene Rückmeldung. In dem VDI-Modell wird zudem der Einfluss der Umgebung auf die Interaktionen zwischen dem Menschen und der Maschine betrachtet. Alle

[10] VDI: Verein Deutscher Ingenieure

äußeren Wirkungen auf den Menschen werden hierbei als Belastungen bezeichnet. Gemäß /VDI 02/ führen diese Belastungen zu einer Beanspruchung des Menschen aufgrund seiner individuellen Eigenschaften und Fähigkeiten. Diese Belastungen und die individuellen Eigenschaften und Fähigkeiten des Menschen stellen die sogenannten leistungsbeeinflussenden Faktoren dar. Sie sind bei der Bewertung der menschlichen Zuverlässigkeit zu berücksichtigen.

Das VDI-Modell dient in einer etwas abgewandelten Form ebenfalls als Grundlage für die in /DIN 11/ enthaltenen Anforderungen an die ergonomische Gestaltung von Mensch-Maschine-Schnittstellen zwecks Minimierung von Personalfehlhandlungen. In /DIN 11/ werden im Gegensatz zum VDI-Modell /VDI 02/ die durch das Arbeitssystem zu erreichenden Ziele als Systemeingang betrachtet. Die Umgebungseinflüsse werden in /DIN 11/ in soziale und in physische Einflüsse unterteilt. Die sozialen Einflüsse betreffen das soziale Umfeld, in dem das Arbeitssystem eingebettet ist, wie. z B. die Organisationsstruktur und die Arbeitsabläufe. Die physischen Umgebungseinflüsse beziehen sich auf Einflüsse aus der Umgebung wie z. B. auf die Beleuchtung oder Lärm. Die Unterteilung der Umgebungseinflüsse ermöglicht eine strukturiertere Analyse der Auswirkungen der Umgebung auf die Zuverlässigkeit des Gesamtsystems. Die Maschine wird in /DIN 11/ übergeordnet als unterstützendes und dementsprechend gestaltetes interaktives System zum Erreichen der Arbeitssystemziele betrachtet. Gemäß /DIN 11/ müssen die Schnittstellen und Interaktionen zwischen der Maschine und den mit dieser Maschine arbeitenden Personen, die menschlichen Aspekte in allen Lebenszyklusstufen berücksichtigen. Insbesondere sollten die Interaktionen zwischen der Bedienperson und der Maschine so gestaltet werden, dass sie für die Bedienperson leicht anzuwenden sind und dabei ein akzeptables Niveau an mentalem Wohlbefinden sichergestellt wird /DIN 11/.

In /HAR 10/ wird auf Basis des VDI-Modells das in Abb. 3.3 dargestellte generische Modell eines Arbeitssystems zur Bewertung der menschlichen Zuverlässigkeit an Mensch-Maschine-Schnittstellen vorgeschlagen.

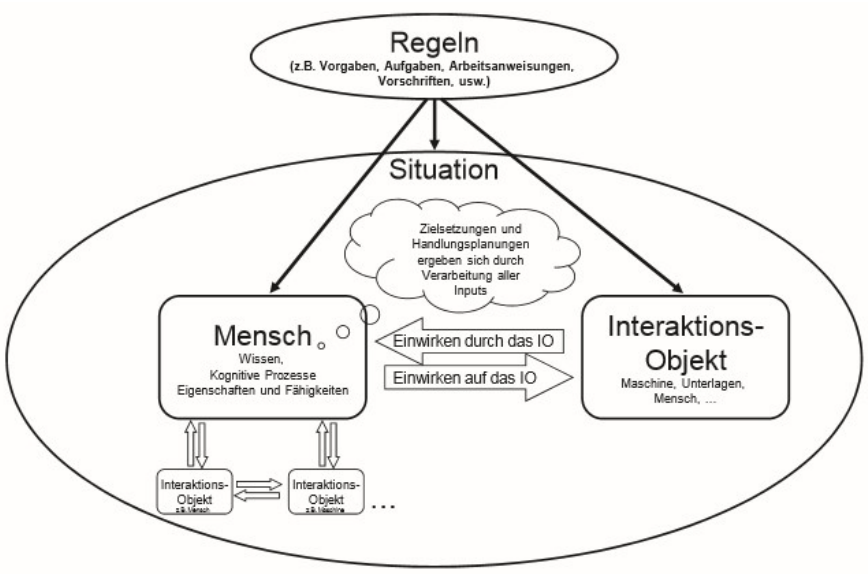

Abb. 3.3 Arbeitssystem-Modell aus /HAR 10/

Bei diesem Modell wurde der Begriff „Maschine“ durch den allgemeineren Begriff „Interaktionsobjekt“ ersetzt. Dies dient dazu, andersgeartete relevante Interaktionen für die Bewertung der menschlichen Zuverlässigkeit bei der Durchführung einer Aufgabe an Mensch-Maschine-Schnittstellen abzudecken, welche nicht als Interaktionen mit einer Maschine angesehen werden, wie z. B. Arbeit mit Unterlagen oder Interaktion mit Menschen. Das in Abb. 3.3 dargestellte Teilelement „Situation“ des Arbeitssystems berücksichtigt gemäß /HAR 10/ die Umgebungseinflüsse und zeitliche Aspekte wie z. B. Arbeitsdauer und Zeitbudget. Gemäß den Ausführungen in /HAR 10/ wirkt der Mensch im Arbeitssystem über Mensch-Maschine-Schnittstellen auf ein Interaktionsobjekt ein, welches selbst zum Teil die Art der Interaktion bestimmt und über die Mensch-Maschine-Schnittstelle Rückmeldungen über verschiedene Sinneskanäle (u. a. visuelle und akustische Informationen an rechnerbasierten Arbeitsplätzen) an den Menschen gibt. Diese Interaktion ist in die aktuelle Situation eingebettet und wird von Regeln bzw. Festlegungen bestimmt. Die Eigenschaften des Menschen, des Interaktionsobjektes, der Situation und der Regeln beeinflussen die Gesamtzuverlässigkeit des Arbeitssystems. Diese Eigenschaften der Teilelemente „Mensch“, „Situation“, „Regeln“ und „Interaktionsobjekt“ des Arbeitssystems werden in /HAR 10/ als leistungsbeeinflussende Faktoren betrachtet. Sie sind im Zuge einer Untersuchung der Zuverlässigkeit des Arbeitssystems zu bewerten /HAR 10/.

3.2.3 Das AUTOS-Modell

Das AUTOS-Modell wurde erarbeitet, um eine Vereinheitlichung des Konzepts des menschenzentrierten Designs und Engineering bei der Entwicklung von interaktiven Systemen zu ermöglichen /BOY 11/. Das menschenzentrierte Design zielt darauf ab, interaktive Systeme nutzerfreundlich und nützlich zu gestalten. Dazu werden Anwender mit ihren Bedürfnissen und Erwartungen in den Mittelpunkt gestellt und menschliche Faktoren sowie Wissen und Methoden zur Benutzerfreundlichkeit und Benutzbarkeit berücksichtigt /ION 22/. Dies fördert die Minimierung von Fehlhandlungen des Benutzers an Mensch-Maschine-Schnittstellen solcher Systeme.

Im AUTOS-Modell werden bei der Modellierung und Bewertung eines Mensch-Maschine-Systems fünf Elemente betrachtet /BOY 11/:

- Artefakt (A): Das Element „Artefakt“ steht übergeordnet für das System, welches im Rahmen des AUTOS-Modells weiter in Hardware und Software unterteilt wird. Die Mensch-Maschine-Schnittstellen für die Bedienung, die Steuerung und die Überwachung des Systems sind dem Element „Artefakt“ zugeordnet. Die Faktoren, welche die Artefakte betreffen, werden als Maschinenfaktoren bezeichnet.

- Benutzer (U): Der Benutzer bedient das System über die Mensch-Maschine-Schnittstelle. Unter das Element „Benutzer“ fallen individuelle menschliche Eigenschaften und Fähigkeiten sowie weitere soziale Faktoren wie die Teamfähigkeit, Kommunikationsfähigkeit und die Fähigkeit zur Entscheidungsfindung. Die dem Element „Benutzer“ zugeordneten Aspekte werden hier als Benutzerfaktoren bezeichnet.

- Aufgabe (T): Das Element „Aufgabe“ steht für die an der Mensch-Maschine-Schnittstelle von der Bedienperson durchzuführende Aufgabe. Hierunter fallen auch Aspekte, welche die Komplexität der Aufgabe beeinflussen, wie z. B. die Angemessenheit der anzuwendenden Verfahren, die Anzahl der Teilaufgaben sowie zeitliche Aspekte (Zeitbudget, Aufgabendauer, Zeitdruck, usw.).

- Organisatorisches Umfeld (O): Dieses Element berücksichtigt das organisatorische Umfeld, in dem das Mensch-Maschine-System eingebettet ist. Das organisatorische Umfeld schließt alle anderen Menschen und/oder Maschinen ein, die mit dem Benutzer interagieren, der die Aufgabe unter Verwendung des Systems ausführt. Diese Interaktionen beeinflussen die Durchführung der Aufgabe an der Mensch-Maschine-Schnittstelle des Systems.

- Situation (S): Das Element beschreibt die Situation, in der die Handlung der Bedienperson eines Systems an der zugehörigen Mensch-Maschine-Schnittstelle stattfindet. Die Situationen können normal oder abnormal sein. Sie können sogar Notfälle sein.

Die Aspekte, welche die Aufgabe, das organisatorische Umfeld und die Situation betreffen, werden im AUTOS-Modell als Interaktionsfaktoren bezeichnet. Charakteristisch für das AUTOS-Modell ist weiterhin, dass die Beziehungen zwischen den genannten fünf Elementen bei der Bewertung des Arbeitssystems auch betrachtet werden sollen. Diese Beziehungen bestimmen die Interaktionen zwischen den Elementen. Beispielsweise wird die Beziehung zwischen der Aufgabe und dem Benutzer durch ergonomische Aspekte und das Training bestimmt. Soziale Aspekte prägen die Beziehung zwischen dem Benutzer und dem organisatorischen Umfeld. Hinsichtlich der Beziehung zwischen dem Benutzer und der Situation ist das Situationsbewusstsein des Benutzers relevant. Die Mensch-Maschine-Schnittstelle könnte durch die Beschreibung von menschlichen Faktoren, Maschinenfaktoren und Interaktionsfaktoren charakterisiert werden.

Zur Veranschaulichung der Zusammenhänge zwischen den fünf Elementen des AUTOS-Modells und deren Beziehungen zueinander wird das Modell als Pyramide dargestellt, die AUTOS-Pyramide (siehe Abb. 3.4), an deren Spitze der Benutzer (das U im AUTOS-Modell) der Mensch-Maschine-Schnittstelle steht. Die vier Eckpunkte der Grundfläche der AUTOS-Pyramide stehen jeweils für die Elemente „Artifact“, „Task“, „Organization“ und „Situation“ im AUTOS-Modell. Die Beziehungen zwischen den fünf Elementen des AUTOS-Modells werden durch die Kanten und die zwei Diagonalen der Grundfläche der Pyramide repräsentiert.

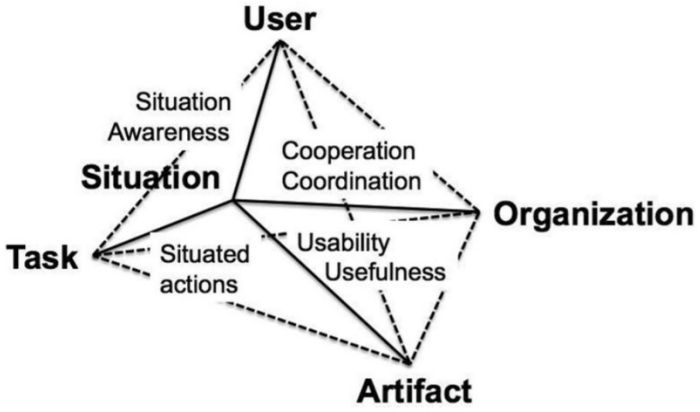

Abb. 3.4 Die AUTOS-Pyramide zur Modellierung eines Arbeitssystems zwecks Bewertung von Mensch-Maschine-Schnittstellen nach /BOY 11/

3.2.4 Der EVADIS-Leitfaden

Der EVADIS-Leitfaden wurde von der GMD[11]-Projektgruppe EVADIS entwickelt. Er dient als Instrumentarium zur ganzheitlichen Analyse von Mensch-Computer-Schnittstellen /MUR 87/.

Mit dem EVADIS-Leitfaden kann die softwareergonomische Qualität von Benutzerschnittstellen empirisch überprüft werden. Die Bewertung der Benutzerschnittstellen schließt alle Benutzerschnittstellenkategorien entsprechend dem in Abschnitt 3.2.1 beschriebenen IFIP-Modell (Ein/Ausgabe-, Dialog- und Werkzeugschnittstelle) ein. Die Organisationsschnittstelle gemäß dem IFIP-Modell wird nicht betrachtet. Das hierbei verwendete Prüfverfahren besteht aus der Beantwortung einer Reihe von Fragen, die aus mehreren allgemeinen softwareergonomischen Kriterien abgeleitet wurden, wie sie beispielsweise für Dialogschnittstellen in /DIN 88/ enthalten sind.

Insgesamt wurden den Fragen des EVADIS-Leitfadens von den Entwicklern folgende übergeordnete Kriterien zugeordnet /MUR 87/:

- **Aufgabenangemessenheit**: Die eigentliche Arbeitsaufgabe des Benutzers soll unterstützt werden, ohne dass sie durch die spezifischen Eigenschaften des Systems zusätzlich belastet wird.
- **Selbsterklärungsfähigkeit:** Der Dialog soll entweder unmittelbar verständlich sein oder aber, wenn dies nicht der Fall ist, soll das System dem Benutzer auf Verlangen den Einsatzzweck sowie die Einsatzweise des Dialogs erläutern können. Soweit der Dialog nicht unmittelbar verständlich ist, sollen dem Benutzer auf Verlangen auch der Leistungsumfang der Arbeitsmittel des Systems erklärt werden können. Dadurch soll der Benutzer sich eine zweckmäßige Vorstellung von den Systemzusammenhängen für seine Aufgabenerledigung machen können.
- **Steuerbarkeit**: Die Möglichkeit, den zeitlichen Ablauf des Dialogs, seine Geschwindigkeit - inklusive Unterbrechungen - und die Reihenfolge der einzelnen Dialogschritte zu beeinflussen. Das impliziert, dass der Benutzer nicht vom System "getrieben" wird, dass er die Geschwindigkeit des Dialogablaufs an seine individuelle

[11] GMD: Gesellschaft für Mathematik und Datenverarbeitung; Die GMD – Forschungszentrum Informationstechnik GmbH war eine zwischen 1968 und 2001 bestehende deutsche Großforschungseinrichtung für angewandte Mathematik und Informatik mit Sitz in Sankt-Augustin.

Arbeitsgeschwindigkeit anpassen kann, dass er andererseits aber auch nicht auf Systemantworten warten muss, wenn er diese für den Fortgang des Dialogs nicht benötigt. Wenn ein Dialogschritt unterbrochen wird, sollte der Benutzer einen "Wiederaufnahmepunkt" definieren können, der ihn in die Lage versetzt, zu jeder Zeit an diesem beliebig gewählten Wiederaufnahmepunkt den Dialog fortzusetzen, ohne umfangreiche neuerliche Vorbereitungen treffen zu müssen.

- **Verlässlichkeit**: Das Dialogverhalten des Systems soll denjenigen Erwartungen des Benutzers entsprechen, die er aus Erfahrungen mit Arbeitsabläufen - mit und ohne Computer - mitbringt.

- **Fehlertoleranz**: Fehlertoleranz ist eine Forderung, die es dem Benutzer trotz eines Eingabefehlers erlaubt, zu einem gewünschten Arbeitsergebnis zu kommen. Allerdings muss dem Benutzer die Ursache des Fehlers zum Zweck seiner Behebung verständlich gemacht werden. Es mag in einigen Fällen sinnvoll sein, eindeutige Fehler automatisch korrigieren zu lassen. Allerdings muss dieser Mechanismus vom Benutzer bei Bedarf abschaltbar sein. Fehlertransparent ist ein System, wenn es dem Benutzer Fehler zum Zwecke der Behebung und künftigen Vermeidung verständlich macht.

- **Transparenz**: Das System soll für den Benutzer "durchschaubar" sein. Dieses Kriterium bezieht sich sowohl auf die Systemleistungen, also z.B. auf die Beschaffenheit der einzelnen Anwendungsmodule, der Kommandostruktur, der Tiefe und Breite der Menübäume etc. ("statische" Transparenz) als auch auf Meldungen des Systems an den Benutzer, wie Präsenzanzeigen, Fehlermeldungen, außergewöhnliche Zustände wie Überlastung etc. ("dynamische" Transparenz).

- **Erlernbarkeit**: Die Nutzung der Systeme soll möglichst leicht erlernbar sein. Dieses Kriterium sollte jedoch angemessen berücksichtigt werden und nicht so, dass es zu Systemen führt, die letztendlich beim Benutzer zu einer Belastung wegen kognitiver Unterforderung führen.

- **Übersichtlichkeit**: Das Kriterium bezieht sich auf die Anordnung der Daten auf dem Bildschirm, u. a. auf die übersichtliche Gestaltung der Kommandozeilen, Systemhilfen etc.

- **Flexibilität:** Dieses Kriterium bezieht sich vor allem auf die Werkzeugschnittstelle. Es fordert eine möglichst weitreichende Anpassungsmöglichkeit der Softwarewerkzeuge an die individuellen Wünsche, Erfahrungen etc., des Benutzers. Die während

des Umgangs mit einem System schrittweise zunehmende Beherrschung eines Systems durch den Benutzer sollte durch technische Realisierungen dieses Kriteriums Rechnung getragen werden.

Das EVADIS-Verfahren kann von Softwareergonomie-Experten ohne Versuchspersonen angewandt werden und ist primär für den Test von computergestützten Bürosystemen gedacht. /MUR 87/

Der EVADIS-Leitfaden wurde insbesondere durch Einbeziehung der Organisationsschnittstelle gemäß dem IFIP-Modell zum EVADIS II-Leitfaden weiterentwickelt. Gegenstand des EVADIS II-Evaluationsverfahrens sind Softwaresysteme für den Büro- und Verwaltungsbereich. Typische Benutzer sind daher beispielsweise Schreibkräfte, Sachbearbeiter oder Fach- bzw. Führungskräfte. Typische Einzel- bzw. integrierte Anwendungspakete dieser Benutzergruppen sind Datenbanken, Tabellenkalkulation, Grafik-/Bildverarbeitung, Textverarbeitung und Elektronische Post /OPP 92b/.

Mit der Berücksichtigung der Organisationsschnittstelle in der Bewertung wird mit dem EVADIS II-Leitfaden die Einbettung der Benutzerschnittstellen in einen organisatorischen Kontext (Arbeitsaufgabe, Arbeitsablauf) gemäß dem IFIP-Modell Rechnung getragen. Nicht berücksichtigt beim EVADIS II wird die Ergonomie der Hardware und des Arbeitsplatzes. Das Prüfverfahren beim EVADIS II-Leitfaden besteht, ähnlich wie beim EVADIS-Leitfaden, aus der Beantwortung einer Reihe von Fragen, die aus aufgaben-, organisations- sowie softwareergonomischen Kriterien abgeleitet werden. Hierfür wurden Kriterien zur Bewertung der ergonomischen Aspekte der Organisationsschnittstelle auf Basis arbeitswissenschaftlicher Erkenntnisse eingeführt. Weiterhin wurden die softwareergonomischen Kriterien zur Bewertung der Teilbenutzerschnittstellen (Ein- /Ausgabe-, Dialog- und Werkzeugschnittstelle) im Hinblick darauf, dass eine hinsichtlich Organisation und Aufgabe menschengerechte Arbeit nicht durch den Einsatz eines Bürosystems beeinträchtigt wird. Diesbezügliche Kriterien wurden aus der DIN 66234 Teil 8 /DIN 88/ und aus der ISO 9241, Part 10 /ISO 90/ ausgewählt. Einige dieser ausgewählten Kriterien entsprechen den beim EVADIS-Leitfaden verwendeten, andere wurden zusätzlich eingeführt.

Das EVADIS II-Verfahren steht sowohl als Papierversion als auch als Softwareversion zur Verfügung. Die Softwareversion soll den Anwender des EVADIS II-Leitfadens bei der Durchführung seiner Evaluationsaufgabe rechnergestützt unterstützen /OPP 92c/.

3.2.5 Die „Usability Heuristics“-Bewertungsmethode

Von Jakob Nielsen wurden zehn Regeln für ein gutes Schnittstellendesign aufgestellt. Da diese Regeln eher sogenannte „Daumenregeln“ als tatsächlichen Anforderungen aus Richtlinien entsprechen, wurden sie von ihm als Usability Heuristics (Benutzbarkeits-Heuristiken[12]) bezeichnet. Im Folgenden werden diese zehn Heuristiken aufgeführt und in den jeweiligen Unterpunkten anhand von Beispielen veranschaulicht: /NIE 94/, /HUN 22/

1. Sichtbarkeit des Systemstatus

Das System sollte die Nutzer und Nutzerinnen durch angemessene Rückmeldungen innerhalb einer angemessenen Zeit über den aktuellen Status informieren. Beispiele hierfür sind:

- Die Anzeige des Speicherstatus in einem Word-Dokument anhand eines Fortschrittbalkens.
- Die Bread-Crumb-Navigation (Brotkrümelnavigation) zeigt dem Nutzer meist anhand einer Textzeile an, an welcher Stelle oder in welchem Kontext es sich in einer Software oder auf einer Website befindet. Hinter der Brotkrümelnavigation steht der Gedanke, den Nutzer zu jeder Zeit wissen zu lassen, wo er sich in der Hierarchie einer Software oder einer Webseite befindet.

2. Übereinstimmung zwischen dem System und der realen Welt

Das System sollte die Fachsprache der Benutzerinnen und Benutzer berücksichtigen. Dabei sollten anstelle von systemorientierten Begriffen, Worte, Sätze und Konzepte genutzt werden, die dem Benutzer bzw. der Benutzerin vertraut sind. Das System sollte den Konventionen der realen Welt folgen, so dass die Informationen in einer natürlichen und logischen Reihenfolge erscheinen. Beispiele hierfür sind:

- Gelöschte Elemente sind im Papierkorb zu finden.
- Das Swipen (Wischen) auf dem Handy ist dem Verschieben von Papier nachempfunden.

[12] Heuristiken sind in der Verhaltenspsychologie Vorgehensweisen, mit denen man trotz begrenzterer Zeit und unvollständigem Wissen eine Entscheidung oder Aussage treffen kann. /HUN 22/

3. Benutzerkontrolle und Freiheit

Die Benutzer und Benutzerinnen wählen oft versehentlich ungewollte Systemfunktionen aus. Daher benötigen sie einen deutlich gekennzeichneten "Notausgang", um den unerwünschten Zustand zu verlassen, ohne einen langen Dialog durchlaufen zu müssen. Die Funktionen „Rückgängig“ (undo) und „Wiederherstellen“ (redo) sollten unterstützt werden. Beispiele sind:

- Der Zurück-Knopf im Internetbrowser.
- Das Schließen unerwünschter Fenster mit dem „X“ oben rechts in dem jeweiligen Fenster.

4. Konsistenz und Standards

Die Benutzerinnen und Benutzer sollten sich nicht fragen müssen, ob verschiedene Wörter, Situationen oder Aktionen das Gleiche bedeuten. Deshalb sollten Plattformkonventionen befolgt werden, zum Beispiel:

- Das „X“ oben rechts führt im Allgemeinen zum Schließen des Fensters.
- Das Disketten-Symbol wird im Allgemeinen als Symbol für den Speicherknopf genutzt.

5. Fehlervermeidung

Besser als gute Fehlermeldungen ist ein sorgfältiges Design, welches das Auftreten eines Fehlers oder Problems verhindert. Fehleranfällige Bedingungen sollten beseitigt werden. Alternativ könnte den Benutzern und Benutzerinnen vor dem Ausführen einer Aktion eine Bestätigungsoption angeboten werden. Beispiele sind:

- Bestätigungsabfrage vor dem Absenden einer E-Mail ohne Betreff.
- Rückversicherung vor dem Löschvorgang: „Wollen Sie dieses Dokument wirklich löschen? Die Aktion kann nicht rückgängig gemacht werden.“

6. Wiedererkennen statt Erinnern

Die Gedächtnisbelastung der Benutzer und Benutzerinnen sollte minimiert werden. Hierzu können Objekte, Aktionen und Optionen sichtbar gemacht werden. Die Benutzer und Benutzerinnen sollten sich keine Informationen von einem Teil des Dialogs zu einem anderen merken müssen. Anweisungen für die Nutzung des Systems sollten sichtbar oder leicht abrufbar sein. Beispiele sind:

- Anstelle eines Tutorials, bei dem man sich an die einzelnen Schritte erinnern muss, kann ein schrittweiser Einführungsprozess treten.
- Formularfelder sollten stets sichtbare Beschriftungen haben.

7. Flexibilität und Effizienz der Nutzung

Shortcuts wie z.B. Tastenkürzel können genutzt werden, um die Interaktion für erfahrene Benutzern und Benutzerinnen zu beschleunigen, ohne dass dies unerfahrene Benutzer und Benutzerinnen beeinträchtigt. Somit kann das System sowohl für unerfahrene als auch erfahrene Benutzerinnen und Benutzer ansprechend sein. Es sollte den Benutzerinnen und Benutzern häufig ermöglicht werden, Aktionen anzupassen. Beispiele hierfür sind:

- Tastenkürzel.
- Erweiterung der Funktionen von Browsern mittels Plugins (Zusatzprogramme).

8. Ästhetisches und minimalistisches Design

Dialoge sollten keine Informationen enthalten, die irrelevant sind oder selten benötigt werden. Es sollte bedacht werden, dass jede zusätzliche Informationseinheit in einem Dialog mit den relevanten Informationseinheiten konkurriert und deren relative Sichtbarkeit vermindert. Zum Beispiel:

- Unnötige oder wenig relevante Elemente können verborgen oder visuell reduziert dargestellt werden.

9. Fehler erkennen, diagnostizieren und beheben

Fehlermeldungen sollten in einfacher Sprache (nicht in Code) formuliert sein, das Problem genau benennen und eine konstruktive Lösung vorschlagen. Beispiele sind:

- Ein nicht verfügbares Produkt könnte auf ähnliche Ersatzprodukte verlinken.
- Error 404-Seiten[13], die eine Suchfunktion enthalten.

10. Hilfe und Dokumentation

Obwohl es besser ist, wenn das System ohne Hilfe oder Dokumentation benutzt werden kann, kann es notwendig sein, eine Hilfe oder Dokumentation bereitzustellen.

---

[13] Der HTTP-Fehler mit dem Statuscode „Fehler 404 - Not Found“ zeigt an, dass die vom Client (eine Soft- oder Hardware, die mit einem Server kommuniziert) angeforderten Daten nicht auf dem Webserver gefunden werden können.

Solche Informationen sollten leicht auffindbar sein, sich auf die Aufgabe des Benutzers konzentrieren, konkrete Schritte auflisten und nicht zu umfangreich sein.

Durch die Anwendung der zehn Usability Heuristiken nach Jakob Nielsen lässt sich ein User-Testing nicht vermeiden. Größere Fehler im Interface-Design lassen sich dadurch im Allgemeinen jedoch gut erkennen. Obwohl die meisten Prinzipien selbstverständlich erscheinen, gibt es noch immer eine Vielzahl an Systemen, die davon abweichen. In einer heuristischen Evaluation wird die Benutzerschnittstelle eines Produktes von einer geringen Anzahl von Gutachtern untersucht, um zu überprüfen, inwieweit diese mit den Usability Heuristiken übereinstimmt. Basierend auf Untersuchungen zur Quote der erkannten Probleme in Abhängigkeit von der Anzahl der Gutachter empfiehlt Nielsen drei bis fünf Gutachter für die heuristische Evaluation einer Benutzerschnittstelle einzusetzen. Diese sollten ca. 60 bis 70 Prozent der Usability-Probleme finden. Diese Empfehlung ist hinsichtlich des Verhältnisses von Aufwand und Ertrag getroffen worden. /NIE 94/, /MSG 22/, /EIC 22/

3.2.6 Zusammenfassung der Erkenntnisse zur Modellierung von Arbeitssystemen und Bewertung von Mensch-Maschine-Schnittstellen

Für die Bewertung von Mensch-Maschine-Schnittstellen ist zunächst das Arbeitssystem, in dem die Mensch-Maschine-Schnittstelle eingebettet ist, zu modellieren. Hierbei sind die zu betrachtenden Elemente des Arbeitssystems, die Beziehungen dieser Elemente zueinander sowie die für die Bewertung relevanten Aspekte der Elemente und der Beziehungen zwischen diesen Elementen zu spezifizieren. Die Festlegung der zu berücksichtigenden Elemente und Interaktionen zwischen diesen Elementen hängt vom angestrebten Ziel der Bewertung der Mensch-Maschine-Schnittstelle ab.

Bei den Modellen zur Bewertung der Ergonomie von Benutzerschnittstellen von interaktiven Rechnersystemen wird der Schwerpunkt auf die Benutzerfreundlichkeit der eingesetzten Soft- und Hardwareschnittstellen gelegt. Bei dem zur Bewertung von Benutzerschnittstellen von interaktiven Rechnersystemen häufig verwendeten IFIP-Modell besteht das Arbeitssystem aus den Elementen „Benutzer“, „Benutzerschnittstelle“, „Rechner“, und „Organisatorischer Bereich“. Die Benutzerschnittstelle wird gemäß dem IFIP-Modell in vier verschiedene Teilschnittstellen unterteilt, welche die Beziehungen zwischen den Elementen des zugrunde gelegten Arbeitssystems kennzeichnen und auf verschiedene Aspekte hinsichtlich der Benutzerfreundlichkeit einer Benutzerschnittstelle verweisen. Diesen Teilschnittstellen lassen sich verschiedene Kriterien zuordnen, die für

eine Bewertung der Benutzerschnittstellen herangezogen werden können. Dieses Vorgehen wird beispielsweise bei dem EVADIS-Bewertungsleitfaden angewandt.

Heuristische Methoden zur Bewertung von Mensch-Maschine-Schnittstellen von interaktiven Rechnersystemen wie z. B. die „Usability Heuristics“-Methode von Jakob Nielsen beruhen nicht auf Arbeitssystemmodellen. Bei der „Usability Heuristics“-Methode wurden zehn Regeln als „Daumenregeln“ für ein gutes Schnittstellendesign aufgestellt. Diese Regeln betreffen u. a. die Rückmeldungen des Systems an den Benutzer, die Verwendung von realitätsnahen Symbolen und von dem Benutzer geläufigen Begriffen sowie die Konsistenz der verwendeten Symbole.

Den verwendeten Arbeitssystemmodellen zur Analyse der menschlichen Zuverlässigkeit bei der Durchführung einer Aufgabe an einer Mensch-Maschine-Schnittstelle ist gemein, dass sie die Elemente „Mensch“ und „Maschine“ beinhalten. Abhängig vom angestrebten Ziel der Analyse und vom Detaillierungsgrad der Bewertung werden in den verschiedenen Arbeitssystemmodellen zusätzliche Elemente und Interaktionen zwischen diesen betrachtet, um insbesondere dem Einfluss der Umgebung auf die Interaktionen zwischen dem Menschen und der Maschine Rechnung zu tragen. Dies schließt sowohl die physischen Umgebungsbedingungen wie z. B. Lärm und Beleuchtung als auch das soziale Umfeld wie z. B. die Organisationsstruktur und die Arbeitsabläufe ein. Es werden beispielsweise bei dem AUTOS-Modell u. a. die Elemente „Situation“ und „Organisatorisches Umfeld“ zusätzlich betrachtet. Diese beziehen sich auf die Situation, in der die Handlung an der Mensch-Maschine-Schnittstelle erfolgt, und auf das organisatorische Umfeld, in dem das Mensch-Maschine-System eingebettet ist. Die Erkenntnisse aus der Analyse der menschlichen Zuverlässigkeit dienen u. a. als Grundlage für die Ableitung von Anforderungen an die ergonomische Gestaltung von Mensch-Maschine-Schnittstellen zwecks Minimierung von Personalfehlhandlungen. Dies wird beispielsweise in /DIN 11/ auf Grundlage des VDI-Modells angewandt.

Im Abschnitt 3.3 wird näher darauf eingegangen, wie die gewonnenen Erkenntnisse zur Modellierung von Arbeitssystemen und Bewertung von Mensch-Maschine-Schnittstellen in die Entwicklung der MEDIC-Bewertungsmethode eingeflossen sind.

3.3 Die MEDIC-Bewertungsmethode zur Bewertung von Mensch-Maschine-Schnittstellen softwarebasierter Leittechniksysteme

3.3.1 Untersuchungsrahmen für die entwickelte MEDIC-Bewertungsmethode

Wie bereits erwähnt enthalten die Mensch-Maschine-Schnittstellen softwarebasierter Leittechniksysteme in der Regel verschiedene technische Vorkehrungen gegen mögliche Fehlhandlungen des Personals. Diese technischen Vorkehrungen lassen sich weiter in Maßnahmen zur Fehlerprävention und Maßnahmen zur Fehlerkorrektur unterteilen.

Die Maßnahmen zur Fehlerprävention (oder implizite technische Vorkehrungen) sind inhärent im Design der Mensch-Maschine-Schnittstelle. Sie beziehen sich insbesondere auf die ergonomische Auslegung der Mensch-Maschine-Schnittstelle im Hinblick auf die Förderung eines möglichst fehlerfreien Handelns an der Mensch-Maschine-Schnittstelle. Als Beispiele für derartige Maßnahmen zur Fehlerprävention sind u. a. eine klare, konsistente und übersichtliche Informationsdarstellung an der Mensch-Maschine-Schnittstelle, die Gestaltung der Eingabemasken sowie eine verständliche Gestaltung von Anweisungen in Unterlagen zu nennen. Ausführungsfehlern an der MMS kann beispielsweise durch solche fehlerpräventive Maßnahmen vorgebeugt werden.

Die Maßnahmen zur Fehlerkorrektur (oder explizite technische Vorkehrungen) betreffen die in der MMS enthaltenen Mechanismen, um fehlerhafte Handlungen (z. B. fehlerhafte Eingabe von Werten) zu unterbinden (Blockade), zu korrigieren (Autokorrektur) oder auf diese hinzuweisen (Warnmeldung). Dies kann zum Beispiel realisiert werden, indem der Bedienperson nur eine bestimmte Anzahl von Auswahlmöglichkeiten für numerische Parameter gegeben wird, anstatt der Person eine freie Eingabe zu ermöglichen. Alternativ kann z. B. eine fehlerhafte Eingabe nachträglich durch eine Fehlermeldung angezeigt oder eine Übernahme der fehlerhaften Eingabe ohne Korrektur verhindert werden. Als integraler Bestandteil der MMS unterliegen die Maßnahmen zur Fehlerkorrektur den gleichen Anforderungen, hinsichtlich ergonomischer Auslegung zur Vermeidung von Fehlhandlungen an MMS, wie die technischen Maßnahmen zur Fehlerprävention.

Die im Rahmen dieses Vorhabens entwickelte MEDIC-Bewertungsmethode zur Bewertung von Mensch-Maschine-Schnittstellen zielt darauf ab, potenzielle Mängel von technischen Vorkehrungen gegen Personalfehlhandlungen an typischen MMS von digitalen Leittechniksystemen in Kernkraftwerken zu identifizieren und deren Ursachen zu

analysieren. Die genannten technischen Vorkehrungen zählen zu den im Abschnitt 2.2 definierten sachlichen leistungsbeeinflussenden Faktoren bzw. externen leistungsbeeinflussenden im Rahmen der HRA. Der Schwerpunkt liegt hierbei in der Bewertung der ergonomischen Auslegung der Mensch-Maschine-Schnittstelle im Hinblick auf die Vermeidung bzw. die Minimierung von Personalfehlhandlungen. Die MEDIC-Bewertungsmethode schließt demnach sowohl die fehler**präventiven** als auch die fehler**korrigierenden** technischen Maßnahmen zur Vermeidung bzw. zur Minimierung von Personalfehlhandlungen an der MMS in die Bewertung mit ein, da diese beiden Arten von technischen Vorkehrungen den gleichen ergonomischen Anforderungen unterliegen.

Interne leistungsbeeinflussende Faktoren (siehe Abschnitt 2.2) bei der Durchführung einer Aufgabe an einer MMS werden im Rahmen der MEDIC-Bewertungsmethode nicht betrachtet.

3.3.2 Theoretische Grundlagen der MEDIC-Bewertungsmethode

3.3.2.1 Komponenten des MEDIC-Arbeitssystemmodells

Für die Entwicklung der MEDIC-Bewertungsmethode zur Bewertung der technischen Vorkehrungen gegen Personalfehlhandlungen an Mensch-Maschine-Schnittstellen wurde das in Abb. 3.5 dargestellte Arbeitssystem, nachfolgend MEDIC-Arbeitssystemmodell genannt, zugrunde gelegt. Das MEDIC-Arbeitssystemmodell besteht aus den Komponenten „Unterlagen“, „Mensch“, „Mensch-Maschine-Schnittstelle (MMS)“ und dem zu bedienenden „System“. Es basiert auf den in Abschnitt 3.2 dargestellten Arbeitssystemmodellen zur Analyse der menschlichen Zuverlässigkeit an Mensch-Maschine-Schnittstellen. Insbesondere baut das MEDIC-Arbeitssystemmodell auf dem Konzept des menschenzentrierten Designs und Engineering auf, wie es beispielsweise bei dem AUTOS-Modell angewandt wird.

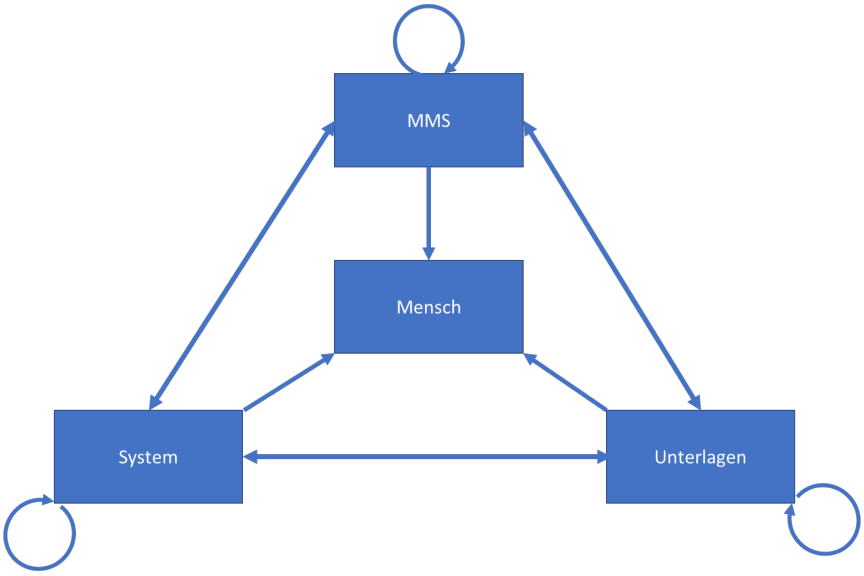

Abb. 3.5 Das MEDIC-Arbeitssystemmodell

Im MEDIC-Arbeitssystemmodell werden sowohl die Komponenten als auch die intra- und interspezifischen Beziehungen der Komponenten betrachtet. Die **intra**spezifischen Beziehungen der Komponenten sind die Beziehungen zwischen den Teilelementen der jeweiligen Komponente und die **inter**spezifischen Beziehungen bezeichnen die Beziehungen zwischen den Komponenten. Die Kreise in der Abb. 3.5 kennzeichnen die Beziehungen zwischen den Teilelementen einer Komponente und die bidirektionalen Verbindungslinien stellen die Beziehungen zwischen den Komponenten des MEDIC-Arbeitssystemmodells dar. Eine Ausnahme im MEDIC-Arbeitssystemmodell bilden die Beziehungen zwischen der Komponente „Mensch“ und den Komponenten „System“, „Unterlagen“ und „MMS“, welche lediglich den Einfluss dieser Komponenten auf die Komponente „Mensch“ darstellen und entsprechend unidirektional in Abb. 3.5 abgebildet sind. Der Grund dafür ist, dass die internen leistungsbeeinflussenden Faktoren des Menschen (s. Kapitel 2.2) bei der Durchführung einer Aufgabe bzw. einer Tätigkeit an einer MMS im Rahmen der MEDIC-Bewertungsmethode nicht betrachtet werden.

Zusammenfassend setzt sich das MEDIC-Arbeitssystem aus den vier Komponenten „Unterlagen“, „System“, „MMS“ und „Mensch“, den Beziehungen zwischen den Teilelementen der jeweiligen Komponenten „System“, „Unterlagen“ und „MMS“ und den Beziehungen zwischen den Komponenten „Unterlagen“, „System“, „MMS“ und „Mensch“ zusammen. Auf die Bedeutung der genannten Beziehungen zur Erzielung eines möglichst fehlerfreien Handelns an der MMS wird im nachfolgenden Abschnitt 3.3.2.2 eingegangen.

Die Komponenten des in Abb. 3.5 dargestellten MEDIC-Arbeitssystemmodells sind wie folgt definiert:

- Mensch: Der Mensch führt eine Aufgabe an einem System durch Interaktion mit der Mensch-Maschine-Schnittstelle (MMS) aus. Der Mensch interagiert mit der MMS unter Berücksichtigung der zugehörigen Unterlagen, um das System entsprechend dem Ziel der auszuführenden Aufgabe zu verändern.

- Die Mensch-Maschine-Schnittstelle (MMS): Die MMS ist der Teil des Arbeitssystems, über die der Mensch mit dem System interagiert, um eine bestimmte Aufgabe auszuführen. Die MMS umfasst Alarme, Anzeigen und Bedienelemente. Im Rahmen dieses Vorhabens werden MMS softwarebasierter Leittechniksysteme, wie im Kapitel 2.1.2 beschrieben, betrachtet. Die MMS kann auch als Teil des Systems betrachtet werden. Da der Schwerpunkt dieses Vorhabens auf der Gestaltung der MMS zwecks Minimierung von Personalfehlhandlungen liegt, wird jedoch eine konzeptionelle Trennung zwischen dem System und der MMS vorgenommen.

- Das System: Das System stellt eine Gruppe von zusammengehörigen mechanischen, elektrischen oder anderen technischen Komponenten dar, die im Verbund und/oder möglicherweise in Verbindung mit anderen Systemen oder Komponenten eine bestimmte Funktion, z. B. eine Steuerungsfunktion, realisieren. Auch Teilsysteme, die bestimmte Teilfunktionen ausführen, werden als Systeme behandelt. Im erweiterten Sinne kann das System auch ein zu steuernder Prozess sein, z. B. Start einer Pumpe, Austausch einer Baugruppe.

- Die Unterlagen: Als Unterlagen werden eine Reihe von Dokumenten (in Papierform und/oder computergestützt) bezeichnet, welche die erforderlichen Informationen (Erläuterungen oder Daten) und/oder Anweisungen zur Unterstützung des Menschen bei der Ausführung einer bestimmten Aufgabe an der MMS enthalten. Die Unterlagen regeln also die Interaktion des Menschen an der MMS. In den Unterlagen sind auch organisatorische Aspekte des betrachteten Systems und der MMS enthalten. Die Unterlagen stellen daher im MEDIC-Arbeitssystemmodell die organisatorische Komponente dar, welche in der Regel in Arbeitssystemmodellen, wie im Kapitel 3.2 erläutert, enthalten ist.

3.3.2.2 MEDIC-Interrelationsmatrix zur Beschreibung der Beziehungen zwischen den Komponenten des MEDIC-Arbeitssystemmodells

Gemäß dem AUTOS-Modell sind neben den Komponenten auch die Beziehungen zwischen den Komponenten eines Arbeitssystems bei der Gestaltung einer MMS zu berücksichtigen. In der MEDIC-Analysemethode werden neben den Beziehungen zwischen den Komponenten auch die Beziehungen zwischen den Teilelementen der jeweiligen Komponenten des Mensch-Maschine-Systems untereinander betrachtet. In Anlehnung an das AUTOS-Modell wird in der MEDIC-Analysemethode davon ausgegangen, dass die Eigenschaften der genannten Beziehungen relevant sind, um eine möglichst fehlerfreie Erledigung einer Aufgabe an der MMS zu erzielen. Die Analyse des Einflusses der Beziehungen zwischen den Teilelementen einer Komponente und der Beziehungen zwischen den Komponenten gemäß dem in Abb. 3.5 dargestellten MEDIC-Mensch-Maschine-System, bildet daher die Grundlage des MEDIC-Analysemodells.

Zur Erläuterung der Bedeutung dieser Beziehungen im Hinblick auf eine Minimierung bzw. Vermeidung von Personalfehlhandlungen an der MMS werden nachfolgend exemplarisch einige relevante Aspekte beschrieben, welche diese Beziehungen bestimmen bzw. beeinflussen. Die Beziehung wird hierbei wie folgt gekennzeichnet „Komponente“ → „Komponente“, wobei die Pfeilrichtung angibt, in welche Richtung die Beziehung betrachtet wird.

- **Unterlagen → Mensch:** Zu den Aspekten der Unterlagen, die auf den Menschen bei der Durchführung der Aufgabe einwirken und demzufolge sein Handeln an der MMS beeinflussen, zählt beispielsweise der Detaillierungsgrad der in den Unterlagen enthaltenen Informationen und Anweisungen für die Durchführung der Aufgabe an der MMS. Der erforderliche Detaillierungsgrad sollte an die Kenntnisse, Fertigkeiten und Fähigkeiten des Menschen für die Durchführung der Aufgabe an der MMS angepasst sein. Dies fördert die Übersichtlichkeit und trägt maßgeblich zur Verständlichkeit der Anweisungen durch den Menschen bei. Weitere Aspekte dieser Wechselwirkung betreffen die Eindeutigkeit und die Vollständigkeit der Informationen und Anweisungen in den Unterlagen im Hinblick auf die zu erfüllende Aufgabe. Letztere sind insbesondere von Bedeutung bei regelbasierter Ausführung von Aufgaben an MMS, da hierdurch ein möglichst fehlerfreies Handeln des Menschen ermöglicht wird. Zudem können die Anweisungen in den Unterlagen so gestaltet sein, dass sie das Situationsbewusstsein des Menschen fördern, wodurch ebenfalls ein fehlerfreies Handeln an der MMS begünstigt wird.

- **Unterlagen → MMS:** Die Beschreibungen und Anweisungen in den Unterlagen sollen so formuliert werden, dass die zu bedienenden Teilkomponenten der MMS vom Menschen immer klar erkennbar sind. Hier können zum Beispiel bildliche Darstellungen der Teilkomponenten der MMS in den entsprechenden Unterlagen die Zuordnung erleichtern. Dies fördert das Verständnis des Menschen und begünstigt demzufolge ein möglichst fehlerfreies Handeln an der MMS.

- **Unterlagen → System:** Sofern es für die Erfüllung der Aufgabe an der MMS relevant ist, sollte bei den in den Unterlagen angegebenen Schritten zur Durchführung der Aufgabe an der MMS ein Bezug zum System hergestellt werden. Neben dem Fördern des Situationsbewusstseins vermeidet dies Missverständnisse beim Menschen und ist somit von Vorteil für ein möglichst fehlerfreies Handeln an der MMS. Der Bezug zum System kann beispielsweise durch Erläuterung der Schritte als Hinweistext oder als graphische Darstellung des relevanten Systemteils in den Unterlagen realisiert werden.

- **Unterlagen → Unterlagen:** Die Gestaltung der Unterlagen wie z. B. die Unterteilung in verschiedenen Abschnitten sowie das Vorhandensein und die Art der Verweise innerhalb der Unterlagen wirken auf den Menschen ein. Die Unterlagen sollen konsistent gestaltet werden, z. B. durch Anwendung von Sprachkonventionen für die Darstellung von Informationen. Denn die dadurch erzielbare Einheitlichkeit in den Unterlagen fördert die Benutzerfreundlichkeit und kann demzufolge fehlervermeidend bzw. fehlerminimierend auf den Menschen wirken.

- **System → Mensch:** Die Eigenschaften des Systems (z. B. die Komplexität und das Design) bestimmen u. a. das Systemverständnis beim Menschen. Menschen entwickeln mentale Modelle von den Systemen, mit denen sie interagieren, und leiten daraus ihre Handlungen und Erklärungen für das Systemverhalten ab /REA 90/. Das Systemdesign beeinflusst dementsprechend die Bildung eines mentalen Modells des Systems beim Menschen. Die mentale Zugänglichkeit des Systems bezieht sich darauf, wie die Auslegung des Systems das Systemverständnis fördern kann und somit dem Menschen die Bildung eines mentalen Modells erleichtern kann. Neben der mentalen Zugänglichkeit spielt auch die physische Zugänglichkeit des Systems eine wichtige Rolle im Hinblick auf die Vermeidung bzw. die Minimierung von Fehlhandlungen. Sie bezieht sich sowohl auf vorhandene Raumverhältnisse (Positionierung im Raum, Zugangswege, räumliche Abstände) als auch auf äußere Bedingungen wie z. B. die Lichtverhältnisse. Der physische Zugang zum System ist

beispielsweise für die Durchführung von Wartungsaufgaben in Leittechnikschränken wie etwa der Austausch von Leittechnikkarten erforderlich.

- **System → MMS:** An den Schnittstellen vom System zur MMS ist festgelegt, inwiefern das System über die MMS verändert werden kann und inwieweit der Systemzustand an der MMS dargestellt werden kann. Der Grad der Nachbildung von Systemzuständen an der MMS hängt hierbei von der an MMS durchzuführenden Aufgabe zusammen. Dies kann von einzelnen Anzeigen und Meldungen bis zu Darstellungen des gesamten Systems reichen. Dies wirkt demnach auf dem Menschen ein und kann bei entsprechender/zielgerichteter Auslegung fehlerminimierend und fehlervermeidend sein. Für die Sicherheit des Systems relevante Eingaben an der MMS und Darstellungen auf der MMS sollten hierbei als solche gekennzeichnet sein.

- **System → System:** Das Systemdesign beeinflusst die Systemverständlichkeit und demzufolge die Bedienung des Systems an der zugehörigen MMS durch den Menschen. Ein konsistenter und strukturierter Aufbau des Systems, bei dem das Zusammenwirken der Teilsysteme klar ersichtlich ist, kann beispielsweise zu einem besseren Verständnis beim Menschen führen. Hierzu zählt u. a. eine konsistente Kennzeichnung von Teilsystemen. Abhängig von der Aufgabe des Systems ist es nicht immer möglich, Konsistenz im Systemdesign vollumfänglich umzusetzen. Falls beim Systemdesign jedoch eine Auswahl zwischen technologisch gleichwertigen Realisierungen besteht, kann die Konsistenz ein ausschlaggebendes Kriterium zur Entscheidungsfindung sein.

- **System → Unterlagen:** Die Komplexität des Systems bestimmt maßgeblich, wie dieses zu beschreiben ist. Dies überträgt sich auf die Unterlagen, in denen das System dargestellt bzw. beschrieben wird. Das Systemdesign als solches ist hierbei grundsätzlich ausschlaggebend für die Gestaltung der Unterlagen. Bei komplexen Vorgängen und Prozessen sind beispielsweise die Unterlagen oft komplexer und umfangreicher als bei weniger komplexen. Die Unterlagen sollen jedoch unabhängig von der Komplexität des Systems soweit möglich Missverständnisse beim Menschen vermeiden und das Situationsbewusstsein beim Menschen fördern. Dies kann durch eine entsprechende Gestaltung der Unterlagen erreicht werden, z. B. durch einen strukturierten Aufbau der Unterlagen, einen der Aufgabe angepassten Detaillierungsgrad der Systembeschreibungen bzw. der Arbeitsanweisungen und die Verwendung von verständnisfördernden Fließbildern zur Darstellung des Systems.

- **MMS → Mensch:** Der Mensch erledigt die Arbeitsaufgabe über die MMS. Die Gestaltung bzw. die Auslegung der MMS beeinflusst daher insbesondere das Auftreten von Personalfehlhandlungen. Bei Gestaltung der MMS unter Einhaltung der Anforderungen zur Berücksichtigung menschlicher Einflussfaktoren können Personalfehlhandlungen an MMS vermieden bzw. minimiert werden. Die Auslegung der MMS sollte, soweit dies realisierbar ist, dem Menschen erleichtern sich ein mentales Modell des zu bedienenden Systems oder des zu verändernden Prozesses zu bilden bzw. dem mentalen Modell, das der Mensch aufgrund seiner Ausbildung und seines Trainings entwickelt hat, entsprechen. Dies kann beispielsweise durch graphische Darstellungen (z. B. Fließbilder) des Systems bzw. des Prozesses auf der MMS erzielt werden. Als bildschirmgestützte Oberflächen realisierte MMS sind in der Regel in Leitständen integriert, welche als Steh- und/oder Sitzplätze realisiert sind. Der physische Zugang zu den entsprechenden Leitständen mit MMS soll für den Menschen sichergestellt werden. Dies betrifft ebenfalls ergonomische Aspekte zur Gestaltung des Arbeitsplatzes des Menschen.

- **MMS → MMS:** Ähnlich wie bei den Unterlagen ist auch bei der Gestaltung der MMS insbesondere auf die Konsistenz zu achten. Dies betrifft sowohl die Wahl, als die Anordnung der zu verwendenden Bedienelemente (Anzeigen, Eingaben) auf der Bedienoberfläche. Die Bedienelemente sollen hierbei zusätzlich voneinander unterscheidbar und dem System eindeutig zuordenbar (siehe **MMS → System**) bleiben. Dies fördert die Benutzerfreundlichkeit und kann demzufolge fehlervermeidend bzw. fehlerminimierend auf den Menschen wirken.

- **MMS → System:** Die Auslegung der MMS bestimmt das Maß, in dem der Mensch Einfluss auf das System nehmen kann. An der MMS sollen daher für die Durchführung der Aufgabe relevante Aspekte des Systems widergespiegelt werden. Dabei ist darauf zu achten, dass alle für die Durchführung der Aufgabe erforderlichen Interaktionselemente an der MMS vorhanden sind. Dies können beispielsweise Anzeigen und Eingabefenster sein. Zusätzlich zu numerischen Anzeigen können auch Fließbilder des Systems zu einer übersichtlichen Darstellung beitragen. Können an einer MMS mehrere Systeme durch den Menschen beeinflusst werden, so ist durch eine entsprechende Auslegung der MMS sicherzustellen, dass es für den Menschen eindeutig erkennbar ist, welches System er zu einem gegebenen Zeitpunkt beeinflusst.

- **MMS → Unterlagen:** Die Beschreibung der MMS in den Unterlagen dient u. a. dem Menschen dazu, sich mit der MMS vertraut zu machen, z. B. vor Durchführung seiner Aufgabe. Hierbei bestimmt die Gestaltung der MMS ähnlich wie beim System

maßgeblich ihre Darstellung bzw. Beschreibung in den Unterlagen. Das Design einer MMS, welches die Benutzerfreundlichkeit fördert, beispielsweise anhand eines klaren und strukturierten Aufbaus der Bedienoberfläche sowie einer ergonomisch optimalen Anordnung und Gestaltung der Bedienelemente auf der Bedienoberfläche, spiegelt sich entsprechend in den Unterlagen wider. Dies fördert das Verständnis der MMS beim Menschen. Grundsätzlich ist es auch möglich, dass die MMS auf die Unterlagen verweist. Zum Beispiel, um auf zusätzliche Informationen hinzuweisen, die an der MMS (z. B. aus Platzgründen) nicht dargestellt werden können, oder um ein schnelles Auffinden für die Durchführung der Aufgabe relevanter Informationen in den Unterlagen zu ermöglichen.

Zur besseren Übersicht sind die betrachteten Beziehungen zwischen den Teilelementen der einzelnen Komponenten und die Beziehungen zwischen den Komponenten des MEDIC-Arbeitssystemmodells in Tab. 3.1 als eine Interrelationsmatrix dargestellt. Die Einträge in dieser Matrix in Tab. 3.1 stellen die zuvor beschriebenen relevanten Aspekte dar, welche die zuvor genannten Beziehungen im MEDIC-Arbeitssystemmodell im Hinblick auf eine Minimierung/Vermeidung von Personalfehlhandlungen an MMS beeinflussen.

Tab. 3.1 Interrelationsmatrix des MEDIC-Arbeitssystemmodells

(Die Beziehungen zwischen den Komponenten sind zeilenweise zu betrachten, d. h. von einem Zeilenelement zu einem Spaltenelement. Die Beziehungen zwischen den Teilelementen der Komponenten betreffende Aspekte sind in der Diagonale beschrieben.)

	Mensch	**MMS**	**System**	**Unterlagen**
Mensch	nicht betrachtet	nicht betrachtet	nicht betrachtet	nicht betrachtet
MMS	Mentale und physische Zugänglichkeit	Gestaltung und Design der MMS	Darstellung des Systems auf der MMS	Darstellung der MMS in den Unterlagen
System	Mentale und physische Zugänglichkeit	Darstellung des Systems auf der MMS	Design des Systems	Darstellung des Systems in den Unterlagen
Unterlagen	Verständnis der Anweisungen	Integration der Anweisungen in der MMS	Darstellung des Systems in den Unterlagen	Gestaltung und Design der Unterlagen

Der Grad der Berücksichtigung der in Tab. 3.1 angegebenen Aspekte bei der Auslegung der MMS ist abhängig von der Art der MMS und von der spezifischen Aufgabe, welche an dieser MMS ausgeführt werden soll.

Obwohl es beispielweise für Wartungsaufgaben an der Servicestation softwarebasierter Leittechniksysteme nicht erforderlich ist, das System auf der MMS darzustellen, muss der Mensch über ein fundiertes Systemverständnis verfügen. Denn ein schlechtes Systemverständnis des Menschen kann zu Fehlern bei der Bedienung des Systems an der MMS führen. Auch ein Design der MMS, welches benutzerfreundlich und verständlich ist, fördert eine möglichst fehlerfreie Handhabung durch den Menschen an der MMS. Die Beschreibung des Systems in den Unterlagen und die Integration der Unterlagen in der MMS sind weitere relevante Aspekte zur Unterstützung einer fehlerfreien Handlung des Menschen an der MMS. Daraus folgt, dass die Eignung von präventiven technischen Vorkehrungen zur Vermeidung von Personalfehlhandlungen an MMS anhand der Eigenschaften der Beziehungen zwischen den Komponenten des Mensch-Maschine-Systems, d. h. der Einträge der Interrelationsmatrix in Tab. 3.1, charakterisiert werden kann.

3.3.2.3 Definitionen von Attributen zur Charakterisierung der MEDIC-Interrelationsmatrix

Neben den erforderlichen Kenntnissen, Fertigkeiten und Fähigkeiten des Menschen für die Ausführung der Aufgabe an der MMS werden die Beziehungen des Menschen mit der MMS, dem System und den Unterlagen bei der Durchführung der Aufgabe vor allem durch situative Aspekte und seine individuellen Leistungsfaktoren (Motivation, Stress, Ermüdung, etc.) beeinflusst.

Im Rahmen der MEDIC-Analysemethode werden, wie bereits in Kapitel 3.3.2.1 erwähnt, solche situativen und individuellen Leistungsfaktoren des Menschen nicht berücksichtigt. Aus diesem Grund wird in der MEDIC-Analysemethode angenommen, dass der Mensch die erforderlichen Qualifikationen/Eignungen, Fähigkeiten, Fertigkeiten und Kenntnisse besitzt, um die Aufgabe zu erfüllen. Die Beziehungen zwischen dem Menschen und den Komponenten des MEDIC-Arbeitssystemmodells werden somit nicht betrachtet. Der Schwerpunkt der hier durchgeführten Untersuchungen liegt auf den potenziellen Ursachen für Fehlhandlungen des Menschen an der MMS in Bezug auf Mängel technischer Vorkehrungen gegen Fehlhandlungen an der MMS.

Für die Bewertung der Eignung von technischen Vorkehrungen gegen Fehlhandlungen an Mensch-Maschine-Schnittstellen wurden Attribute definiert, welche die Einträge der Interrelationsmatrix in Tab. 3.1 charakterisieren. Die eingeführten Attribute werden den jeweiligen Beziehungen zwischen den Komponenten des MEDIC-Arbeitsmodellsystems zugeordnet.

Tab. 3.2 gibt einen Überblick über die definierten Attribute und deren Zuordnung zu den betrachteten Beziehungen für den Fall, dass situative Aspekte und individuelle Leistungsfaktoren des Menschen, wie bereits erwähnt, nicht berücksichtigt werden.

Tab. 3.2 Definition der Attribute zur Charakterisierung der Beziehungen zwischen den Komponenten des MEDIC-Arbeitssystemmodells

(Das Attribut „Eindeutigkeit und Unterscheidbarkeit“ ist aus Platzgründen unter dem Begriff „Eindeutigkeit“ in der Tabelle eingetragen)

	Mensch	**MMS**	**System**	**Unterlagen**
Mensch	nicht betrachtet	nicht betrachtet	nicht betrachtet	nicht betrachtet
MMS	physische Zugänglichkeit mentale Zugänglichkeit	Konsistenz Korrektheit Übersichtlichkeit Eindeutigkeit Vorhandensein	Konsistenz Korrespondenz Vollständigkeit	Konsistenz Korrespondenz
System	physische Zugänglichkeit mentale Zugänglichkeit	Konsistenz Korrespondenz	Konsistenz Korrektheit Übersichtlichkeit Eindeutigkeit Vorhandensein	Konsistenz Korrespondenz
Unterlagen	physische Zugänglichkeit mentale Zugänglichkeit	Konsistenz Korrespondenz Vollständigkeit	Konsistenz Korrespondenz	Konsistenz Korrektheit Übersichtlichkeit Eindeutigkeit Vorhandensein

Nachfolgend werden die in Tab. 3.2 verwendeten Attribute definiert. Bei den Definitionen wird besonders auf als bildschirmgestützte Oberflächen realisierte MMS abgehoben. Sie können sinngemäß auf andere Arten von MMS (z. B. hardwarebasierte MMS) übertragen werden.

- Das Attribut „Konsistenz“ bezieht sich auf die Tatsache, dass die Komponenten „MMS“, „System“ und „Unterlagen“ sowie ihre Beziehungen zueinander möglichst einheitlich zu gestalten sind. Beispielsweise sollten grafische Darstellungen und Textbeschreibungen in MMS die gleichen Symbole verwenden, wenn sie sich auf die gleiche Sache beziehen (der Begriff „Symbole“ bezieht sich hier auf sowohl grafische als auch textliche Elemente oder Bezeichnungen). Dies dient der Wiedererkennbarkeit der Symbole, verhindert Verwechslungen und dient damit der

allgemeinen Benutzerfreundlichkeit und Bedienbarkeit der MMS. Die konsistente Verwendung von Symbolen betrifft nicht nur die Wahl des Symbols selbst, sondern auch dessen Anordnung auf dem Bildschirm, insbesondere im Zusammenspiel mit anderen Elementen auf dem Bildschirm. Dieses Konsistenzprinzip kann sinngemäß auch auf die anderen Elemente des Arbeitssystems und auf die Beziehungen zwischen den Komponenten des Arbeitssystems ausgeweitet werden. Beziehen sich z. B. sowohl die Unterlagen als auch die MMS auf ein bestimmtes Element im System, ist Konsistenz in den Beziehungen „Unterlagen → System“ und „MMS → System“ herzustellen, indem beispielsweise das gleiche Symbol für dieses Element in den Unterlagen und auf der MMS verwendet wird. Für Wartungstätigkeiten an einem Leittechniksystem unterstützt eine konsistente Anordnung und Kennzeichnung der Komponenten im Leittechnikschrank eine bessere Nachvollziehbarkeit der durchzuführenden Aufgabe an der MMS.

- Das Attribut „Korrektheit“ bezieht sich darauf, dass die Komponenten „MMS“, „System“ und „Unterlagen“ möglichst fehlerfrei entwickelt bzw. implementiert werden müssen. Wird z. B. ein falsches Symbol in der MMS verwendet, kann dies zu fehlerhaften Handlungen des Personals führen, deren Ursache für den Menschen nicht sofort ersichtlich ist. Des Weiteren können fehlerhafte Formulierungen in den Unterlagen, z. B. in den Anweisungen, zu fehlerhaften Handlungen des Menschen an der MMS führen.

- Das Attribut „Übersichtlichkeit“ betrifft die Auswahl und die Darstellung der Interaktionsmöglichkeiten an der MMS. Beide Aspekte zielen darauf ab, dem Menschen den Zugriff bzw. den Zugang auf die für die Ausführung der gegebenen Aufgabe erforderlichen Informationen und Elemente an der MMS zu erleichtern. Dies kann beispielsweise durch eine strukturierte Anordnung der Elemente auf der MMS oder durch die Vermeidung überflüssiger Elemente auf der MMS erreicht werden. In Bezug auf die Auslegung des Systems fördert beispielsweise die Aufteilung eines komplex aufgebauten Systems in zueinander funktional getrennte Teilsysteme seine Übersichtlichkeit. Hinsichtlich der Unterlagen dient eine strukturierte Aufteilung der Informationen der Übersichtlichkeit, z. B. durch Verwendung eines Inhaltsverzeichnisses. Dies erleichtert dem Menschen den schnellen Zugang zu den für die Durchführung der Aufgabe erforderlichen Informationen.

- Die Attribute „Eindeutigkeit“ und „Unterscheidbarkeit“ betreffen die Elemente an der MMS und zielen darauf ab, dass diese eindeutig sein müssen, um Fehlhandlungen an der MMS zu minimieren bzw. zu vermeiden. Die Unterscheidbarkeit der Symbole

verhindert beispielsweise Verwechslungen und damit mögliche Fehler, z. B. bei der Eingabe von Werten in einer Eingabemaske. Die Unterscheidbarkeit und die Eindeutigkeit der verwendeten Symbole und grafischen Elemente zur Darstellung der Informationen in den Unterlagen fördert ebenfalls die Minimierung bzw. Vermeidung von Fehlhandlungen an MMS. Systemelemente wie beispielsweise Anzeigeelemente vor Ort sollten eindeutig gekennzeichnet und voneinander unterscheidbar sein. Dies erleichtert dem Menschen deren Zuordnung im Kontext der durchzuführenden Aufgabe.

- Das Attribut „Vorhandensein“ bezieht sich einerseits auf die Tatsache, dass die zur Ausführung einer bestimmten Aufgabe an der MMS notwendigen Interaktionsmöglichkeiten für den Menschen vorhanden sein müssen. Dies schließt auch ein, dass die hierfür notwendigen Systemelemente (z. B. Messgrößen) im Systemdesign berücksichtigt wurden und im System realisiert sind.
  Andererseits bezieht sich das Attribut „Vorhandensein“ auf die Tatsache, dass alle für die Durchführung der Aufgabe erforderlichen Unterlagen vorhanden sein und die erforderlichen Informationen und Beschreibungen in diesen dargestellt werden müssen.
  - Anhand des Attributs „Vorhandensein“ können Arbeitssysteme dahingehend analysiert werden, ob nicht vorhandene Elemente fehlervermeidend bei der Bedienung des Systems gewesen wären.
- Das Attribut „Korrespondenz“ betrifft die Tatsache, dass für die Komponenten „System“, „MMS“ und „Unterlagen“ des MEDIC-Arbeitssystemmodells neben der einheitlichen und eindeutigen Verwendung von Symbolen auch die Wahl der Symbole an sich eine wichtige Rolle spielt. Wo immer möglich, sollten Symbole verwendet werden, deren Bedeutung leicht ersichtlich ist, weil z. B. grafische Darstellungen reale Äquivalente haben, oder weil diese Symbole durch Konventionen/Normen bekannt sind. Im Gegensatz zur Konsistenz, die sich auf eine einheitliche Verwendung verwandter Elemente (z. B. Abbildungen oder Markierungen in den Dokumenten und in der MMS) bezieht, bezieht sich die Korrespondenz auf eine Verbindung zwischen einem verwendeten Symbol an der MMS und dem Element in der realen Welt, auf das es verweist.
- Das Attribut „Vollständigkeit“ bezieht sich auf die Tatsache, dass die Komponenten „System“, „Unterlagen“ und „MMS“ ihre Funktionen im Zusammenhang mit der zu bewältigenden Aufgabe an der MMS erfüllen können. In Bezug auf die Unterlagen

bedeutet dies beispielsweise, dass alle notwendigen Informationen in den Dokumenten vorhanden sein müssen und dass alle erforderlichen Tätigkeitsschritte in den Arbeitsanweisungen beschrieben sein müssen. Die MMS muss hierbei die Ausführung aller erforderlichen Tätigkeitsschritte ermöglichen. Das System muss funktionsfähig und verfügbar sein.

- Das Attribut „physische Zugänglichkeit“ bezieht sich sowohl auf den physischen Zugang als auch auf die Bedienbarkeit bzw. Anwendbarkeit der Interaktionsobjekte für die Durchführung der Aufgabe an der MMS. Die Darstellung von Informationen in den Unterlagen beeinflusst ihre Anwendbarkeit durch den Menschen bei der Durchführung der Aufgabe an der MMS. In den Unterlagen müssen z. B. ausreichende Schriftgrößen verwendet werden, damit diese für den Benutzer lesbar sind. Auch die Gestaltung der MMS beeinflusst seine Bedienbarkeit. Dies betrifft beispielsweise die Position der Bedienelemente auf der MMS. Ist die MMS als Hardwareschnittstelle realisiert, z. B. für Wartungsaufgaben an einem System, ist es notwendig für die Durchführung der Aufgabe einen physischen Zugang zum System sicherzustellen.
- Das Attribut „mentale Zugänglichkeit“ bezieht sich auf das Verständnis des Systems, der MMS und der Unterlagen durch den Menschen. Insbesondere sollen die MMS und die Unterlagen so ausgelegt sein, dass das Verständnis beim Menschen bzw. die Bildung eines mentalen Modells erleichtert wird. In /NUR 02/ wird beispielsweise das sogenannte „Coherence Mapping“ als Charakteristik eingeführt, die bestimmt, inwieweit die Informationsdarstellung für den Menschen verständlich ist. Es ist hierbei zu erwähnen, dass die zuvor definierten Attribute zur Charakterisierung der Beziehungen zwischen den Elementen der MMS sowie der Beziehungen zwischen den Komponenten des MEDIC-Arbeitssystems bei ihrer Erfüllung die mentale Zugänglichkeit der MMS beim Menschen fördern. Sie können zur Charakterisierung der mentalen Zugänglichkeit ebenfalls herangezogen werden.

3.3.3 Die MEDIC-Bewertungsmethode

Im Rahmen der MEDIC-Bewertungsmethode wird davon ausgegangen, dass die spezifischen Attribute zur Charakterisierung der Einträge der Interrelationsmatrix des MEDIC-Arbeitssystems, wie in Kapitel 3.3.2.3 (siehe Tab. 3.2) definiert, erfüllt werden sollen, um Personalfehlhandlungen an MMS zu vermeiden oder zu minimieren.

Die MEDIC-Bewertungsmethode besteht darin, den Erfüllungsgrad der in Tab. 3.2 eingeführten Attribute für ein Arbeitssystem zu bewerten. Hierzu werden die Komponenten

„Unterlagen“, „System“, „MMS“ und „Mensch“ gemäß dem MEDIC-Arbeitssystemmodell des zu bewertenden Arbeitssystems identifiziert. Bei der Bewertung von technischen Vorkehrungen gegen Fehlhandlungen an der MMS eines Arbeitssystems mit der MEDIC-Bewertungsmethode wird daher überprüft, zu welchem Grad die eingeführten Attribute (Konsistenz, Korrektheit, …) die Beziehungen zwischen den Komponenten „Unterlagen“, „System“ und „MMS“ des Arbeitssystems erfüllen. Der Erfüllungsgrad dieser Attribute kann als Bewertungsmaßstab für die Vermeidung bzw. Minimierung von Personalfehlhandlungen an der MMS des zugehörigen Arbeitssystems herangezogen werden.

Zur Ermittlung des Erfüllungsgrades dieser Attribute sind geeignete Bewertungskriterien vom Bewerter zu entwickeln. Hierfür kann ein Katalog von Bewertungskriterien (oder ein Fragebogen) für jedes definierte Attribut, z. B. auf Basis von Anforderungen zur Auslegung von MMS unter Berücksichtigung menschlicher Faktoren, wie beispielsweise in Kapitel 2.3 beschrieben, entwickelt werden. Das Attribut für die betrachtete Beziehung des MEDIC-Arbeitssystemmodells gilt dann als zutreffend, wenn alle dem Attribut zugeordneten Kriterien als erfüllt anzusehen sind. Die Bewertung erfolgt hierbei als Expertenschätzung. Im Rahmen der MEDIC-Bewertungsmethode wurden Kriterien zur Ermittlung des Erfüllungsgrades der eingeführten Attribute aus der NUREG 0700-Richtlinie /NUR 02/ abgeleitet (siehe Kapitel 4.4.1).

Um die Konsistenz einer als graphische Oberfläche realisierten MMS zu überprüfen, kann beispielsweise als Kriterium die Konsistenz der Darstellung der Informationen auf der Benutzeroberfläche überprüft werden, d. h. es sollten die gleichen Symbole (Zeichen, Schriftfarbe, ...) zur Darstellung gleicher Informationen verwendet werden. Es sollte auch auf ein konsistentes Design (Aussehen, Farbe usw.) der Steuerelemente auf der Benutzeroberfläche sowie auf die Beibehaltung einer einheitlichen Platzierung der Bedienelemente auf der Benutzeroberfläche geachtet werden. Hinsichtlich der Unterlagen sollte ein einheitliches Erscheinungsbild der Dokumente verwendet werden, die sich auf denselben Punkt beziehen, um die Konsistenz der Unterlagen zu gewährleisten.

Im nachfolgenden Abschnitt wird detailliert auf die Anwendung der MEDIC-Bewertungsmethode insbesondere auf die Herleitung der Bewertungskriterien eingegangen.

3.4 Anwendung der MEDIC-Bewertungsmethode

3.4.1 Der MEDIC-Anwendungsleitfaden

Ein Anwendungsleitfaden für die MEDIC-Bewertungsmethode wurde im Rahmen dieses Vorhabens entwickelt, um eine einheitliche Verwendung der Methode und eine systematische Vorgehensweise bei ihrer Anwendung zu ermöglichen. In Abb. 3.6 sind die durchzuführenden Schritte bei der Anwendung der MEDIC-Bewertungsmethode übersichtlich dargestellt.

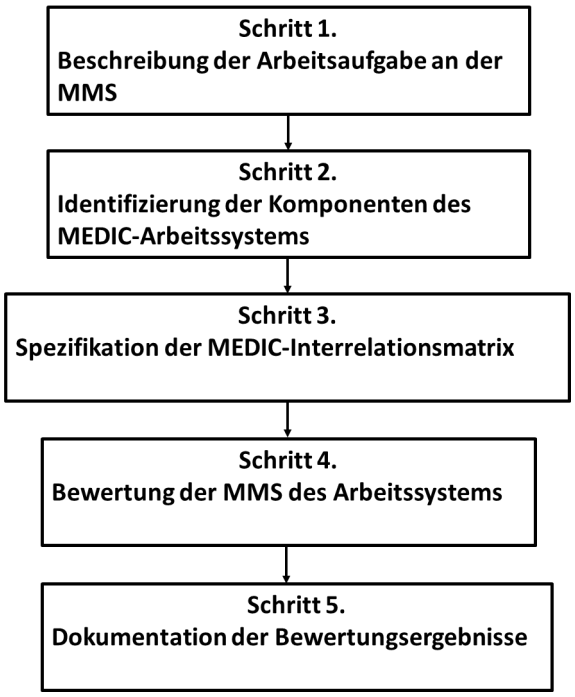

Abb. 3.6 Überblick über die durchzuführenden Schritte bei der Anwendung der MEDIC-Bewertungsmethode

Nachfolgend werden die fünf durchzuführenden Schritte bei der Anwendung der MEDIC-Bewertungsmethode beschrieben.

- **Schritt 1: Beschreibung der Arbeitsaufgabe**
  In diesem Schritt ist die auszuführende Arbeitsaufgabe an der MMS zu beschreiben. Hierzu zählen beispielsweise eine Wartungsaufgabe an einem digitalen Leittechniksystem oder eine Überwachungs- und Steuerungsaufgabe an einem verfahrenstechnischen System, welches von einem digitalen Leittechniksystem gesteuert wird. Als MMS werden die in Abb. 2.1 dargestellten typischen MMS softwarebasierter Leittechniksysteme betrachtet.

- **Schritt 2: Identifizierung der Komponenten des MEDIC-Arbeitssystems**
  Grundlage für die MEDIC-Bewertungsmethode ist das in Kapitel 3.3.2.1 eingeführte MEDIC-Arbeitssystemmodell, welches aus den Komponenten „Unterlagen“, „System“, „MMS“ und „Mensch“ besteht. In diesem Schritt sind die Komponenten „MMS“, „System“, „Unterlagen“ und „Mensch“ gemäß dem MEDIC-Arbeitssystemmodell für die Durchführung der Arbeitsaufgabe an der MMS anzugeben und zu beschreiben.

- **Schritt 3: Spezifikation der MEDIC-Interrelationsmatrix**
  Zur Charakterisierung der Beziehungen zwischen den Komponenten des eingeführten MEDIC-Arbeitssystemmodells im Rahmen der MEDIC-Bewertungsmethode wurde die MEDIC-Interrelationsmatrix definiert (siehe Kapitel 3.3.2.2). Den Einträgen dieser MEDIC-Interrelationsmatrix sind Attribute zur Charakterisierung der Beziehungen zwischen den Komponenten des MEDIC-Arbeitssystemmodells zugeordnet worden. Diese in der MEDIC-Bewertungsmethode eingeführte Interrelationsmatrix stellt einen generischen Rahmen zur Bewertung von Arbeitssystemen dar. Abhängig von der durchzuführenden Aufgabe an der MMS des zugrunde liegenden Arbeitssystems sind in diesem Schritt die zu berücksichtigenden Beziehungen zwischen den einzelnen Komponenten des Arbeitssystems und demzufolge die Interrelationsmatrix sowie die Attribute zur Charakterisierung der Beziehungen zwischen den Komponenten des MEDIC-Arbeitssystems zu spezifizieren.

- **Schritt 4: Bewertung der MMS des Arbeitssystems**
  Die im Schritt 3 spezifizierte Interrelationsmatrix stellt die Grundlage für die Bewertung der realisierten technischen Vorkehrungen zur Vermeidung von Fehlhandlungen bei der Erledigung der Arbeitsaufgabe an der MMS des zugrundeliegenden Arbeitssystems dar. In diesem Schritt wird überprüft, inwieweit die eingeführten Attribute zur Charakterisierung bzw. zur Kennzeichnung der Komponenten des Arbeitssystems bzw. der Beziehungen zwischen den Komponenten des Arbeitssystems, in dem die zugrundeliegende MMS eingebettet ist, zutreffen. Hierzu ist anhand von relevanten kerntechnischen Regelwerken bzw. Normen mit Auslegungsanforderungen an MMS insbesondere unter Berücksichtigung menschlicher Aspekte (z. B. /NUR 02/, /EPRI 04/ oder /KTA 17b/) ein entsprechender Kriterien- bzw. Fragenkatalog für das betrachtete Attribut zu entwickeln. Das Attribut für die betrachtete Komponente bzw. für die betrachtete Beziehung des MEDIC-Interaktionsmodells gilt dann als zutreffend, wenn alle dem Attribut zugeordneten Kriterien als erfüllt anzusehen sind. Nicht erfüllte Kriterien bzw. teilweise erfüllte Kriterien sind als potenziell fehlerverursachend an der MMS zu werten. Eine in sich konsistente Darstellung und

Verwendung verwandter Elemente auf einer Bedienoberfläche für Steuerungsaufgaben kann beispielsweise das Potenzial an Fehlhandlungen des Bedienpersonals minimieren. Im Rahmen der MEDIC-Bewertungsmethode wird dann überprüft, inwieweit das Attribut „Konsistenz“ für die Steuerelemente auf der Benutzeroberfläche zutrifft. Der Erfüllungsgrad des Attributs „Vorhandensein“ kann z. B. dadurch bewertet werden, in dem überprüft wird, ob alle Interaktionsmöglichkeiten oder Interaktionsobjekte (z. B. Eingabefelder, Anzeigen für Systemrückmeldungen, Quittierung von Meldungen, etc.), die zur Erledigung der Aufgabe notwendig sind, an der Benutzerschnittstelle vorhanden sind. Fehlende oder unvollständige Interaktionsmöglichkeiten oder Interaktionsobjekte sind fehlerfördernd. Daneben ist auch die Verfügbarkeit von Möglichkeiten zur Korrektur oder Vermeidung von Fehleingaben an der Benutzerschnittstelle zu überprüfen.

- **Schritt 5: Dokumentation des Bewertungsergebnisses**
  In diesem Schritt wird das Bewertungsergebnis auf einem Bewertungsbogen zusammengefasst. Bildausschnitte der Komponenten „MMS“, „Unterlagen“ und „System“ sind zur Dokumentation der Bewertung zu erstellen und dem MEDIC-Bewertungsbogen als Anhang beizufügen.

3.4.2 Anwendungsbeispiele

3.4.2.1 Betrachtete Anwendungsfälle

Mit der entwickelten MEDIC-Bewertungsmethode können sowohl bereits eingesetzte MMS als auch in der Entwicklung befindliche MMS hinsichtlich der Eignung der technischen Vorkehrungen gegen Personalfehlhandlungen bewertet werden. Hierbei kann die MEDIC-Bewertungsmethode auch iterativ eingesetzt werden, so dass potenziell entdeckte Mängel bei den technischen Vorkehrungen nacheinander verbessert werden können.

Für die Bewertung von in der Entwicklung befindlichen MMS mit der MEDIC-Bewertungsmethode wurde im Rahmen dieses Vorhabens ein eigenständiges Arbeitssystem für eine Steuerungsaufgabe an einer MMS entwickelt. Das Arbeitssystem und die dem Arbeitssystem zugehörige MMS sind angelehnt an eine typische MMS softwarebasierter Leittechniksysteme für Steuerungsaufgaben wie im Kapitel 2.1.2 beschrieben. Dieses entwickelte Arbeitssystem, „MMS-Warte“ genannt, wurde anschließend mit der MEDIC-

Bewertungsmethode bewertet. In Kapitel 3.4.2.2 sind die Ergebnisse dieser Arbeitsschritte dargestellt.

Für die Anwendung der MEDIC-Bewertungsmethode zur Bewertung von bereits eingesetzten MMS wurden im Rahmen dieses Vorhabens MMS betrachtet, die als ursächlich für Personalfehlhandlungen bei meldepflichtigen Ereignissen in Kernkraftwerken identifiziert wurden. Hierzu wurde nach entsprechenden relevanten Ereignissen recherchiert. Durch eine nachträgliche Bewertung dieser Ereignisse unter Zuhilfenahme der MEDIC-Bewertungsmethode lassen sich die Ursachen für die festgestellten Personalfehlhandlungen in das MEDIC-Analysemodell einordnen und Rückschlüsse auf Designmängel bei den technischen Vorkehrungen gegen Fehlhandlungen an der zugrunde liegenden MMS ziehen. In Kapitel 3.4.2.2 sind die Ergebnisse dieser Arbeitsschritte dargestellt.

Als weiteres Anwendungsfeld wurde im Rahmen dieses Vorhabens die Eignung der MEDIC-Bewertungsmethode zur Bewertung von Arbeitssystemen für Wartungs- und Instandhaltungsaufgaben an einem softwarebasierten Leittechniksystem erprobt. Hierbei wurde insbesondere auf die Bedeutung der Arbeitsanweisungen bei der Durchführung solcher Tätigkeiten abgehoben, da Wartungs- und Instandhaltungsarbeiten überwiegend anhand von Tätigkeitsanweisungen durchgeführt werden, welche von einem regelbasierten Verhalten[14] der Ausführenden ausgehen. In Kapitel 3.4.2.3 sind die Ergebnisse der MEDIC-Bewertung für ein hierfür eigenentwickeltes Arbeitssystem dargestellt.

3.4.2.2 Anwendungsbeispiel für die Bewertung eines Arbeitssystems: Das Wassertanksystem

Um die Anwendbarkeit der MEDIC-Bewertungsmethode zu erproben, wurde mit dem MEDIC-Analysewerkzeug das Arbeitssystem „MMS-Warte“ für die Überwachung und Steuerung eines einfachen Wassertanksystems entwickelt.

[14] Regelbasiertes Verhalten: Verhalten meist weniger vertrauter Aufgaben gegenüber, die auf eine normale Erfahrung und Fähigkeiten des Betreffenden basieren. /VDI 02/

3.4.2.2.1 Beschreibung des Arbeitssystems „MMS-Warte“

Das Arbeitssystem „MMS-Warte“ besteht gemäß dem MEDIC-Arbeitssystemmodell (siehe Kapitel 3.3.2) aus den Komponenten „System“, „MMS“, „Unterlagen“ und „Mensch“.

Als „System“ wird ein Wassertanksystem zugrunde gelegt, welches auf dem von der GRS entwickelten System „TeSys“ /GRS 21/ basiert.

Das Wassertanksystem besteht aus zwei mit Wasser gefüllten und auf unterschiedlichen Höhen aufgestellten Behältern, die miteinander durch zwei Schlauchleitungen verbunden sind. An den Behältern ist jeweils ein handbetätigtes Ablassventil zur Entleerung der Behälter angebracht. Von dem Ablassventil des oberen Behälters (Behälter 1) zweigt eine Verbindungsleitung in die Einfüllöffnung des unteren Behälters (Behälter 2) ab. In dieser Verbindungsleitung ist ein motorgesteuertes Regelventil eingebaut, welches als Absperrventil gesteuert wird. Durch Öffnen des Ablassventils am oberen Behälter fließt das Wasser in die Verbindungsleitung zwischen oberem und unterem Behälter und bei geöffnetem Absperrventil aufgrund der Geodätik in den unteren Behälter ein. Zum Fördern des Wassers vom unteren zum oberen Behälter ist eine motorgetriebene Förderpumpe mit vorgeschaltetem Rückschlagventil in der Verbindungsleitung zwischen dem Ablassventil am unteren Behälter und der Einfüllöffnung des oberen Behälters vorhanden.

Die Behälterfüllstände werden auf Unterschreiten eines Minimalwerts (L-MIN) bzw. Überschreiten eines Maximalwertes (L-MAX) mittels Füllstandssensoren überwacht. Die verfahrenstechnische Aufgabe der Überwachung und Steuerung des Wassertanksystems besteht darin, eine Überfüllung (Füllstand > L-MAX) bzw. zu starke Entleerung (Füllstand <L-MIN) der Behälter zu verhindern. Die Überwachung des Füllstands L-MIN des unteren Behälters dient auch dazu, die Förderpumpe vor Kavitation zu schützen. Hierzu werden die Förderpumpe (ein-/ausgeschaltet) und das Absperrventil (offen/geschlossen) in den Verbindungsleitungen zwischen den beiden Behältern abhängig von den Behälterfüllstandsgrenzwerten gesteuert.

Erreicht der Füllstand im unteren Behälter den Grenzwert L-MAX, so wird die Förderpumpe automatisch gestartet und das Wasser vom unteren in den oberen Behälter zurückgefördert. Die Förderpumpe wird bei Erreichen des Füllstandes L-MIN im unteren Behälter oder L-MAX im oberen Behälter abgeschaltet.

Erreicht der Füllstand im oberen Behälter den Grenzwert L-MAX, so wird das Absperrventil geöffnet und das Wasser fließt vom oberen in den unteren Behälter. Das Absperrventil wird bei Erreichen des Füllstandes L-MAX im unteren Behälter geschlossen.

Im Rahmen der Entwicklung des Arbeitssystems „MMS-Warte“ wurde der verfahrenstechnische Prozess (Wasserkreislauf mit Behältern, Pumpe und Ventilen) und die leittechnische Ansteuerung des Wassertanksystems (Ansteuerung der Pumpe und des Absperrventils über die Füllstandsgrenzwerte L-MIN und L-MAX der Behälter) auf Basis der Spezifikationen in /GRS 21/ mit der Komponente MEDIC-MMS des MEDIC-Analysewerkzeugs simuliert. Nähere Details zum MEDIC-Analysewerkzeug und zu seinem Einsatzzweck im Rahmen des Vorhabens sind im Kapitel 4 beschrieben.

In diesem Anwendungsbeispiel wird angenommen, dass die Überwachung und Steuerung des Wassertanksystems, ähnlich wie in einem Kernkraftwerk, über die Füllstandsgrenzwerte der Behälter gestaffelt erfolgt. Hierbei sind Füllstandsgrenzwerte für automatische Maßnahmen vorgesehen, welche das Schließen des Absperrventils sowie das Abschalten der Förderpumpe auslösen. Dies dient zum einen dem Aggregateschutz der Förderpumpe, um diese vor Kavitationsschäden zu schützen, zum anderen wird auch eine Überfüllung der Behälter dadurch verhindert.

Die Aufgabe des Menschen bei der Bedienung des Wassertanksystems besteht darin, die Wasserfüllstände der Tanks zu überwachen und das Absperrventil (Öffnen/Schließen) oder die Pumpe (Starten/Stoppen) durch Betätigen der Soft-Control-Tasten auf der MMS vor dem Ansprechen der Füllstandgrenzwerte für die automatischen Maßnahmen entsprechend zu aktivieren. Dem Menschen stehen hierzu Unterlagen zur Verfügung, welche Systembeschreibungen und Arbeitsanweisungen enthalten.

In Abb. 3.7 ist ein Überblick der als graphische Benutzeroberfläche entwickelten MMS des Wassertanksystems dargestellt.

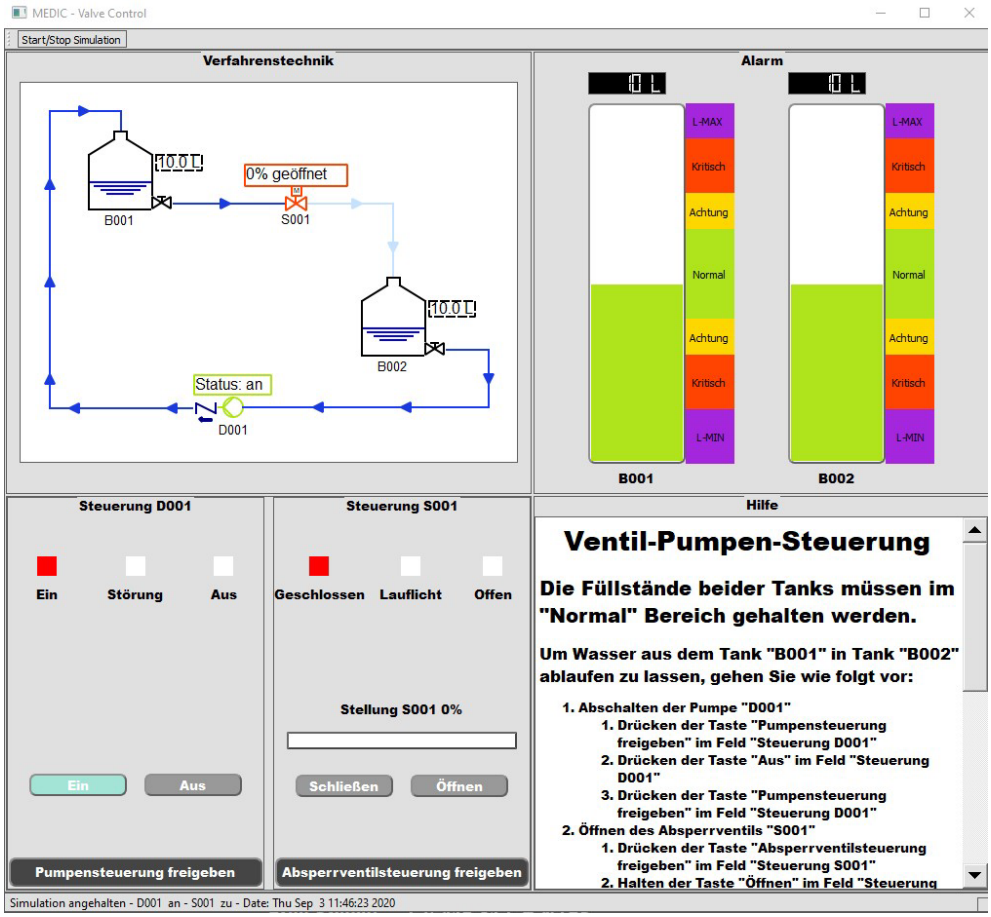

Abb. 3.7 Graphische Benutzeroberfläche der MMS des Wassertanksystems

Die Benutzeroberfläche ist in vier Bereiche unterteilt. Der Systemaufbau ist in dem verfahrenstechnischen Bereich abgebildet. In dem Alarmbereich sind füllstandsabhängige Alarmanzeigen der beiden Behälter dargestellt. Die Soft-Control-Tasten zur Steuerung der Förderpumpe und des Absperrventils sind dem Steuerungsbereich der graphischen Oberfläche zugeordnet. Zur Betätigung der Pumpe bzw. des Absperrventils müssen zuvor die Steuerungen der Pumpe bzw. des Absperrventils durch Betätigen der zugehörigen Freigabetasten („Pumpensteuerung freigeben“ bzw. „Absperrventilsteuerung freigeben“) freigegeben werden. Anweisungen, Beschreibungen und Warnmeldungen des Wassertanksystems sind im Hilfebereich der graphischen Bedienoberfläche integriert. Zusätzlich zu den im Hilfebereich der graphischen Oberfläche integrierten Hilfen sind im verfahrenstechnischen Bereich sogenannte Tooltips zur Beschreibung der verfahrenstechnischen Komponenten und deren Aufgabe integriert. Diese Tooltips sind als Hover-over-Elemente realisert. Sie dienen der Information des Menschen und erscheinen, sobald der Mensch den Mauszeiger über die entsprechenden verfahrenstechnischen Komponenten bewegt.

Im Alarmbereich sind die verschiedenen Alarmzustände, welche anhand von definierten Füllstandsgrenzwerten festgelegt sind, farblich kodiert. Dies dient dazu, den Menschen durch optische Anzeigen auf kritische Zustände aufmerksam zu machen und sein Situationsbewusstsein bei der Erledigung der Aufgabe zu verbessern. Zusätzlich zu den optischen Anzeigen wird der Mensch ebenfalls akustisch durch einen Signalton vor kritischen Zuständen gewarnt. Aus diesen abhängig vom Systemzustand generierten Warnanzeigen werden dem Menschen automatisch Anweisungen/Hilfestellungen aus dem „Unterlagen"-Bereich der graphischen Bedienoberfläche eingeblendet, um das System in den Normalzustand zurück zu führen.

Die graphische Bedienoberfläche des Wassertanksystems „MMS-Warte" wurde mit der Komponente MEDIC-MMS des MEDIC-Analysewerkzeugs entwickelt. Um eine unabhängige Bewertung des Arbeitssystems „MMS-Warte" mit der MEDIC-Bewertungsmethode zu gewährleisten, wurden für die Entwicklung der „MMS-Warte" und für die Bewertung der „MMS-Warte" verschiedene Personen des MEDIC-Projektteams eingesetzt.

3.4.2.2.2 Bewertung der MMS des Wassertanksystems mit der MEDIC-Bewertungsmethode

Im vorangegangenen Abschnitt wurde bereits die Aufgabe des Menschen an der Mensch-Maschine-Schnittstelle des Wassertanksystems beschrieben. Entsprechend dem im Kapitel 3.4.1 dargestellten MEDIC-Anwendungsleitfaden sind im nächsten Schritt die Komponenten des für die Bewertung der MMS des Wassertanksystems zugrundeliegenden Arbeitssystems „MMS-Warte" zu identifizieren.

Für das Arbeitssystem „MMS-Warte" ist das Wassertanksystem das zu bedienende System. Der verfahrenstechnische Anzeigebereich, der Alarmbereich und der Steuerungsbereich der graphischen Bedienoberfläche (siehe Abb. 3.7) werden hier als MMS des Arbeitssystems „MMS-Warte" betrachtet. Die in der graphischen Bedienoberfläche integrierten Hilfetexte, Beschreibungen und Anweisungen stellen gemäß dem MEDIC-Arbeitssystemmodell die Unterlagen des Arbeitssystems „MMS-Warte" dar.

Für die Bewertung der in der MMS realisierten technischen Vorkehrungen gegen Fehlhandlungen wurde die MEDIC-Interrelationsmatrix wie in Tabelle 3.2 angegeben zugrunde gelegt. Bewertungskriterien wurden aus den im Kapitel 2.3 dargestellten Anforderungen abgeleitet. In Tab. 3.3 sind die erzielten Ergebnisse der MEDIC-Bewertung des Arbeitssystems „MMS-Warte" für die Bewertung der MMS des Wassertanksystems

zusammenfassend dargestellt. Ein Attribut gilt hierbei als erfüllt, wenn es alle ihm zugrunde gelegten Bewertungskriterien erfüllt.

Tab. 3.3 Zusammenfassende Darstellung der Ergebnisse der MEDIC-Bewertung des Arbeitssystems „MMS-Warte“

Erfüllte Attribute sind mit (✓), nicht erfüllte mit (×) und nicht betrachtete Attribute mit (-) gekennzeichnet.

	Mensch	**MMS**	**System**	**Unterlagen**
Mensch	-	Nicht betrachtet	Nicht betrachtet	Nicht betrachtet
MMS	Physische Zugänglichkeit (×) Mentale Zugänglichkeit (✓)	Konsistenz (×) Korrektheit (✓) Übersichtlichkeit (×) Eindeutigkeit (×) Vorhandensein (✓)	Konsistenz (-) Korrespondenz (✓) Vollständigkeit (×)	Konsistenz (×) Korrespondenz (✓)
System	Physische Zugänglichkeit (-) Mentale Zugänglichkeit (✓)	Konsistenz (-) Korrespondenz (✓)	Konsistenz (✓) Korrektheit (✓) Übersichtlichkeit (✓) Eindeutigkeit (✓) Vorhandensein (✓)	Konsistenz (✓) Korrespondenz (✓)
Unterlagen	Physische Zugänglichkeit (×) Mentale Zugänglichkeit (✓)	Konsistenz (×) Korrespondenz (✓) Vollständigkeit (×)	Konsistenz (✓) Korrespondenz (✓)	Konsistenz (×) Korrektheit (✓) Übersichtlichkeit (×) Eindeutigkeit (✓) Vorhandensein (✓)

Nachfolgend werden exemplarisch einige in Tab. 3.3 angegebenen Ergebnisse der Bewertung der MMS des Wassertanksystems mit der MEDIC-Bewertungsmethode ausgehend von dem zugrunde gelegten Arbeitssystem „MMS-Warte“ kurz erläutert.

- **Korrespondenz:** Die verwendeten Symbole für die Wasserbehälter sind als solche erkennbar und die Fließrichtung des Wassers zwischen den beiden Behältern wird durch Pfeile angezeigt. Somit sind die Beziehungen zwischen Symbolen auf der Benutzeroberfläche und dem System, auf das sie sich beziehen, offensichtlich. Die Anordnung der verfahrenstechnischen Darstellung spiegelt die Höhenverhältnisse im System wider. Das Attribut „Korrespondenz“ ist bezogen auf die Beziehungen System → MMS und MMS→ System erfüllt.

- **Konsistenz:** Es werden verschiedene Farben verwendet, um die Öffnung des Ventils (Rot für AUF) und den Betriebszustand der Förderpumpe (Grün für EIN), obwohl diese sich auf den ähnlichen Betriebszustand beziehen. Auch die Rückmeldung des Betriebszustands der Pumpe im Steuerungsbereich der MMS stimmt nicht mit dem Betriebszustand der Pumpe überein. Eine rot leuchtende Rückmeldelampe zeigt

nämlich an, dass die Förderpumpe in Betrieb ist. Diese stimmt nicht mit der Farbe überein, die zur Anzeige des Betriebszustands „EIN“ der Förderpumpe auf der MMS verwendet wird (Grün für EIN). Es sollte der gleiche Farbcode verwendet werden, um ähnliche Betriebszustände anzuzeigen. Daraus folgt, dass das Attribut „Konsistenz“ für die MMS nicht erfüllt ist.

- **Vorhandensein:** Alle zur Erledigung der Aufgabe erforderlichen Elemente sind vorhanden. Soft Control-Elemente zur Ansteuerung der Förderpumpe und des Absperrventils mit entsprechenden Rückmeldeanzeigen sind im Bereich der Bedienelemente der MMS angeordnet. Außerdem sind Anweisungslisten mit weiteren Zusatzinformationen ebenfalls in die MMS integriert. Das Attribut „Vorhandensein“ ist für die MMS erfüllt.

Ausführlichere Erläuterungen zu den weiteren Bewertungsergebnissen der MMS des Wassertanksystems finden sich im Anhang A.1 des Berichts. Die Ergebnisse sind nach den zu betrachtenden Beziehungen zwischen den Komponenten des Arbeitssystemmodells und den diesen Beziehungen zugeordneten Attributen sortiert.

Zusammenfassend ergibt sich aufgrund der nicht erfüllten Attribute aus der MEDIC-Bewertung der MMS des Wassertanksystems, dass die für die MMS des Wassertanksystems vorgesehenen technischen Vorkehrungen gegen Personalfehlhandlungen nicht ausreichend sind, um alle durch die MEDIC-Bewertungsmethode eingeführten Attribute vollständig zu erfüllen. Demzufolge besteht Verbesserungspotenzial für die genannten technischen Vorkehrungen. Das Design der MMS wäre nun in einen weiteren Schritt unter Berücksichtigung der Ergebnisse der MEDIC-Bewertung entsprechend zu verbessern und anschließend einer weiteren MEDIC-Bewertung zu unterziehen. Dieser Vorgang wäre so lange iterativ zu wiederholen, bis alle Attribute erfüllt sind. Im Rahmen dieser Iteration können weitere Bewertungskriterien herangezogen werden.

3.4.2.3 Betrachtung von Ereignissen in Kernkraftwerken

3.4.2.3.1 Vorgehensweise

In diesem Abschnitt wird die Anwendbarkeit der MEDIC-Bewertungsmethode bei der nachträglichen Bewertung von Ereignissen in Kernkraftwerken, bei denen Personalfehlhandlungen an der MMS ursächlich waren, am Beispiel eines relevanten Ereignisses demonstriert.

Auf Basis der vorliegenden Informationen zum Ereignis werden die Ursachen für das Ereignis in das entwickelte MEDIC-Arbeitssytemmodell einsortiert. Ziel ist hierbei, Mängel der technischen Vorkehrungen gegen Fehlhandlungen an den betroffenen MMS, die zum Ereignis geführt haben, aufzuzeigen. Hierzu werden zunächst die beim Ereignis beteiligten Komponenten gemäß dem MEDIC-Arbeitssystemmodell identifiziert. Darauf aufbauend wird anschließend dargestellt, welche Wechselwirkungen zwischen den Komponenten des gemäß der MEDIC-Bewertungsmethode zugrunde zulegenden Arbeitssystems für die Durchführung der Aufgabe an der MMS beim Ereignis betroffen waren. Abhängig von den vorliegenden Informationen insbesondere zum Design der MMS wird für die beim Ereignis betroffenen Wechselwirkungen gezeigt, welche Attribute zur Charakterisierung dieser Wechselwirkungen nicht erfüllt und somit fehlerverursachend waren.

3.4.2.3.2 Betrachtetes Ereignis: Absturz eines Brennelements in einer Siedewasserreaktoranlage

Beschreibung des Ereignisablaufes:

In der betroffenen Siedewasserreaktoranlage kam es im Rahmen des jährlichen Brennelementwechsels zum Absturz eines Brennelementes. Der Ablauf stellt sich wie folgt dar:

Aus einer noch mit vier Brennelementen voll beladenen Kernzelle sollte ein Brennelement (BE) entladen werden. Beim Anheben des Brennelementes verhakte sich der Brennelementkastenbefestiger mit dem Kastenbefestiger des Nachbarelementes, so dass beide Brennelemente aus dem Kern gezogen wurden. Aufgrund der erhöhten Lastanzeige stoppte das Personal den Vorgang kurz nach dem Anheben des Brennelements. Da zuvor keine automatische Abschaltung des Hubwerks über den Lastgrenzwert erfolgt war, setzte das Personal das Entladen des Brennelements in Langsamfahrt fort. Um die Ursache für die weiterhin erhöhten Werte der Lastanzeigen zu ergründen, wollte das Personal im Verlauf des Hebevorgangs zweimal das anzuhebende Brennelement mit dem Fernglas beobachten. Wegen der unruhigen Wasseroberfläche war dies jedoch nicht möglich. Eine Unterwasserkamera wurde nicht eingesetzt. Nachdem sich die beiden Brennelemente einige Zentimeter über dem oberen Kerngitter befanden, wurde der Hubvorgang beendet, weil die vorgesehene Hubhöhe erreicht war. Zu diesem Zeitpunkt zeigte die Lastanzeige etwa das doppelte BE-Gewicht an.

Etwa eine Minute später rutschte dann das zweite mitgezogene Brennelement ab, fiel auf der Position der Kernzelle auf das obere Kerngitter zurück und blieb dort in Schrägstellung stehen. Zu Beschädigungen von Brennelementhüllrohren mit Aktivitätsfreisetzung ist es nicht gekommen.

Die Brennelemente eines Siedewasserreaktors sind jeweils mit einem Kasten umgeben. Die Kastenbefestiger fixieren den Brennelementkasten am Brennelement mittels einer Schraubverbindung. Sie stellen außerdem sicher, dass zwischen den Brennelementen ein Spalt verbleibt, in dem die Steuerstäbe verfahren werden können. Brennelement und Brennelementkasten bilden eine Einheit und werden zusammen in den Reaktor geladen und entladen.

Die zwei ineinander verhakten Brennelemente stammten von verschiedenen Herstellern. Ursächlich für das Verhaken der beiden Brennelemente waren Konstruktionsunterschiede in der Gestaltung des Brennelementkastens und des Brennelementkastenbefestigers. Nach Ansicht von Gutachter und Betreiber wurde das Verhaken der Brennelemente durch eine strahlungsbedingte Verbiegung der Brennelementkästen begünstigt.

Zum fälschlichen Anheben der beiden Brennelemente haben laut Gutachter und Betreiber zwei unabhängige Fehler beigetragen:

- **Ausfall der automatischen Lastabschaltung**:
  Die Überwachung der Brennelementwechselmaschine ist mit zwei Überlastgrenzwerten versehen, einem für die Handhabung der Steuerelemente und einem für die Handhabung der Brennelemente. Die Überwachung ist zweikanalig ausgeführt. Die Brennelementwechselmaschine schaltet bei der Brennelementhandhabung ab, wenn die Last in einem Kanal den Wert von 3850 N überschreitet (die Gewichtskraft eines Brennelements beträgt ca. 2800 N). Im vorliegenden Fall funktionierte diese Abschaltung auf beiden Kanälen nicht, weil die Grenzwertverarbeitung der Lastmesseinrichtung nicht funktionsbereit war. Eine Meldung, die diesen Zustand angezeigt hätte oder eine automatische Sperre der Bedienung der Brennelementwechselmaschine gab es nicht. Die Ursachen für den nicht erkannten Ausfall der automatischen Lastabschaltung sind auf eine Reihe von dem Ereignis vorangegangenen technischen und organisatorischen Mängeln in Zusammenhang mit dem Betrieb, der Wartung und der Instandhaltung der BE-Wechselmaschine zurückzuführen.

- **Nichtbeachten der Lastanzeigen:**
  Beim Anheben der Last zeigte die analoge Lastanzeige eine Last von ca. 4000 N an und erreichte damit den Endausschlag. Die zusätzliche digitale Anzeige zeigte zunächst eine Last von ca. 6000 N an, worauf das Personal den Anhebevorgang kurz stoppte, dann aber weiterfuhr, weil die automatische Lastabschaltung nicht erfolgt war. Beim Ausfahren aus dem Kern wurde zeitweise eine Last von ca. 8400 N erreicht. Nachdem beide Brennelemente über das obere Kerngitter angehoben worden waren, zeigte die Lastmessung das doppelte BE-Gewicht an.

Wegen der erhöhten Lastanzeigen und der nicht erfolgten Lastabschaltung wurde vom Bedienungspersonal zweimal erfolglos versucht, den Anhebevorgang mit dem Fernglas zu beobachten. Die hohen Werte der Lastanzeigen wurden vom Bedienungspersonal auf Reibkräfte beim Entladevorgang zurückgeführt. Dem Personal war in Schulungen vermittelt worden, dass beim Lösen einzelner Brennelemente, bedingt durch die Kastenverbiegung infolge der Neutronenbestrahlung, zunächst hohe Kräfte auftreten können und dass in einem solchen Fall gezielt die Lastabschaltung angefahren werden kann und muss, um die Brennelemente zu lösen. Ein Versagen der Lastabschaltung wurde nicht unterstellt und entsprechend in den Schulungen auch nicht berücksichtigt. In den Betriebsvorschriften (BHB) gab es keine expliziten Angaben zu einzuhaltenden Maximallasten. An den analogen Anzeigen auf dem Bedienpult waren keine Markierungen für maximale Lasten angebracht. Weiterhin war die Lastanzeige ergonomisch ungünstig (zum Beispiel kein Farbwechsel im Überlastbereich, aber im Unterlastbereich; Skalenbeschriftung und Anzeigebereich der Analogskala ungünstig, kleine Schrift für Darstellung der Absolutlast).

MEDIC-Bewertung des Ereignisses:

Die Bewertung des Ereignisses erfolgt gemäß dem MEDIC-Leitfaden. Es sind demnach zunächst die Arbeitsaufgabe und die Komponenten des MEDIC-Arbeitssystems zu identifizieren. Aus der Ereignisbeschreibung ergibt sich Folgendes:

- Arbeitsaufgabe: Anheben eines Brennelementes mit seinem Brennelementkasten aus einer Kernzelle
    - Komponenten des MEDIC-Arbeitssystems
        - System: Brennelementwechselmaschine mit zugehörigen Überlastüberwachungseinrichtungen (Lastmesseinrichtung, Grenzwertverarbeitung, Abschalteinrichtung bei Überlast); Brennelement mit Brennelementkasten; Unterwasserkamera, Fernglas.
        - Unterlagen: Betriebshandbuch mit entsprechenden Betriebsvorschriften.
        - MMS: Bedienpult der Brennelement-Wechselmaschine mit analogen Lastanzeigen; Zusätzliche digitale Lastanzeige.
        - Mensch: Personal mit entsprechender Ausbildung (Schulungen).

Bei der vorliegenden Arbeitsaufgabe handelt es sich um eine Steuerungs- und Überwachungsaufgabe an einer MMS. Es wird demnach für die Bewertung des Arbeitssystems die MEDIC-Interrelationsmatrix, wie in Kapitel 3.3.2 (Tab. 3.2) eingeführt, zugrunde gelegt. Im Rahmen der Bewertung werden zunächst die für das Ereignis relevanten Beziehungen zwischen den Komponenten des MEDIC-Arbeitssystems identifiziert, die bei den beobachteten Personalfehlhandlungen betroffen waren. Anschließend werden die Ursachen für diese beobachteten Fehlhandlungen in Bezug auf die Erfüllung der Attribute zur Charakterisierung Beziehungen in der MEDIC-Interrelationsmatrix dargestellt.

Die automatische Abschaltung bei Überlast ist im Rahmen der MEDIC-Bewertung als eine Maßnahme zur Fehlerkorrektur (explizite technische Vorkehrung gegen Fehlhandlungen) anzusehen. Eine funktionsfähige automatische Lastabschaltung hätte das Mitanheben eines zweiten BE und demzufolge den Absturz dieses zweiten BE verhindern können. Der Ausfall der automatischen Lastabschaltung im vorliegenden Ereignis ist auf eine Reihe von dem Ereignis vorangegangenen technischen und organisatorischen Defiziten zurückzuführen, welche durch mehrere Arbeitssysteme beschrieben werden können. Da die erforderlichen Informationen über die beteiligten Arbeitssysteme für das

Einordnen der Ursachen für diesen Ausfall in das MEDIC-Analysenmodell nicht vorhanden sind, wird der Ausfall der automatischen Lastabschaltung nicht weiter analysiert.
Das Nichtbeachten der Lastanzeigen bzw. der Überlastanzeigen beim Anheben der Brennelemente durch das Bedienpersonal ist als unmittelbare Ursache für das Ereignis anzusehen. Trotz erhöhter Lastanzeige hat das Personal den Hebevorgang des Brennelements mit der BE-Wechselmaschine fortgesetzt. Bei sachgemäßer Interpretation der Lastanzeigewerte hätte das Personal den Hebevorgang rechtzeitig stoppen müssen.

Die Ursachen dieser Fehlhandlungen (Nichtbeachten der Lastanzeige und Fortsetzen des Hebevorgangs trotz Überlastanzeige) lassen sich mehreren Beziehungen des MEDIC-Arbeitssystems zuordnen, wie nachfolgend auf Grundlage der Angaben aus der Ereignisbeschreibung erläutert wird.

- **Beziehung System → Mensch:** Das Systemverständnis war beim Personal aufgrund mangelhafter Schulung nicht ausreichend vorhanden bzw. fehlerhaft. Gemäß den Ausführungen aus der Ereignisbeschreibung wurden vom Bedienungspersonal die hohen Werte der Lastanzeigen auf Reibkräfte beim Entladevorgang zurückgeführt. Dem Personal war in Schulungen vermittelt worden, dass beim Lösen einzelner Brennelemente zunächst hohe Kräfte auftreten können und dass in einem solchen Fall gezielt die Lastabschaltung angefahren werden kann und muss, um die Brennelemente zu lösen. Ein Versagen der Lastabschaltung wurde nicht unterstellt und entsprechend in den Schulungen auch nicht berücksichtigt. Die mentale Zugänglichkeit des Systems beim Personal war dadurch beeinträchtigt. Dem Personal war es aus diesen Gründen nicht möglich, den Systemzustand eindeutig zu erkennen und richtig zu interpretieren.

- **Beziehung MMS → Mensch:** Die Lastanzeige war ergonomisch ungünstig (kein Farbwechsel im Überlastbereich, aber im Unterlastbereich; Skalenbeschriftung und Anzeigebereich der Analoganzeige ungünstig, kleine Schrift für Darstellung der Absolutlast), so dass die physische Zugänglichkeit der MMS beim Menschen erschwert wurde.

- **Beziehung MMS → System:** Die Überlastbereiche waren auf der MMS nicht gekennzeichnet und die Nichtverfügbarkeit der automatischen Lastabschaltung wurde nicht angezeigt. Der auf der MMS dargestellte Systemzustand entsprach nicht dem tatsächlich vorliegenden Systemzustand. Das Attribut „Korrespondenz“ war hier nicht erfüllt.

- **Beziehung Unterlagen → Mensch:** In den Betriebsvorschriften (BHB) für die Bedienung des Systems gab es keine expliziten Angaben zu einzuhaltenden Maximallasten. In der Ereignisbeschreibung wird angemerkt, dass das Personal keine Unterwasserkamera eingesetzt hat. Dies deutet daraufhin, dass es keine klaren Vorgaben hinsichtlich des Einsatzes der Unterwasserkamera in den Unterlagen gab, z. B. bei Näherung an die Maximallasten oder bei widersprüchlichen Anzeigen der analogen und digitalen Lastanzeigen. Das Bild der Unterwasserkamera hätte in diesem Fall eine sinnvolle Erweiterung der MMS darstellen können, um den Fehler zu erkennen. Dies deutet auf eine Nichterfüllung des Attributs „Vorhandensein" bei den Unterlagen, wodurch die mentale Zugänglichkeit des Systems anhand der Anweisungen in den Unterlagen beim Menschen erschwert wurde.
- **Beziehung MMS ←→ MMS:** Der Endausschlag der Analoganzeige stimmte nicht mit dem Endausschlag der zusätzlichen digitalen Anzeige überein. Das Attribut „Konsistenz" war nicht erfüllt.

Die vorangegangenen Ausführungen demonstrieren die Anwendbarkeit der MEDIC-Bewertungsmethode bei der nachträglichen Bewertung von Ereignissen mit Bezug zu Fehlhandlungen an MMS. Es lassen sich nachträglich fehlerverursachende technische Vorkehrungen an den betroffenen MMS aufzeigen, so dass diese nachträglich verbessert werden können. Bei dem beschriebenen Ereignis wurden beispielsweise als Maßnahmen gegen Wiederholung der Anzeigebereich der Analoganzeige der Last erweitert und die Grenzwerte markiert. Zudem wurden die Anweisungen für die Handhabung von Einrichtungen der BE-Wechselmaschine ergänzt und die Beobachtungsmöglichkeiten mittels Unterwasserkamera erweitert.

3.4.2.4 Anwendungsbeispiel zur Bewertung eines Arbeitssystems für die Durchführung einer Wartungsaufgabe an einem softwarebasierten Leittechniksystem

Die entwickelte MEDIC-Bewertungsmethode wurde zur Erprobung ebenfalls verwendet, um ein mit den Komponenten von MEDIC-AnTeS (siehe Kapitel 4) entwickeltes Arbeitssystem für den Tausch einer Prozessorbaugruppe mit anschließendem Hochladen der Software an dem rechnerbasierten Leittechniksystems TXS der Firma Framatome zu bewerten. Der Schwerpunkt lag hierbei auf der Analyse der für die Durchführung dieser Wartungsaufgabe eigenständig entwickelten Arbeitsanweisung. Das Ziel war es,

potenzielle Mängel im Arbeitsablauf gemäß der entwickelten Arbeitsanweisung zu identifizieren.

Folgende Annahmen wurden bei der Entwicklung der Arbeitsanweisung getroffen:

- Die entwickelte Arbeitsanweisung wurde für einen gering ausgebildeten Menschen d. h. möglichst unabhängig vom Vorwissen des ausführenden Menschen erstellt. Sie enthielt dementsprechend alle notwendigen Schritte in sehr detaillierter Form, um die Aufgabenstellung zu erfüllen.
- Die Arbeitsanweisung muss an die gegebenen Umstände (räumliche Bedingungen, Arbeitssicherheitsaspekte, Werkzeuge und Werkzeugbeschaffung, Zugang zu der TXS-Servicestation etc.) angepasst sein.
- Die Arbeitsanweisung soll möglichst alle Tätigkeiten am TXS-Leittechnikschrank und an der TXS-Servicestation abdecken.

Die entwickelte Arbeitsanweisung bestand aus drei Unterlagen:

(1) Informationsblatt zu der Arbeitsanweisung
- Übersichtsdokument mit allen relevanten Informationen für die Durchführung der gestellten Aufgabe (Leittechnikschrank, Baugruppen, Servicestation).

(2) Detaillierte Beschreibung der durchzuführenden Tätigkeiten
- Ausführliche Beschreibung der durchzuführenden Tätigkeiten,
- Erläuterungen und Abbildungen zu den Arbeitsschritten und zu den leittechnischen Komponenten und
- chronologischer Ablauf in Bezug auf die durchzuführenden Arbeitsschritte.

(3) Checkliste zur Arbeitsanweisung
- Enthält die Arbeitsschritte zu den Tätigkeiten in zusammengefasster Form zum Abhaken und ist
- chronologisch aufgebaut.

In Abb. 3.8 ist ein Auszug der Checkliste zur entwickelten Arbeitsanweisung für den Austausch der Prozessorbaugruppe dargestellt.

Checkliste zur Arbeitsanweisung

Tausch einer SVE2 Verarbeitungseinheit und Hochladen der Anwendungssoftware

Die Abarbeitung der Checkliste erfolgt chronologisch.

Lokalisierung Leittechnikschrank und Baugruppe

Zugang zu Räumlichkeiten mit der Leittechnik kriegen	
Lokalisierung und Öffnung des Leittechnikschranks mit auszutauschender SVE2 Baugruppe	
Lokalisierung des Baugruppenträgers und der auszutauschenden SVE2 Baugruppe	

Herunterfahren des Baugruppenträgers und darin verbauten Baugruppen

Anlegen des ESD Bandes	
Stromzufuhr zum Ziel-Baugruppenträger trennen	

Extraktion einer SVE2 Baugruppe

Lösen der Halterungsschrauben der SVE2 Baugruppe	
Lösen der Halterungsschrauben der SL22 Baugruppe	
Lösen der angeschlossenen Kabel	
Herauslösen der Baugruppen durch die Laschen	

Lösen von SL22 Baugruppen von einer SVE2 Baugruppe

Lösen der Befestigungsschrauben der SL22 Baugruppe	
Herausziehen der SL22 Baugruppe	

Vorbereitung der neu einzusetzenden SVE2 Baugruppe

Kippschalter der neuen SVE2 Baugruppe konfigurieren	
Montage der alten SL22 Baugruppe auf die neue SVE2 Baugruppe	
Festschrauben der obersten SL22 Baugruppe	

Abb. 3.8 Auszug aus der Checkliste zur Arbeitsanweisung

Detaillierte Angaben zu der Arbeitsanweisung mit weiteren Abbildungen der einzelnen Unterlagen und Beschreibungen der Tätigkeitsschritte finden sich im Anhang A.2 des Berichtes.

Der Arbeitsablauf bei der Durchführung der Aufgabe sieht vor, dass die Arbeitsschritte zu den einzelnen Tätigkeitsblöcken vom Menschen anhand der drei vorhandenen Dokumente durchgeführt werden. Somit sind die Checkliste zur Arbeitsanweisung, das Informationsblatt zur Arbeitsanweisung und die detaillierte Beschreibung der vom Menschen durchzuführenden Tätigkeiten einzusetzen. Auf der Checkliste wird nach erfolgreicher Durchführung eines Arbeitsschrittes ein Häkchen als Erledigungsvermerk gesetzt.

Der vorgesehene Arbeitsablauf bei der Durchführung der Aufgabe wurde mit der MEDIC-Bewertungsmethode auf potenzielle Defizite analysiert. Hierbei wurden die drei Unterlagen zur Arbeitsanweisung dahingehend bewertet, ob sie eine möglichst fehlerfreie Durchführung der Aufgabe unterstützen.

Um eine unabhängige Bewertung der Arbeitsanweisung mit der MEDIC-Bewertungsmethode zu gewährleisten, wurden für die Entwicklung der Arbeitsanweisung und für ihre Bewertung verschiedene Personen des MEDIC-Projektteams eingesetzt.

Für die Bewertung gemäß der MEDIC-Interrelationsmatrix wurden

- die Attribute „Konsistenz“, „Übersichtlichkeit“ und „Eindeutigkeit“ zur Charakterisierung der Beziehung Unterlagen → Unterlagen,
- das Attribut „Korrespondenz“ zur Charakterisierung der Beziehung Unterlagen → System,
- das Attribut „Vollständigkeit“ zur Charakterisierung der Beziehung Unterlagen → MMS und
- das Attribut „physische Zugänglichkeit“ zur Charakterisierung der Beziehung Unterlagen → Mensch

herangezogen.

Die MEDIC-Bewertung der Arbeitsanweisung in Bezug auf die genannten Beziehungen und Attribute ergab Folgendes:

- Das Kriterium „Konsistenz“ trifft zu.
- Das Kriterium „Übersichtlichkeit“ trifft nur zum Teil zu.
- Das Kriterium „Eindeutigkeit“ trifft nicht zu.
- Das Kriterium „Korrespondenz“ trifft zu.
- Das Kriterium „Vollständigkeit“ trifft nicht zu.
- Die Unterteilung der Arbeitsanweisung zur Durchführung der Aufgabe in drei Unterlagen ist aufgrund der unpraktischen Handhabbarkeit hinsichtlich der „physischen Zugänglichkeit“ ungünstig. Der Zusammenhang zwischen den drei Unterlagen in den Tätigkeitsanweisungen, z. B durch Querverweise, wurde nicht immer hergestellt. Dies stellt ein weiteres Fehlerpotenzial dar.

Weitere Erläuterungen zu diesen Ergebnissen der MEDIC-Bewertung der Arbeitsanweisung finden sich im Anhang A.2.

Zusammenfassend ist festzuhalten, dass anhand der Bewertung der Arbeitsanweisung mit der MEDIC-Bewertungsmethode, das Potenzial für Fehlhandlungen bei der Durchführung der Aufgabe auf Basis der Unterlagen der Arbeitsanweisung, erkannt wurde.

Zur Validierung dieses MEDIC-Bewertungsergebnisses wurde in einem weiteren Schritt die Arbeitsaufgabe unter Zuhilfenahme der Arbeitsanweisung durch eine Testperson in Beisein einer Aufsichtsperson (zur Protokollierung und Beobachtung des Arbeitsablaufs) durchgeführt. Es wurde anschließend ausgewertet, inwieweit die Testperson auf Basis der Unterlagen der Arbeitsanweisungen, die Aufgabe ohne Nachfrage vollständig und korrekt durchführen konnte. Die Fähigkeit der MEDIC-Bewertung, Fehlhandlungen bei der Durchführung der einzelnen Tätigkeitschritte der Arbeitsaufgabe zu prognostizieren, bestätigte sich. Dies belegt die Eignung der MEDIC-Bewertung, potenzielle Fehlhandlungen an MMS aufgrund Mängel technischer Vorkehrungen zu identifizieren.

3.5 Zusammenfassung

In diesem Kapitel wurde die MEDIC-Bewertungsmethode zur Bewertung von technischen Vorkehrungen gegen Personalfehlhandlungen vorgestellt.

Die MEDIC-Bewertungsmethode dient der qualitativen Bewertung von technischen Präventivmaßnahmen gegen Fehler durch Personalhandlungen an MMS, mit dem Ziel potenzielle Mängel technischer Vorkehrungen gegen Fehlhandlungen des Personals an typischen MMS digitaler Leittechniksysteme zu identifizieren und zu analysieren.

Für die Entwicklung der MEDIC-Bewertungsmethode wurde zunächst das zugrunde zulegende MEDIC-Arbeitssystemmodell entwickelt. Das MEDIC-Arbeitssystemmodell besteht aus den Komponenten „Unterlagen“, „Mensch“, „MMS“ und dem zu bedienenden „System“. Neben den genannten Komponenten werden im MEDIC-Arbeitssystemmodell die Beziehungen zwischen den Komponenten und die Beziehungen zwischen den Teilelementen der jeweiligen Komponenten des Arbeitssystems untereinander betrachtet.

In der MEDIC-Bewertungsmethode wird davon ausgegangen, dass neben den Komponenten auch die Eigenschaften der zuvor genannten Beziehungen relevant sind, um eine möglichst fehlerfreie Erledigung einer Aufgabe an der MMS zu erzielen.

Für die Bewertung der Eignung von technischen Vorkehrungen gegen Fehlhandlungen an Mensch-Maschine-Schnittstellen mit der MEDIC-Bewertungsmethode, wurden Attribute (Konsistenz, Korrektheit, …) zur Charakterisierung der genannten Beziehungen zwischen den Komponenten des MEDIC-Arbeitssystemmodells definiert. Im Rahmen der MEDIC-Bewertungsmethode wird davon ausgegangen, dass diese Attribute erfüllt werden sollen, um Personalfehlhandlungen an MMS zu vermeiden oder zu minimieren. Bei der Bewertung von technischen Vorkehrungen gegen Fehlhandlungen an der MMS eines Arbeitssystems mit der MEDIC-Bewertungsmethode wird daher überprüft, zu welchem Grad die eingeführten Attribute die Beziehungen zwischen den Komponenten des Arbeitssystems erfüllen. Der Erfüllungsgrad dieser Attribute kann als Bewertungsmaßstab für die Vermeidung bzw. Minimierung von Personalfehlhandlungen an der MMS des zugehörigen Arbeitssystems herangezogen werden. Im Rahmen der MEDIC-Bewertungsmethode wurden Bewertungskriterien aus der NUREG 0700-Richtlinie /NUR 02/ abgeleitet.

Die Eignung der entwickelten MEDIC-Bewertungsmethode zur Bewertung technischer Vorkehrungen gegen Personalfehlhandlungen an MMS wurde anhand von drei Anwendungsbeispielen erprobt: Zunächst wurde als Beispiel für die Bewertung von in der Entwicklung befindlichen MMS ein Arbeitssystem für eine Steuerungsaufgabe an einer MMS, „MMS-Warte“ genannt, entwickelt und anschließend bewertet. Zur Bewertung von bereits eingesetzten Arbeitssystemen mit der MEDIC-Bewertungsmethode wurden anschließend meldepflichtige Ereignisse in Kernkraftwerken betrachtet, bei denen MMS als ursächlich für Personalfehlhandlungen identifiziert wurden. Die für die betrachteten Ereignisse ursächlichen MMS wurden nachträglich mit der MEDIC-Bewertungsmethode bewertet. Als weiteres Anwendungsbeispiel wurde die Eignung der MEDIC-Bewertungsmethode zur Bewertung von Arbeitssystemen für Wartungs- und Instandhaltungsaufgaben an einem softwarebasierten Leittechniksystem anhand eines hierfür entwickelten Arbeitssystems, „MMS-Schrank“ genannt, erprobt. Der Schwerpunkt der Bewertung des Arbeitssystems „MMS-Schrank“ war hierbei potenzielle Mängel im Arbeitsablauf auf Basis der entwickelten Arbeitsanweisung zu identifizieren.

Die Bewertung des Arbeitssystems „MMS-Warte“ mit der MEDIC-Bewertungsmethode zeigte, dass die für die Bewertung relevanten Attribute nicht vollumfänglich erfüllt wurden. Daraus ergab sich, dass die für das Arbeitssystem „MMS-Warte“ vorgesehenen technischen Vorkehrungen gegen Personalfehlhandlungen nicht ausreichend sind, um die Bewertungskriterien der MEDIC-Methode zu erfüllen. Das Design der MMS wäre nun

in einen weiteren Schritt unter Berücksichtigung der Ergebnisse der MEDIC-Bewertung entsprechend zu verbessern und anschließend einer weiteren MEDIC-Bewertung zu unterziehen. Dieser Vorgang wäre so lange iterativ zu wiederholen, bis alle Attribute erfüllt sind. Im Rahmen dieser Iteration können weitere Bewertungskriterien herangezogen werden.

Die erzielten Ergebnisse bei der nachträglichen Bewertung eines Ereignisses mit Bezug zu Fehlhandlungen an MMS demonstrieren die Anwendbarkeit der MEDIC-Bewertungsmethode bei der Bewertung von bereits eingesetzten Arbeitssystemen. Es lassen sich mit der MEDIC-Bewertungsmethode nachträglich fehlerverursachende technische Vorkehrungen an den betroffenen MMS aufzeigen, so dass diese nachträglich verbessert werden können.

Die Bewertung des Arbeitssystems „MMS-Schrank“ mit der MEDIC-Bewertungsmethode zeigte, auf Basis der Analyse der Unterlagen, das Potenzial für Fehlhandlungen bei der Durchführung der Aufgabe auf. Zur Validierung dieses MEDIC-Bewertungsergebnisses wurde in einem weiteren Schritt die Arbeitsaufgabe unter Zuhilfenahme der Arbeitsanweisung durch eine Testperson in Beisein einer Aufsichtsperson (zur Protokollierung und Beobachtung des Arbeitsablaufs) durchgeführt. Es wurde anschließend ausgewertet, inwieweit die Testperson auf Basis der Unterlagen der Arbeitsanweisungen die Aufgabe ohne Nachfrage vollständig und korrekt durchführen konnte. Hierbei kam es zu Fehlhandlungen der Testperson. Dies bestätigte die Fähigkeit der MEDIC-Bewertungsmethode, Fehlhandlungen bei der Durchführung einzelner Tätigkeitschritte der Arbeitsaufgabe zu prognostizieren.

Die aufgeführten Anwendungsbeispiele belegen die Eignung der MEDIC-Bewertungsmethode, potenzielle Mängel technischer Vorkehrungen gegen Personalfehlhandlungen an MMS zu identifizieren.

4 Entwicklung eines Analysewerkzeuges zur Bewertung von technischen Vorkehrungen gegen Fehler durch Personalhandlungen in softwarebasierten Leittechniksystemen

Für die Anwendung der MEDIC-Bewertungsmethode wurde im Rahmen des Vorhabens das MEDIC-Analysewerkzeug entwickelt.

4.1 Komponenten und Einsatzzweck des entwickelten Analysewerkzeugs

Das entwickelte MEDIC-Analysewerkzeug zur Bewertung von technischen Vorkehrungen gegen Fehler durch Personalhandlungen an MMS in softwarebasierten Leittechniksystemen besteht aus mehreren eigenständigen Softwaretools, welche bei der Bewertung von MMS spezifisch eingesetzt werden können. Dieser modulare Aufbau wurde gewählt, um das MEDIC-Analysewerkzeug flexibel einsetzen und beliebig erweitern zu können. Folgende Softwaretools wurden entwickelt.

- MEDIC-Tool
  Zur softwaregestützten Bewertung von typischen MMS softwarebasierter Leittechniksysteme wurde die Software MEDIC-Tool entwickelt. Grundlage für die Software MEDIC-Tool ist die im Kapitel 3 dargestellte MEDIC-Bewertungsmethode.

- MEDIC-MMS
  Neben der softwaregestützten Bewertung von MMS, stellt die Entwicklung von als graphische Benutzeroberflächen realisierten MMS softwarebasierter Leittechniksysteme eine weitere Komponente des MEDIC-Analysewerkzeugs dar. Das hierfür entwickelte Framework[15] wird nachfolgend als MEDIC-MMS bezeichnet.

- MEDIC-AnTeS
  Als MEDIC-AnTeS wird die Komponente des MEDIC-Analysewerkzeugs bezeichnet, mit der zu bewertende Arbeitssysteme für die Durchführung von Wartungs- und Instandhaltungsaufgaben an softwarebasierten Leittechniksystemen realisiert und spezifiziert werden. Mit MEDIC-AnTeS können beispielsweise TXS-basierte

[15] Framework: Ein Framework oder Software-Framework ist eine Plattform für die Entwicklung von Softwareanwendungen. Es bietet eine Grundlage, auf der Softwareentwickler Programme für eine bestimmte Plattform erstellen können. Ein Framework kann beispielsweise vordefinierte Klassen und Funktionen enthalten, die für die Verarbeitung von Eingaben, die Verwaltung von Hardware-Geräten und die Interaktion mit der Systemsoftware verwendet werden können. /TEC 22/

Arbeitssysteme mit den vorhandenen Komponenten des Moduls 1 „Reales Leittechniksystem“ des GRS-AnTeS /GRS 21/ entwickelt und nachgebildet werden.

Nachfolgend werden die einzelnen Komponenten des MEDIC-Analysewerkzeugs erläutert.

4.2 MEDIC-MMS

Mit der Komponente MEDIC-MMS des MEDIC-Analysewerkzeugs können graphische Benutzeroberflächen wie sie typischerweise in softwarebasierten Leittechniksystemen als MMS für Steuerungs- und Überwachungsaufgaben eingesetzt werden (sieheAbb. 2.1), entwickelt werden. Hierbei ist es möglich sowohl graphische Benutzeroberflächen neu zu entwickeln als auch bereits als MMS eingesetzte graphische Benutzeroberflächen nachzubilden. Mit der letztgenannten Möglichkeit können bei vorhandenen Informationen zum Design einer MMS diese nachträglich in Bezug auf die Eignung der realisierten technischen Vorkehrungen zur Vermeidung von Personalfehlhandlungen bewertet bzw. analysiert werden. Die Entwicklung von neuen eigenständigen graphischen Benutzeroberflächen ermöglicht es, die Wirksamkeit der technischen Vorkehrungen parallel zu der Entwicklung der Benutzeroberfläche zu analysieren und gegebenenfalls Verbesserungsmaßnahmen vorzunehmen. Im Rahmen dieses Vorhabens wurde diese Möglichkeit für die Erprobung der MEDIC-Bewertungsmethode verwendet. Hierbei wurden die MEDIC-Bewertungsmethode und das Tool MEDIC-MMS von verschiedenen Teams unabhängig voneinander, ohne Informationsaustausch zwischen den Teams, entwickelt.

Für die Entwicklung von MEDIC-MMS wurde als Programmiersprache Python /PYT 22/ gewählt, da Python eine der derzeit meistgenutzten frei verfügbaren Programmiersprachen ist. Zudem steht dem Programmierer eine Vielzahl von Python-Paketen für unterschiedliche Anwendungsfälle zur Verfügung. Es wurde für die Entwicklung von MEDIC-MMS das Paket *PyQt* /PYP 22/ verwendet, welches die Anbindung der in der Programmiersprache *C++* entwickelten plattformübergreifenden Bibliothek für die Entwicklung von grafischen Benutzeroberflächen *Qt* an *Python* darstellt.

Mit MEDIC-MMS ist es auch möglich, verfahrenstechnische Prozesse zu simulieren, welche von einer graphischen Benutzeroberfläche gesteuert werden. Da *Threading*[16] in *Qt* eingebunden ist, können die Benutzeroberfläche und die Simulation des zu steuernden verfahrenstechnischen Prozesses parallel ausgeführt werden ohne, dass sie sich gegenseitig blockieren. Das Tool MEDIC-MMS unterstützt auch in seiner derzeitigen Version die Anbindung von optischen (z. B. Farbwechsel von Elementen auf der Benutzeroberfläche) und akustischen (z. B. ein Alarmton) Anzeigen und Meldungen sowie die Integration von Handlungsanweisungen und -erläuterungen für den Menschen.

Das Tool MEDIC-MMS wurde objektorientiert entwickelt, wodurch seine Flexibilität gewährleistet ist. Somit sind Erweiterungen und Änderungen in MEDIC-MMS immer möglich.

Das Framework MEDIC-MMS umfasst eine Vielzahl von implementierten Klassen und Funktionen. Im Folgenden ist eine Übersicht der implementierten Klassen, Funktionen und deren Zusammenwirken dargestellt (siehe Abb. 4.1):

- *src*: Bei src handelt es sich um ein Python-Paket. Hier wird der gesamte Quellcode und weitere Dateien abgelegt. Zusätzlich zu „src“ wird automatisch ein Ordner für die log-Dateien angelegt (nicht in Abb. 4.1 dargestellt).
    - *„build*“ ist ein Unterpaket von „*src*“, für die Erstellung der Oberfläche.
        - *„GUI*“ ist ein Unterpaket von *„build“* mit den externen *PyQt*-Dateien zum Erstellen der Oberfläche.
        - *files* ist ein Ordner mit weiteren Unterordnern. Hier liegen notwendige Dateien zur Funktionalität der Oberfläche wie z.B. Icons etc.
            - *„main“* ist ein weiteres Unterpaket von src hier liegen ein weiteres Unterpaket für die Entwicklungsumgebung sowie ein Ordner für Dateien anderer Programmiersprachen:
                - *„sketch“* ist ein Ordner für *sketch*-Programme (Programmiersprache für Arduino) zum Verbinden von einem Arduino mit der entwickelten Oberfläche.

[16] Threading: Threading wird in Python verwendet, um mehrere Threads (Tasks, Funktionsaufrufe) gleichzeitig auszuführen.

- *„python“* ist ein Unterpaket von „main“ mit der *Python*-Programmierumgebung. In Python sind drei weitere Unterpakete enthalten.

    - *„handler“* ist ein Unterpaket von „python“ mit *Python*-Dateien für verschiedene Funktionen, beispielsweise zum Aufbau einer Verbindung zum Arduino, Verzeichnisse zu den Icons, Style Sheets etc..

    - *„widgets“* ist das zweite Unterpaket von „python“ . Dies beinhaltet widgets in *PyQt*, die wiederholt angewendet werden können, beispielsweise sind die Pumpe, das Ventil oder die Wassertanks der MEDIC-Warte als Widgets hinterlegt. Dadurch können sie auch für andere Oberflächen herangezogen werden.

    - *„simulator*“ ist das dritte Unterpaket von „python“. In diesem Unterpaket sind die Module aller relevanten Simulationen abgelegt. Grundlegend existiert ein Modul *„base_class“* mit den minimalen Funktionen, welche eine Simulation beinhalten muss. Das Modul *MEDIC-Warte*, welches zur Realisierung des Arbeitssystems „MMS-Warte“ (siehe Kapitel 3.4.2.2) entwickelt wurde, erbt von der *„base_class“* und ergänzt diese mit den für MEDIC-Warte notwendigen Funktionen und Methoden. Als weiteres das Modul *rpv-Simulation* im Diagramm angezeigt, welches an dieser Stelle nicht weiter erläutert wird.

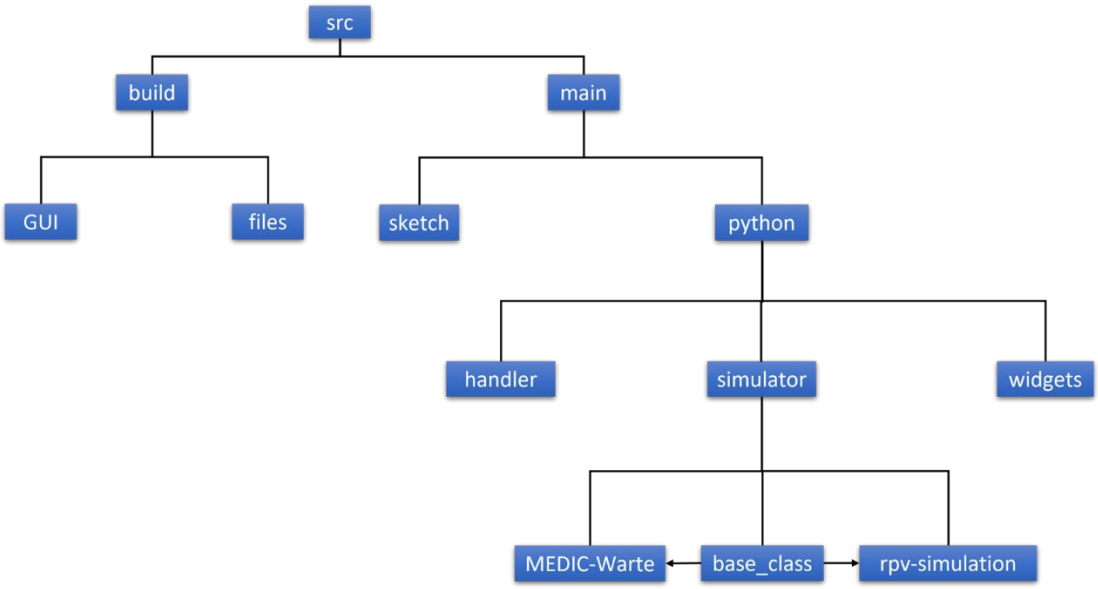

Abb. 4.1 Strukturbaum des MEDIC-Frameworks

Hier mit den verschiedenen Paketen, Unterpaketen und Ordnern. Die erstellten Pakete sind im Verzeichnis *„python“* abgelegt.

Die Möglichkeit der parallelen Ausführung der verfahrenstechnischen Simulation und der graphischen Benutzeroberfläche in MEDIC-MMS sowie insbesondere die Flexibilität von MEDIC-MMS sind von Vorteil für die Bewertung der Eignung von technischen Vorkehrungen zur Vermeidung bzw. Minimierung von Personalfehlhandlungen an MMS, da hierdurch eine Betrachtung von relevanten Aspekten des zugrundeliegenden Arbeitssystems und ein iteratives Vorgehen bei der Bewertung ermöglicht wird. Die Simulation des verfahrenstechnischen Prozesses bzw. des Systems stellt die Komponente „System“ des Arbeitssystems dar. Sie ermöglicht es beispielsweise Systemrückmeldungen an der graphischen Benutzeroberfläche nachzubilden und somit die Beziehungen System → MMS und MMS → Mensch gemäß MEDIC-Arbeitssystemmodell bei der Bewertung der technischen Vorkehrungen zu betrachten. Bei festgestellten Defiziten an den technischen Vorkehrungen können die sich daraus ergebenden Änderungen für die zu bewertende MMS mit MEDIC-MMS implementiert und die MMS anschließend erneut bewertet werden.

Im Rahmen dieses Vorhabens wurde mit der Komponente MEDIC-MMS des MEDIC-Analysewerkzeugs die graphische Benutzeroberfläche des Arbeitssystems „MMS-Warte“ für die Bewertung des Wassertanksystems mit der MEDIC-Bewertungsmethode entwickelt. Dies diente der Erprobung der MEDIC-Bewertungsmethode. Weitere Details

zu der graphischen Benutzeroberfläche des Arbeitssystems „MMS-Warte“ sind in Kapitel 3.4.2.2 enthalten.

4.3 MEDIC-AnTeS

MEDIC-AnTeS ist die Komponente des MEDIC-Analysewerkzeugs, mit der Arbeitssysteme für die Durchführung von Wartungs- und Instandhaltungsaufgaben an softwarebasierten Leittechniksystemen über typische hierfür verwendete MMS (siehe Abb. 2.1) entwickelt und spezifiziert werden. MEDIC-AnTeS ermöglicht es, entsprechende TXS-basierte Arbeitssysteme mit den vorhandenen Komponenten des Moduls 1 „Reales Leittechniksystem“ des GRS-AnTeS /GRS 21/ zu entwickeln bzw. nachzubilden. Das sind im Einzelnen folgende Komponenten:

- Leittechnische Komponenten des rechnerbasierten Leittechniksystems Teleperm XS (TXS) des Herstellers Framatome (ehemals AREVA).
- TXS-Servicestation mit der TXS-Engineering-Software z. B. für die Konfiguration von leittechnischen Baugruppen des TXS-Systems und die Generierung von Anwendersoftware.
- Systembeschreibungen der leittechnischen Komponenten des TXS-Systems.
- TXS-Arbeitsanweisungen zur Durchführung von Wartungs- und Instandhaltungsaufgaben in einem TXS-System.

Mit MEDIC-AnTeS können (ähnlich wie mit MEDIC-MMS für Arbeitssysteme für Steuerungs- und Überwachungsaufgaben) sowohl neue als auch bereits vorhandene TXS-basierte Arbeitssysteme für die Durchführung von Wartungsaufgaben an softwarebasierten Leittechniksystemen gemäß dem MEDIC-Arbeitsmodell entwickelt bzw. nachgebildet werden und anschließend mit der MEDIC-Bewertungsmethode bewertet werden. Auf anderen digitalen Leittechnikplattformen basierende Arbeitssysteme für Wartungs- und Instandhaltungsaufgaben können bei Vorliegen entsprechender Informationen grundsätzlich auch unabhängig von MEDIC-AnTeS mit der MEDIC-Bewertungsmethode bewertet werden.

Wartungs- und Instandhaltungstätigkeiten an Leittechniksystemen werden in der Regel anhand von Tätigkeitsanweisungen durchgeführt, welche von einem regelbasierten Verhalten des Ausführenden ausgehen. In MEDIC-AnTeS können basierend auf den

vorliegenden TXS-Arbeitsanweisungen und TXS-Systembeschreibungen eigenständige Arbeitsanweisungen entwickelt werden. Dies ermöglicht es, beispielsweise durch Variationen der Gestaltung der Tätigkeitsanweisungen, den Einfluss der Gestaltung und des Detaillierungsgrades der Tätigkeitsanweisungen auf die korrekte Durchführung der Wartungsaufgabe an den MMS eines softwarebasierten Leittechniksystems zu analysieren.

Bei der Entwicklung von Arbeitssystemen mit MEDIC-AnTeS werden insbesondere die relevanten Spezifika (Typ und Aufbau der verwendeten MMS, Art der durchzuführenden Aufgabe) von Wartungs- und Instandhaltungsaufgaben an einem softwarebasierten Leittechniksystem bei deren Bewertung mit der MEDIC-Bewertungsmethode berücksichtigt.

Bei der Entwicklung von Arbeitssystemen für Wartungsaufgaben an einem softwarebasierten Leittechniksystem mit MEDIC-AnTeS sind die folgenden Schritte durchzuführen:

1. Spezifizierung der Aufgabenstellung des ausführenden Menschen: z. B. Austausch einer Baugruppe, Modifikationen der Anwendersoftware oder betriebsbedingte Änderung von Anlagenparametern in leittechnischen Funktionen,
2. Entwicklung einer Arbeitsanweisung für die durchzuführende Aufgabe (Detaillierungsgrad der Arbeitsanweisung ist abhängig von den vorausgesetzten Kenntnissen des ausführenden Menschen),
3. Spezifizierung der zu verwendenden MMS: z. B. Kartensteckplätze im Leittechnikschrank, Taster und Schalter an den Baugruppen, Befehlszeilen-Shell (Bash) der Engineering-Tools im Servicegerät…).

Im Rahmen dieses Vorhabens wurde mit der Komponente MEDIC-AnTeS das Arbeitssystem „MMS-Schrank“ für den Austausch einer Prozessorbaugruppe mit anschließendem Hochladen der Anwendungssoftware entwickelt. Dies diente der Erprobung der MEDIC-Bewertungsmethode. Weitere Details zu dem entwickelten Arbeitssystem „MMS-Schrank“ und dessen Bewertung mit der MEDIC-Bewertungsmethode sind in Kapitel 3.4.2.4 enthalten.

Mit MEDIC-MMS entwickelte graphische Benutzeroberflächen für Steuerungs- und Überwachungsaufgaben können an MEDIC-AnTeS gekoppelt werden, in dem die Steuerung des verfahrenstechnischen Systems im MEDIC-MMS mit dem Modul 1 von AnTeS realisiert wird. Dies ermöglicht es beispielsweise, im Rahmen der Bewertung zu analysieren, ob vorgesehene technische Vorkehrungen gegen Personalfehlhandlungen für

Wartungsarbeiten an einem Leittechniksystem (z. B. Durchführung von Änderungsarbeiten im laufenden Betrieb der Anlage) geeignet sind, potenzielle Rückwirkungen von Wartungs- und Instandhaltungsarbeiten auf dem laufenden verfahrenstechnischen Prozess auszuschließen. Derartige Rückwirkungen können sich beispielsweise durch widersprüchliche Anzeigen (wie z. B. Fehlanregung von Grenzwerten, Unterdrückung von Grenzwerten, Stellungsanzeigen von Stellgliedern) an der MMS zur Steuerung des verfahrenstechnischen Prozesses bemerkbar machen. Zur Analyse des Einflusses solcher Rückwirkungen auf die Bedienung eines Systems können über entsprechende TXS-Systemschnittstellen zur Prozesssteuerung (Steuerungsinterface) und zur Entwicklung, Wartung und Überwachung des TXS-Systems widersprüchliche Anzeigen auf Bedienoberflächen nachgebildet werden.

4.4 MEDIC-Tool

Das MEDIC-Tool wurde entwickelt, um den Nutzer der MEDIC-Bewertungsmethode systematisch durch die Bewertung von Arbeitssystemen mit der MEDIC-Bewertungsmethode zu führen. Es dient dazu, die Bewertung von technischen Vorkehrungen mit der MEDIC-Bewertungsmethode zu vereinfachen und die Reproduzierbarkeit der Ergebnisse zu verbessern.

Für die Entwicklung des MEDIC-Tools wurde ebenfalls die frei verfügbare Programmiersprache Python /PYT 22/ gewählt. Für die Nutzerinteraktion wurde die grafische Benutzeroberfläche (GUI – graphical user interface) des MEDIC-Tools mit PyQt5 /PYP 22/ realisiert. Dadurch ist der Einsatz auf unterschiedlichen Betriebssystemen (MacOS, Windows, Linux) möglich. Das MEDIC-Tool wurde objektorientiert entwickelt, so dass eine Erweiterung/Änderung des MEDIC-Tools jederzeit möglich ist.

In den folgenden Abschnitten werden die Bewertungsgrundlage und die einzelnen Funktionen des MEDIC-Tools näher vorgestellt.

4.4.1 Bewertungsgrundlage des MEDIC-Tools

Nacheinander werden dem Nutzer des MEDIC-Tools in Bezug auf die Bewertungsaufgabe Einzelfragen bzw. zu prüfende Kriterien und Erläuterungen zur Frage bzw. zum Kriterium angezeigt. Der Nutzer kann dann die angezeigte Frage mit „Erfüllt“ oder „Nicht Erfüllt“ beantworten. Als Grundlage für die Bewertung des Erfüllungsgrades der Kriterien

und demzufolge für die Beantwortung der Fragen bzw. der Prüfung der Kriterien wurde die NUREG 0700-Richtlinie /NUR 02/ herangezogen. Diese NUREG 0700-Richtlinie hat sich aufgrund ihres hohen Detaillierungsgrades in Bezug auf die Anforderungen zur Vermeidung von Personalfehlhandlungen an Mensch-Maschine-Schnittstellen (siehe Kapitel 2.3.2.8) in diesem Vorhaben als die relevanteste erwiesen. Die Verwendung einer einheitlichen Bewertungsgrundlage beim MEDIC-Tool ermöglicht die Reproduzierbarkeit der Ergebnisse und die Vergleichbarkeit der Ergebnisse unterschiedlicher Bewerter.

Bei der Auswahl der Anforderungen aus der NUREG 0700-Richtlinie wurden zunächst Anforderungen für die Bewertung von als graphische Oberflächen realisierten MMS betrachtet. Als relevante Kapitel aus der NUREG-0700-Richtlinie wurden die Kapitel „Allgemeine Informationsanzeige“, „Benutzerschnittstellen Interaktion und Management“, „Softwaresteuerung“ und „Mensch-Maschine-Schnittstellen-Systeme“ ausgewählt. Aus diesen Kapiteln wurden 1308 relevante Anforderungen identifiziert. Diese 1308 Anforderungen wurden vom Englischen ins Deutsche übersetzt und in dem MEDIC-Bewertungsdiagramm übersichtlich dargestellt. Die Einteilung der identifizierten relevanten Anforderungen erfolgt in dem MEDIC-Bewertungsdiagramm unter Verwendung einer Farb- bzw. Musterkodierung.

Das MEDIC-Bewertungsdiagramm weist eine Baumstruktur auf. Die Hauptäste dieses Baums sind den ausgewählten Kapiteln „Allgemeine Informationsanzeige“, „Benutzerschnittstellen Interaktion und Management“, „Softwaresteuerung“ und „Mensch-Maschine-Schnittstellen-Systeme“ aus der NUREG-0700-Richtlinie zugeordnet und bilden Hauptkategorien zur Klassifizierung von Anforderungen an MMS. Diesen Hauptkategorien sind entsprechende Unterkategorien zugeordnet, welche die nächste Ebene der Baumstruktur bilden. Die den Hauptkategorien zugeordneten Unterkategorien können abhängig von der betrachteten Hauptkategorie wiederum in weiteren Unterkategorien aufgeteilt werden, welche weitere Ebenen der Baumstruktur bilden. Die Anforderungen an MMS sind unterhalb der jeweiligen Unterkategorien aufgelistet und bilden die unterste Ebene der Baumstruktur. Beispielsweise ist die Hauptkategorie „Allgemeine Informationsanzeige“ in den Unterkategorien „Allgemeine Anzeigenrichtlinien“, „Anzeigenformat“, „Anzeigenelemente“, „Qualität der Daten und Anzeigenrate“, „Anzeigenseiten“ und „Anzeigegeräte“ gegliedert, welche Anforderungen an die Informationsdarstellung an der MMS betreffend Format, Schriftgröße, Schriftart, Zeichenabstand, Beschriftung der Diagramme, verwendete Anzeigegeräte (Hardware) usw. enthalten.

In Abb. 4.2 ist ein Ausschnitt des MEDIC-Bewertungsdiagramms mit einigen ausgewählten Anforderungen dargestellt.

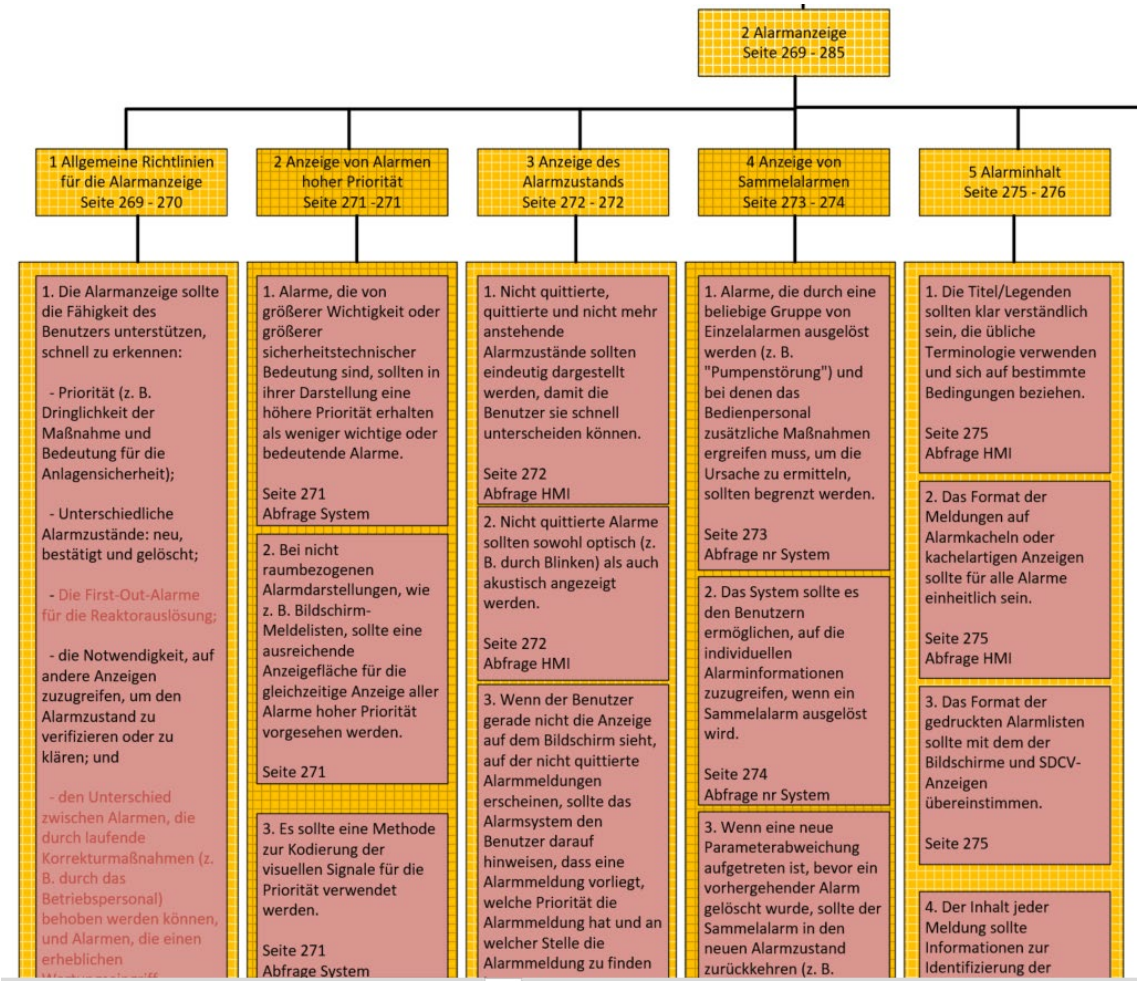

Abb. 4.2 Ausschnitt des MEDIC-Bewertungsdiagramms

Hier mit den ausgewählten Anforderungen: Hauptkategorie „Alarmanzeige“ mit den Unterkategorien „Allgemeine Richtlinien für die Alarmanzeige“, „Anzeige von Alarmen hoher Priorität“, „Anzeige des Alarmzustands“, „Anzeige von Sammelalarmen“ und „Alarminhalt“. Die entsprechenden Anforderungen sind unterhalb der jeweiligen Unterkategorien aufgelistet.

Die identifizierten 1308 Anforderungen wurden weiter nach Projektrelevanz selektiert, indem z. B. Hardwareanforderungen (Beleuchtung, Typ von verwendeten Monitoren und Eingabegeräten) nicht berücksichtigt wurden, da die Software „MEDIC-Tool“ im derzeitigen Entwicklungsstand der softwaregestützten Bewertung von als graphischen Oberflächen realisierten typischen MMS softwarebasierter Leittechniksysteme gemäß der im Kapitel 3 dargestellten MEDIC-Bewertungsmethode dient. Das MEDIC-Bewertungsdiagramm umfasst dadurch letztlich 1200 Anforderungen aus der NUREG-Richtlinie und stellt das Grundgerüst der Software MEDIC-Tool dar.

Für ein „Proof of Concept“ (PoC) des MEDIC-Tools wurden aus den 1200 Anforderungen im Bewertungsdiagramm zunächst 30 Anforderungen für die Implementierung in das MEDIC-Tool ausgewählt. Diese 30 Anforderungen wurden so ausgewählt, dass sie eine repräsentative Teilmenge der gesamten 1200 Anforderungen aus den betrachteten Hauptkategorien „Allgemeine Informationsanzeige“, „Benutzerschnittstellen Interaktion und Management“, „Softwaresteuerung“ und „Mensch-Maschine-Schnittstellen-Systeme“ darstellen. Anschließend wurden die gewählten Anforderungen den Beziehungen zwischen den Komponenten des MEDIC-Arbeitssystemmodells (Mensch, MMS, System, Unterlagen) und den diesen Beziehungen zugehörigen MEDIC-Attributen (Übersichtlichkeit, Vorhandensein, Eindeutigkeit, Korrespondenz und Konsistenz) soweit anwendbar zugeordnet. Einige ausgewählte Anforderungen zur Überprüfung von MEDIC-Attributen mit ihren entsprechenden Zuordnungen zu den Beziehungen „MMS → Mensch“, „MMS ←→ MMS“, „MMS → System“ und „Unterlagen → Mensch“ sind beispielhaft in Tab. 4.1 angegeben.

Tab. 4.1 Ausgewählte Anforderungen aus /NUR 02/ zur Überprüfung von MEDIC-Attributen

Hier: Beispiele für ausgewählte Anforderungen aus /NUR 02/ zur Überprüfung von MEDIC-Attributen für die Beziehungen „MMS → Mensch“, „MMS ←→ MMS“, „MMS → System“ und „Unterlagen → Mensch“. Die den Anforderungen zugehörigen MEDIC-Attribute sind in Klammern angegeben.

MMS →Mensch	**MMS ←→ MMS**	**MMS → System**	**Unterlagen → Mensch**
Die Eigenschaften und Merkmale der Anzeige, die zur Darstellung des Prozesses verwendet wird, sollten vom Bediener leicht wahrgenommen und interpretiert werden können. (mentale Zugänglichkeit)	*Alle Begriffe, die in der Benutzeroberfläche des Systems verwendet werden, und ihre Abkürzungen sollten in ihrer Bedeutung konsistent sein.* (Konsistenz) *Für alle Anzeigefunktionen (z. B. Beschriftungen) sollten einheitliche Konventionen für die Oberflächengestaltung gelten.* (Konsistenz) *Alarme und Sollwerte sollten so gestaltet sein, dass nur Parameter und Bedingungen, die außerhalb des normalen und erwarteten Bereichs liegen und die die Aufmerksamkeit des Menschen oder Maßnahmen erfordern, in den Alarmzustand versetzt werden.* (Übersichtlichkeit) *Die Benutzer und Benutzerinnen sollten auf unvollständige Verfahrensschritte aufmerksam gemacht werden.* (Vorhandensein)	*Es sollte eine eindeutige Zuordnung zwischen den Merkmalen und Funktionen des darzustellenden Systems und den Merkmalen der Anzeigedarstellung geben, d. h., Änderungen im Erscheinungsbild der Anzeigeform sollten in einer eins-zu-eins-Beziehung zu den dargestellten Anlagenzuständen stehen. Diese Änderungen sollten sich aus expliziten Regeln ergeben, die die physikalische Form der Anzeige und ihre Bedeutung mit dem dargestellten Anlagenzustand in Beziehung setzen.* (Korrespondenz)	*Jede Prozedur sollte identifizierende Informationen enthalten, einschließlich Titel, Verfahrensnummer, Revisionsnummer, Datum und organisatorische Genehmigung. Diese Informationen helfen dem Benutzer, den richtigen Kontext für die Verwendung der Prozedur herzustellen.* (mentale Zugänglichkeit) *Für jede Prozedur sollten die übergeordneten Ziele und die Anwendbarkeit angegeben werden, einschließlich der Kategorie, z. B. Notfall oder anomaler Zustand.* (mentale Zugänglichkeit)

4.4.2 Funktionen des MEDIC-Tools

Die Nutzerinteraktion im MEDIC-Tool erfolgt über ihre grafische Benutzeroberfläche. Als Sprache wird in der grafischen Oberfläche der Software MEDIC-Tool Deutsch verwendet. Die graphische Benutzeroberfläche des MEDIC-Tools besteht aus fünf Dialogfenstern: das „Willkommen“-Fenster, das „Allgemeine Informationen“-Fenster, das „Hauptfenster“, das „Bewertungsfenster“ und das „Hilfefenster“. Der Bewerter wird anhand dieser Fenster in den Bewertungsprozess mit dem MEDIC-Tool geführt. Nach Beendigung der Bewertung wird vom MEDIC-Tool ein Bewertungsbogen in pdf-Format ausgegeben. Der Inhalt dieses Bewertungsbogens sowie die Funktionen der jeweiligen Dialogfenster des MEDIC-Tools werden nachfolgend detailliert beschrieben.

4.4.2.1 Willkommen beim MEDIC-Tool

Nach dem Start des MEDIC-Tools öffnet sich automatisch ein „Willkommen“-Fenster (Abb. 4.3). Hier hat der Nutzer die Möglichkeit durch das Klicken auf „Neue Bewertung“ eine neue Bewertung zu starten oder durch das Klicken auf „Bewertung laden“ an einer bereits vorhandenen Bewertung zu laden und weiterzuarbeiten.

Abb. 4.3 Das „Willkommen“-Fenster öffnet sich automatisch nach dem Start des MEDIC-Tools

4.4.2.2 Allgemeine Informationen

Startet man eine neue Bewertung, öffnet sich das Eingabefenster für die allgemeinen Informationen (Abb. 4.4) der MEDIC-Bewertung.

Abb. 4.4 Eingabefenster „Neue Bewertung“

In dem Fenster „Allgemeine Informationen“ wird eine Vorauswahl für die Bewertung vorgenommen, sowie alle allgemeinen Informationen der Bewertung angegeben.

In den obigen sechs Feldern des Fensters „Allgemeine Informationen“ kann der Name des Bearbeiters, die Spezifikation der MMS sowie die zur Verfügung stehenden Dokumente eingetragen werden. Außerdem kann eine detaillierte Aufgabenbeschreibung hinterlegt werden. Die unteren sogenannten „Check Boxes“ dienen einer Vorauswahl der später angezeigten Anforderungen. Beispielsweise kann u. a. angegeben werden, ob die zu bewertende Oberfläche „Alarme“ oder Fließbilder (Checkbox „Flussdiagramme“ im Fenster „Allgemeine Informationen“) enthält. Bei der Bewertung werden anschließend nur noch relevante Anforderungen angezeigt. Mit „Übernehmen“ werden die allgemeinen Informationen für diese Bewertung übernommen, danach öffnet sich das Hauptfenster des MEDIC-Tools.

4.4.2.3 Hauptfenster

Das Hauptfenster (Abb. 4.5) ist der Ausgangspunkt für alle weiteren Schritte der MEDIC-Bewertung.

Abb. 4.5 Hauptfenster des MEDIC-Tools

Hier: Anzeige der allgemeinen Informationen und des aktuellen Bewertungsstandes. Von hier aus können weitere Schritte zur Bewertung der MMS vorgenommen werden.

In Abb. 4.6 sind die verschiedenen Bereiche des Hauptfensters des MEDIC-Tools dargestellt. Zunächst werden alle angegebenen allgemeinen Informationen im Bereich 3 angezeigt. Unterhalb der allgemeinen Informationen, im Bereich 4, wird der Fortschritt in der MEDIC-Bewertung in Form einer Fortschrittanzeige („Progressbar“ in PyQt genannt) angezeigt. In diesem Beispiel ist der aktuelle Bearbeitungsstand bei 0%, da noch keine der 23 Anforderungen beantwortet wurde. Oberhalb der allgemeinen Informationen, im

Bereich 2, wurde ein „Toolbar“ implementiert. Hier ist ein schneller Zugriff auf „Speichern“, „Neue Bewertung“, „Bewertung öffnen“ und „Bewertungsbogen erstellen“ möglich. Die gleichen Aktionen sind ebenso über das Menü „Datei“ in dem Menübar in Bereich 1, ausführbar. Weitere aktuelle Informationen, wie der Status nach dem Speichern, werden in dem Statusbar (Bereich 6) angezeigt.

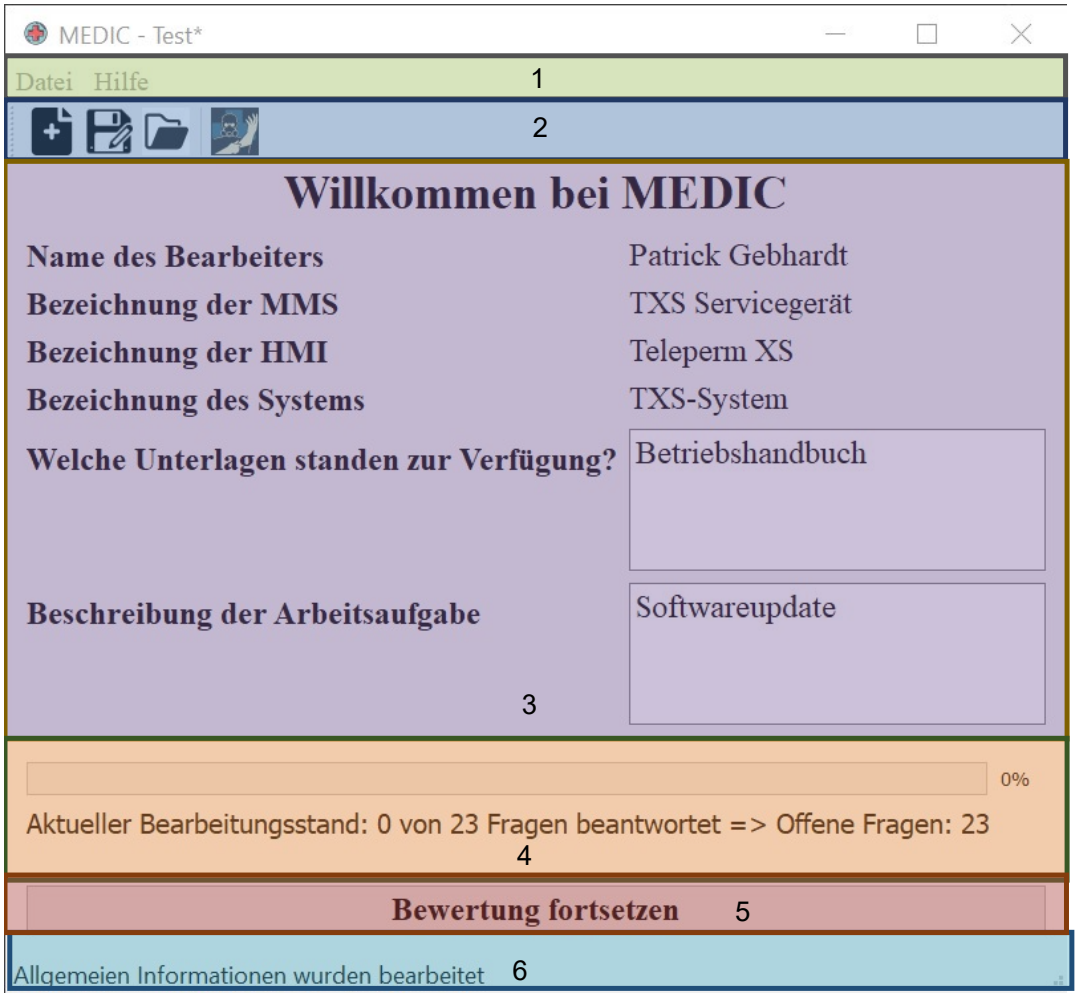

Abb. 4.6 Aufteilung des Hauptfensters des MEDIC-Tools

Oberhalb des Bereichs 1 sind die als Standard-Steuerelemente „Minimieren“, „Maximieren“ und „Schließen“ von Anwendungsfenstern in Betriebssystemen für das Hauptfenster des MEDIC-Tools enthalten. Durch das Klicken auf „Bewertung fortsetzen“ im Bereich 5 öffnet sich das Bewertungsfenster (Kapitel 4.4.2.4).

4.4.2.4 Bewertungsfenster

Eine kleine Auswahl der in Kapitel 4.4.1 erarbeiteten Fragen wurde im MEDIC-Tool, in das MEDIC-Bewertungsfenster, implementiert. In dem Bewertungsfenster (siehe Abb. 4.7) werden die Anforderungen aufgelistet, bereits gestellte Antworten dargestellt und eine Weiterleitung zum zugrundeliegenden Dokument, aus dem die Kriterien abgeleitet wurden, angeboten. In der jetzigen Fassung des MEDIC-Tools sind Kriterien aus der NUREG 0700 /NUR 02/ implementiert. Der Bewerter erhält daher den entsprechenden Auszug aus /NUR 02/.

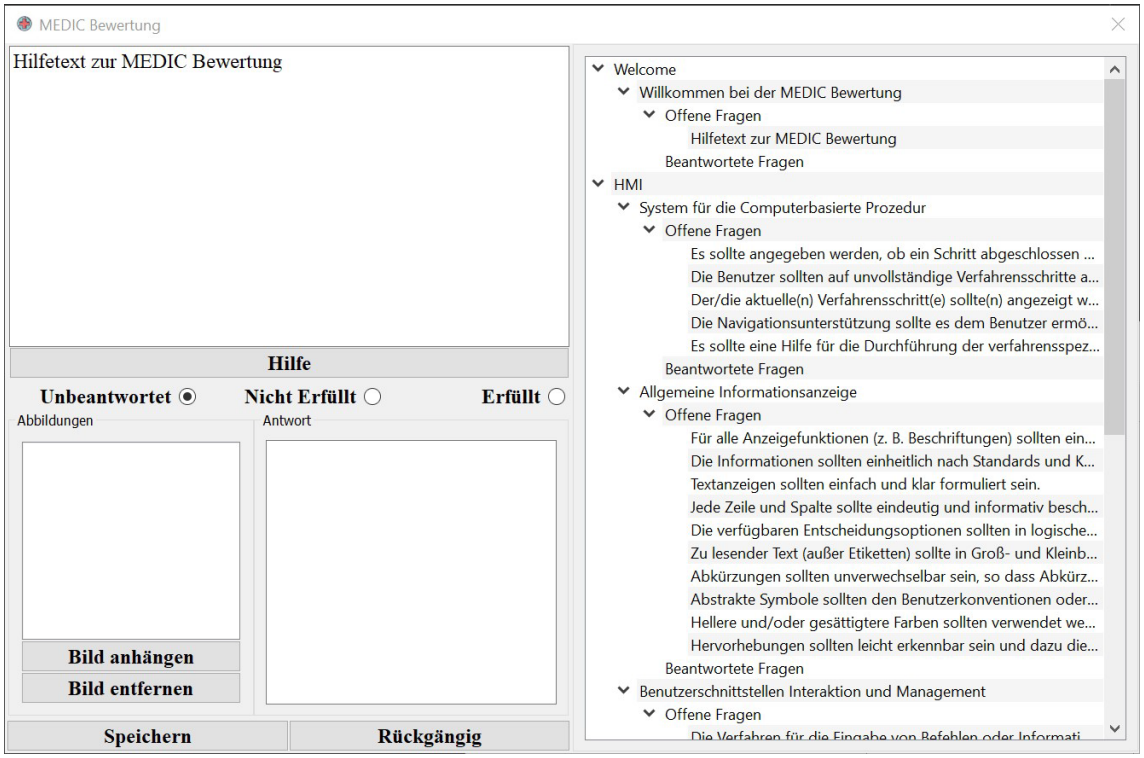

Abb. 4.7 Das Bewertungsfenster nach dem Starten einer Bewertung

Die Anforderungen werden auf der rechten Seite des Bewertungsfensters (siehe Bereich 2 der Abb. 4.8) in einer sogenannten Baumansicht („TreeView“ in PyQt genannt) übersichtlich dargestellt. Dabei sind die Anforderungen zunächst in vier Hauptkategorien gemäß den vier MEDIC-Komponenten „Unterlagen“, „MMS“ (im MEDIC-Tool „HMI“), „System“ und „Mensch“ (im MEDIC-Tool „Human“) unterteilt worden. Zusätzlich gibt es eine „Willkommen“ Hauptkategorie, in welcher eine Erläuterung zur MEDIC-Bewertungsmethode und der Umgang mit dem MEDIC-Tool beschrieben wird. Innerhalb der Hauptkategorien wurden die Anforderungen weiter in Unterkategorien unterteilt. Die Unterkategorien entsprechen der aus NUREG-0700 übernommenen Einteilung der

Anforderungen. Beispielsweise werden unter „Allgemeine Informationsanzeige“ alle allgemeinen Anforderungen an eine Informationsanzeige aufgelistet. Zuletzt wurden die Anforderungen in „Offene Fragen“ und „Beantwortete Fragen“ aufgeteilt. Dadurch ist ein sofortiger Überblick über die in diesem Bereich noch zu beantwortenden Fragen gewährleistet. Nach der Auswahl einer dieser Fragen aus dem „TreeView“ (ein Einfaches „Anklicken“ der Anforderung), wird die Frage im Bereich 1 (siehe Abb. 4.8) vollständig angezeigt. Der Button „Hilfe“ im Bereich 3 (siehe Abb. 4.8) führt den Anwender auf die der Frage zugehörigen originalen Anforderung aus der NUREG-0700 (vgl. Kapitel 4.4.2.5) in englischer Sprache. Die Bereiche 4, 5 und 6 (siehe Abb. 4.8) dienen der Beantwortung der Frage. Im Bereich 4 sind drei sogenannte „Radio Buttons“ angelegt, hier kann der Nutzer zwischen „Unbeantwortet“, „Nicht Erfüllt“ und „Erfüllt“ entscheiden. Der Standardwert ist „Unbeantwortet“. Dies bedeutet, dass die Frage bisher noch nicht beantwortet wurde.

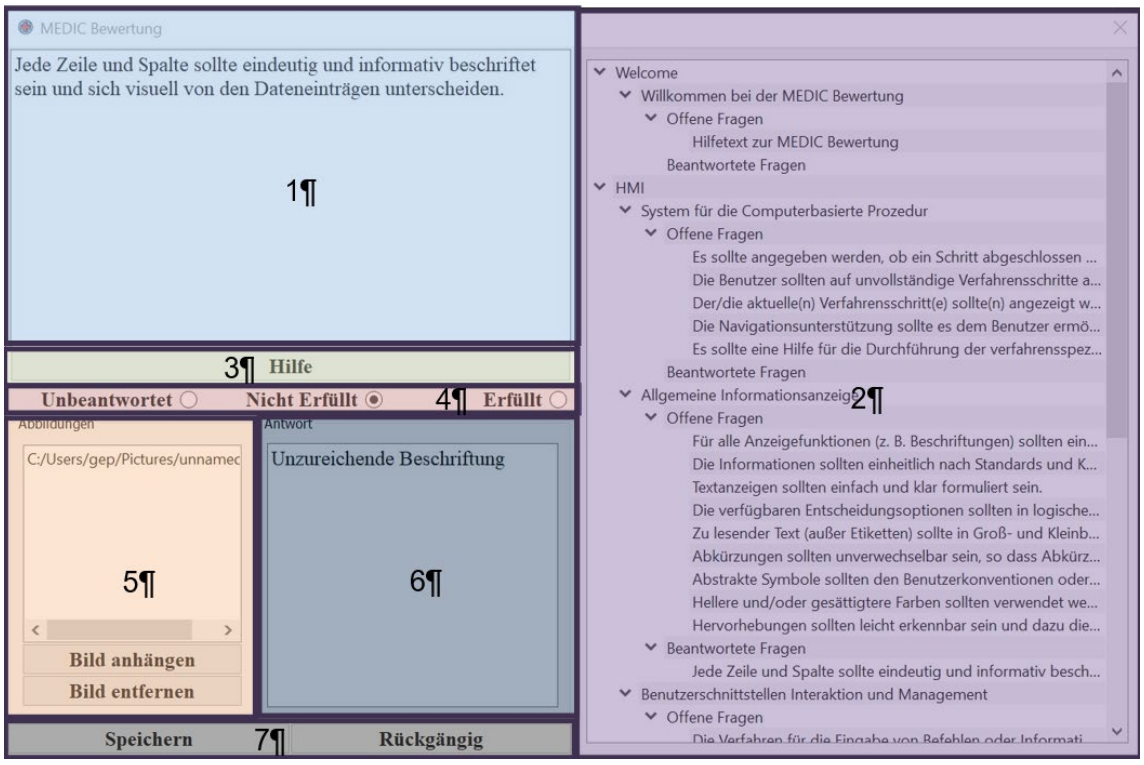

Abb. 4.8 Einteilung des Bewertungsfensters in verschiedene Bereiche

Selbsterklärend stehen die Antwortmöglichkeiten „Nicht Erfüllt“ und „Erfüllt“ dafür, dass die der Frage zugehörige Anforderung entweder erfüllt ist oder nicht. Nach Auswahl einer dieser beiden Möglichkeiten und nach dem Speichern ändert sich der Fortschrittbalken im MEDIC-Hauptfenster (Abb. 4.6, Bereich 4). Es ist außerdem möglich, Bilder (Abbildungen oder Screenshots der zu bewertenden MMS) mit den Fragen zu verknüpfen

(Bereich 5). Entweder können die Bilder per Drag-n-Drop angehängt oder durch Klicken auf „Bild anhängen“ hinzugefügt werden. Die hinzugefügten Bilder werden anschließend bei Auswahl der entsprechenden Frage aufgelistet dargestellt. Durch Auswahl eines der Bilder aus der Liste und durch das Klicken auf „Bild entfernen“, kann das angehängte Bild, wenn gewünscht, wieder entfernt werden. Im Bereich 6 kann zudem ein Antworttext verfasst werden. Beispielsweise beim Nichterfüllen der Frage/Anforderung ist es möglich, eine Begründung für diese Nichterfüllung zu hinterlegen. Letztlich kann, wie bereits erwähnt, der Fortschritt der Bewertungsaufgabe im Bereich 7 gespeichert werden. Es ist auch möglich, alle bisherigen Änderungen seit dem letzten Speichern rückgängig zu machen. Nach dem Beantworten aller Fragen und dem Speichern kann zum Hauptfenster zurückgekehrt und der Bewertungsbogen erstellt werden. Wie eingangs bereits erwähnt, verweist der „Hilfe“-Button auf die Textpassage im NUREG-0700. Dies wird im folgenden Abschnitt genauer erläutert. Anschließend wird die Struktur des Bewertungsbogens näher beschrieben.

4.4.2.5 Hilfefenster

Das Hilfefenster (Abb. 4.9) besteht aus zwei Bereichen. Auf der linken Seite werden alle Verweise auf die passende Stelle in NUREG-0700 aufgelistet. Durch einen Klick auf das Element in der Liste wird die passende Stelle im NUREG-0700 aufgerufen und auf der rechten Seite des Hilfefensters in englischer Sprache angezeigt. Über die Buttons an der rechten Toolbar kann durch das geöffnete Dokument „geblättert“, die geöffnete Seite vergrößert oder die Ansicht umgestaltet werden.

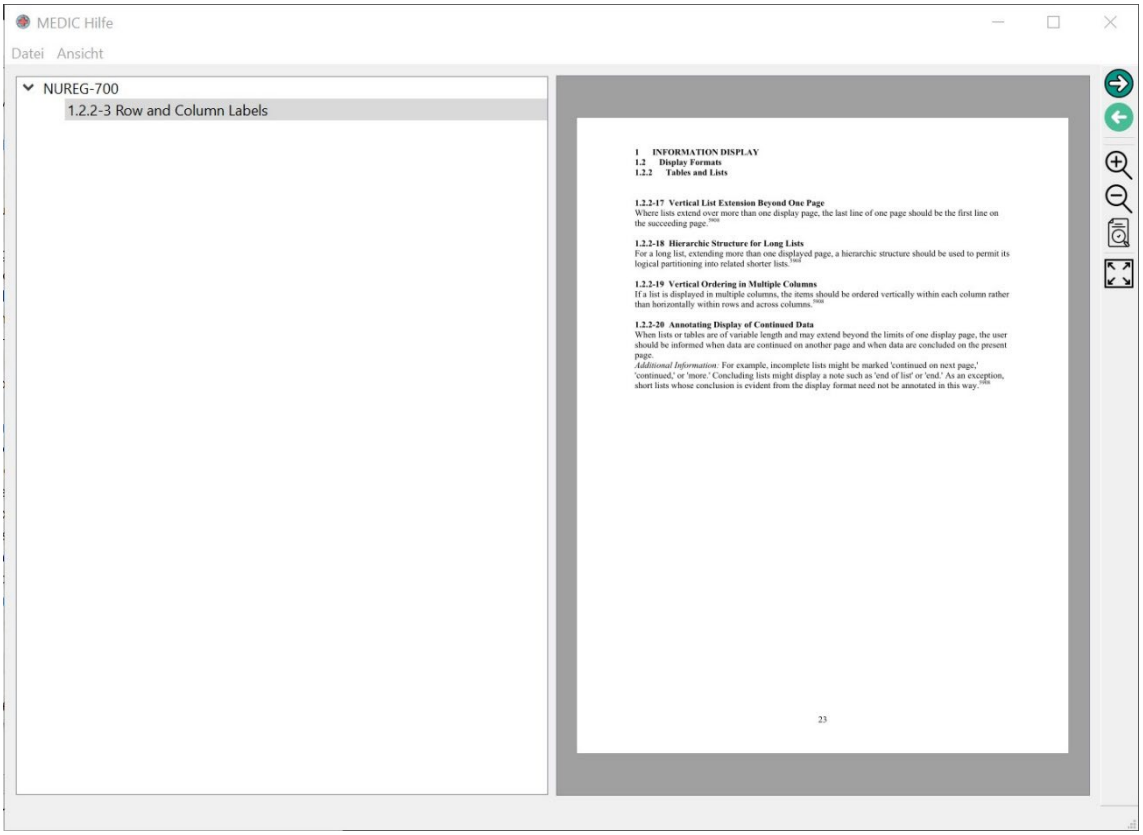

Abb. 4.9 Hilfefenster mit der relevanten NUREG Anforderung

Das Hilfefenster kann zudem auch vom Hauptfenster aus aufgerufen werden. Jedoch werden nun alle Informationen angezeigt (sieheAbb. 4.10), im Gegensatz zum Aufrufen aus dem Bewertungsfenster, wo nur die spezifische Passage angezeigt wird.

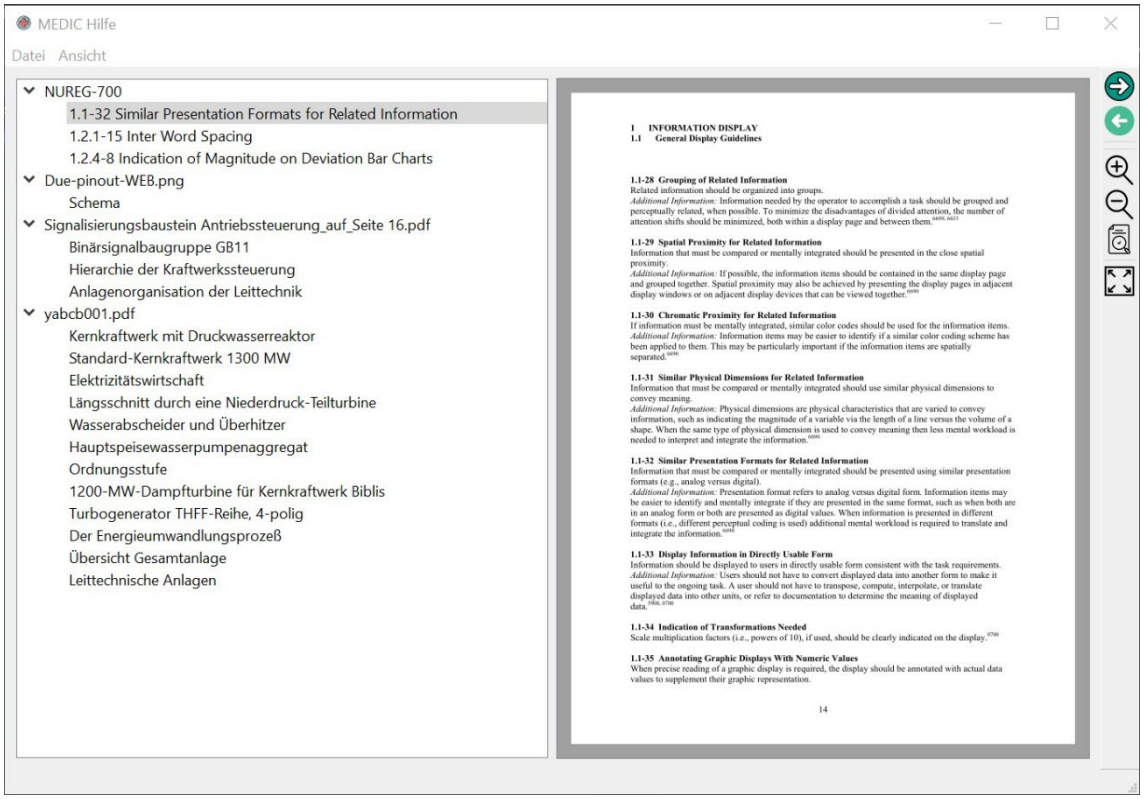

Abb. 4.10 Hilfefenster mit allen Anforderungen und verwiesenen Dokumenten

Die für die Bewertung hinterlegten Dokumente werden in ihrer jeweiligen Originalsprache angezeigt.

4.4.2.6 Bewertungsbogen

Im ersten Kapitel des Bewertungsbogens werden alle angegebenen allgemeinen Informationen tabellarisch angezeigt. Das darauffolgende Kapitel beinhaltet den Leitfaden zur MEDIC-Bewertungsmethode. Hier finden sich alle Erläuterungen zur MEDIC-Bewertungsmethode. Im dritten Kapitel werden schließlich alle Anforderungen an die zugrundeliegende MMS dargestellt. Die Unterpunkte zu den dargestellten Anforderungen beinhalten die Information, ob die Anforderung erfüllt wurde, die angegebene Beschreibung zur Antwort, die Zuordnung zu den MEDIC-Attributen, Informationen zu dem Abschnitt in der NUREG 0700 und alle angehängten Abbildungen. Im letzten Abschnitt des MEDIC-Bewertungsbogens erfolgt die eigentliche Bewertung der MMS. Dabei wird der Erfüllungsgrad der MEDIC-Attribute aufgelistet. Es wird angegeben, wie viele der zu den MEDIC-Attributen zugeordneten Anforderungen „Erfüllt“, „Nicht Erfüllt“ oder „Unbeantwortet“ sind. Außerdem werden die MEDIC-Attribute in einem MEDIC- Radarplot dargestellt (vgl. Abb. 4.11). Die Achsen des Diagramms geben dabei den Erfüllungsgrad der jeweiligen Attribute in Prozent an.

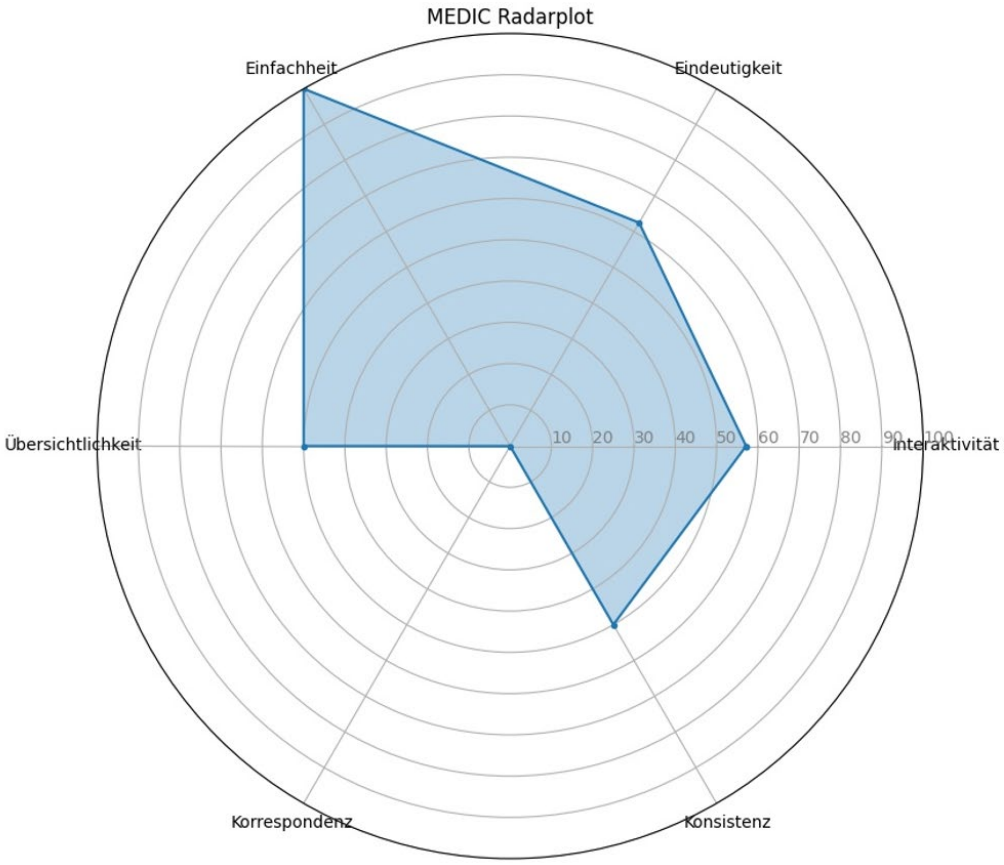

Abb. 4.11 Beispiel eines MEDIC-Diagramms

4.5 Zusammenfassung

Für die Anwendung der MEDIC-Bewertungsmethode wurde im Rahmen des Vorhabens das MEDIC-Analysewerkzeug zur Bewertung von technischen Vorkehrungen gegen Fehler durch Personalhandlungen an MMS in softwarebasierten Leittechniksystemen entwickelt. Das MEDIC-Analysewerkzeug besteht aus den eigenständigen Tools „MEDIC-MMS“, „MEDIC-Tool“ und „MEDIC-AnTeS“, welche flexibel zur Bewertung von technischen Vorkehrungen zur Vermeidung von Personalfehlhandlungen, eingesetzt werden können.

Mit dem Framework „MEDIC-MMS“ können als graphische Benutzeroberflächen realisierten MMS, wie sie typischerweise in softwarebasierten Leittechniksystemen als MMS für Steuerungs- und Überwachungsaufgaben eingesetzt werden, entwickelt werden. Hierbei ist es möglich sowohl graphische Benutzeroberflächen neu zu entwickeln als

auch bereits eingesetzte graphische Benutzeroberflächen bei verfügbaren Informationen zum Design nachzubilden. Die so entwickelten graphischen Benutzeroberflächen können anschließend in Bezug auf die Eignung der realisierten technischen Vorkehrungen zur Vermeidung von Personalfehlhandlungen gemäß der MEDIC-Bewertungsmethode bewertet werden.

Die Software „MEDIC-Tool“ dient der softwaregestützten Bewertung von als graphischen Oberflächen realisierten typischen MMS softwarebasierter Leittechniksysteme gemäß der im Kapitel 3 dargestellten MEDIC-Bewertungsmethode. Die Nutzerinteraktion mit der Software MEDIC-Tool erfolgt über eine hierfür entwickelte grafische Benutzeroberfläche, welche aus entsprechenden Dialogfenstern besteht. Der Bewerter wird anhand dieser Fenster in den Bewertungsprozess mit dem MEDIC-Tool geführt, indem ihm in Bezug auf die Bewertungsaufgabe nacheinander Einzelfragen bzw. zu prüfende Kriterien und Erläuterungen zur Frage bzw. zum Kriterium angezeigt werden. Der Bewerter kann dann die angezeigte Frage mit „Erfüllt“ oder „Nicht Erfüllt“ beantworten. Als Bewertungsgrundlage wird in der derzeitigen Softwareversion des MEDIC-Tools die NUREG 0700-Richtlinie aufgrund ihres hohen Detaillierungsgrades in Bezug auf die Anforderungen zur Vermeidung von Fehlhandlungen an Mensch-Maschine-Schnittstellen herangezogen.

Als MEDIC-AnTeS wird die Komponente des MEDIC-Analysewerkzeugs bezeichnet, mit der zu bewertende Arbeitssysteme für die Durchführung von Wartungs- und Instandhaltungsaufgaben an softwarebasierten Leittechniksystemen realisiert und spezifiziert werden. Mit MEDIC-AnTeS können beispielsweise TXS-basierte Arbeitssysteme mit den vorhandenen Komponenten des Moduls 1 „Reales Leittechniksystem“ des GRS-AnTeS /GRS 21/ entwickelt und nachgebildet werden. Die so entwickelten Arbeitssysteme können anschließend mit der MEDIC-Bewertungsmethode gemäß Kapitel 3 bewertet werden.

5 Zusammenfassung und Schlussfolgerung

Das Ziel dieses Vorhabens war die Entwicklung einer Methode zur Bewertung von technischen Vorkehrungen gegen Personalfehlhandlungen an Mensch-Maschine-Schnittstellen (MMS) digitaler Leittechniksysteme. Ein wichtiger Schwerpunkt der Arbeiten lag auf der Analyse potenzieller Mängel von technischen Vorkehrungen gegen Personalfehlhandlungen an typischen MMS digitaler Leittechniksysteme.

Hierfür wurden zunächst die relevanten Begriffe und Vorgehensweisen auf Grundlage des Standes von Wissenschaft und Technik (z. B. in kerntechnischen Normen und Fachberichten) identifiziert und beschrieben.

Typischerweise werden Modelle des ´ Arbeitssystems (bzw. des Mensch-Maschine-Systems) für die Analyse und Bewertung der menschlichen Zuverlässigkeit bei der Durchführung einer Aufgabe bzw. Tätigkeit in der Arbeitswissenschaft verwendet. Das Arbeitssystem setzt sich entsprechend aus mehreren Komponenten zusammen, die für die Erledigung der Arbeitsaufgabe an der Mensch-Maschine-Schnittstelle notwendig sind und zur Erreichung des Aufgabenziels zusammenwirken. Zu den Komponenten eines Arbeitssystems zählen u. a. der Mensch als Systembediener, die Mensch-Maschine-Schnittstelle, die zu bedienende Einrichtung sowie die Arbeitsumgebung. Die Mensch-Maschine-Schnittstelle ist hierbei die Komponente des Arbeitssystems, welche als direktes Kommunikationsmittel zwischen Menschen und zu bedienender Einrichtung vorgesehen ist und über die der Betrieb der Einrichtung gesteuert und überwacht wird. In softwarebasierten Leittechniksystemen werden für Steuerungs- und Überwachungsaufgaben in der Regel bildschirmgestützte Benutzeroberflächen mit Softcontrol-Elementen als MMS eingesetzt. Für Softwarewartungsaufgaben in softwarebasierten Leittechniksystemen werden menügeführte grafische Benutzeroberflächen mit Auswahl- und Dialogfenstern der eingesetzten Engineering-Tools als MMS eingesetzt. MMS in den Leittechnikschränken digitaler Leittechniksysteme enthalten neben grafischen Benutzeroberflächen auch konventionelle Bedienelemente wie z. B. Schlüsselschalter und Diagnosestecker.

In einem weiteren Arbeitsschritt wurden relevante nationale und internationale kerntechnische Regelwerke, Normen, und Richtlinien nach Anforderungen zur Vermeidung bzw. Minimierung von Personalfehlhandlungen an Mensch-Maschine-Schnittstellen ausgewertet. Da der Einsatz von bildschirmgestützten Benutzeroberflächen (grafische Benutzeroberflächen) als Mensch-Maschine-Schnittstellen charakteristisch für

softwarebasierte Leittechniksysteme ist, wurden diese kerntechnischen Regelwerke, Normen und Richtlinien insbesondere nach spezifischen Anforderungen an die Auslegung und Gestaltung von als graphischen Benutzeroberflächen eingesetzten MMS für softwarebasierte Leittechniksysteme zwecks Minimierung von Personalfehlhandlungen ausgewertet. Die in diesen Regelwerken, Normen und Richtlinien identifizierten Anforderungen hinsichtlich technischer Vorkehrungen gegen Personalfehlhandlungen an Mensch-Maschine-Schnittstellen unterscheiden sich in dem Detaillierungsgrad und in den berücksichtigten Aspekten. So weist insbesondere die Richtlinie NUREG 0700 /NUR 02/ hier einen sehr hohen Detaillierungsgrad auf. Allen ausgewerteten Regelwerken, Normen und Richtlinien ist gemeinsam, dass ergonomische Aspekte einer hohen Bedeutung bei der Vermeidung bzw. Minimierung von Personalfehlhandlungen zukommt.

Für die Analyse von Ursachen für potenzielle Mängel von technischen Vorkehrungen gegen Personalfehlhandlungen an typischen MMS digitaler Leittechniksysteme wurde im Rahmen dieses Vorhabens die MEDIC-Bewertungsmethode zur qualitativen Bewertung von technischen Vorkehrungen gegen Personalfehlhandlungen an MMS softwarebasierter Leittechniksysteme entwickelt.

Hierfür wurde zunächst anhand einer Literaturrecherche der für das Vorhaben relevante Stand von Wissenschaft und Technik zur Modellierung von Arbeitssystemen für die Bewertung von Mensch-Maschine-Schnittstellen ermittelt. Es ergibt sich daraus, dass für die Bewertung von Mensch-Maschine-Schnittstellen zunächst das Arbeitssystem, in dem die Mensch-Maschine-Schnittstelle eingebettet ist, zu modellieren ist. Hierbei sind die zu betrachtenden Elemente des Arbeitssystems, die Beziehungen dieser Elemente zueinander sowie die für die Bewertung relevanten Aspekte der Elemente und der Beziehungen zwischen diesen Elementen zu spezifizieren. Die Festlegung der zu berücksichtigenden Elemente und Interaktionen zwischen den Elementen des Arbeitssystems hängt vom angestrebten Ziel der Bewertung der Mensch-Maschine-Schnittstelle ab. Dies stellt ein wesentliches Unterscheidungsmerkmal zwischen den verschiedenen Arbeitssystemmodellen dar.

Bei den Modellen zur Bewertung der Ergonomie von Benutzerschnittstellen von interaktiven Rechnersystemen wird der Schwerpunkt auf die Benutzerfreundlichkeit der eingesetzten Soft- und Hardwareschnittstellen gelegt. Für die Bewertung der Benutzerfreundlichkeit wird die Benutzerschnittstelle in Teilschnittstellen unterteilt, welche auf verschiedene Aspekte hinsichtlich der Benutzerfreundlichkeit einer Benutzerschnittstelle

verweisen. Zu diesen Modellen gehört beispielsweise das von der „International Federation for Information Processing“[17] (IFIP) entwickelte „IFIP-Modell“, welches als Grundlage für in verschiedenen Normen enthaltene Anforderungen wie beispielsweise ISO 9241 „Ergonomie der Mensch-System-Interaktion“ dient.

Den verwendeten Arbeitssystemmodellen zur Analyse der menschlichen Zuverlässigkeit bei der Durchführung einer Aufgabe an einer Mensch-Maschine-Schnittstelle ist gemeinsam, dass sie die Elemente „Mensch“ und „Maschine“ beinhalten. Diese Arbeitssystemmodelle unterscheiden sich insbesondere dadurch, wie der Einfluss der Umgebung auf die Interaktionen zwischen dem Menschen und der Maschine berücksichtigt wird. Dies schließt sowohl die physischen Umgebungsbedingungen wie z. B. Lärm und Beleuchtung als auch das soziale Umfeld wie z. B. die Organisationsstruktur und die Arbeitsabläufe ein. Zu diesen Modellen gehört das vom VDI[18] entwickeltes Modell eines Arbeitssystems zur Beschreibung der menschlichen Zuverlässigkeit an Mensch-Maschine-Schnittstellen, welches beispielsweise als Grundlage für die in /DIN 11/ enthaltenen Anforderungen an die ergonomische Gestaltung dient.

Basierend auf den gewonnenen Erkenntnissen zu Arbeitssystemmodellen für die Bewertung von Mensch-Maschine-Schnittstellen wurde anschließend das MEDIC-Arbeitssystemmodell als Grundlage für die im Rahmen dieses Vorhabens entwickelte MEDIC-Bewertungsmethode erstellt. Das MEDIC-Arbeitssystemmodell besteht aus den Komponenten „Mensch“, „Unterlagen“, „Mensch-Maschine-Schnittstelle (MMS)“ und dem zu bedienenden „System“.

Im MEDIC-Arbeitssystemmodell werden sowohl die Beziehungen zwischen den Teilelementen der Komponenten als auch die Beziehungen zwischen den Komponenten des Arbeitssystems, in dem die MMS eingebettet ist, untereinander betrachtet. Die menschlichen leistungsbeeinflussenden Faktoren (z. B. Motivation, Qualifikation) bei der Durchführung der Aufgabe werden im Rahmen der MEDIC-Bewertungsmethode noch nicht berücksichtigt, da im Rahmen dieses Vorhabens die potenziellen Ursachen für Personalfehlhandlungen an der MMS in Bezug auf Mängel technischer Vorkehrungen gegen Fehlhandlungen an der MMS im Vordergrund standen.

---

[17] Internationalen Dachorganisation für nationale Gesellschaften und Akademien der Wissenschaften im Bereich der Informations- und Kommunikationstechnologie

[18] VDI: Verein Deutscher Ingenieure

Im Rahmen der MEDIC-Bewertungsmethode wird angenommen, dass die Eigenschaften der Beziehungen zwischen den Komponenten des MEDIC-Arbeitssystemmodells die Minimierung bzw. die Vermeidung von Personalfehlhandlungen an MMS maßgeblich mitbestimmen. Es wurden daher im Rahmen der MEDIC- Bewertungsmethode Attribute zur Charakterisierung dieser Beziehungen eingeführt. Diese Attribute (Konsistenz, Korrektheit, …) betreffen die allgemeine Ergonomie und Verständlichkeit der Mensch-Maschine-Schnittstelle. Sie sind in der MEDIC-Interrelationsmatrix zusammengefasst. Gemäß der MEDIC-Bewertungsmethode sollen diese Attribute erfüllt sein, um Personalfehlhandlungen an MMS zu vermeiden bzw. zu minimieren.

Bei der Bewertung von technischen Vorkehrungen gegen Fehlhandlungen an einem Arbeitssystem mit der MEDIC-Bewertungsmethode wird daher überprüft, inwieweit die eingeführten Attribute zur Charakterisierung bzw. Kennzeichnung der Teilelemente der MMS und der Beziehungen zwischen den Teilelementen erfüllt sind. Das Attribut für das betrachtete Teilelement bzw. für die betrachtete Beziehung des MEDIC- Arbeitssystemmodells gilt dann als erfüllt, wenn alle dem Attribut zugeordneten Kriterien als erfüllt anzusehen sind. Die Bewertung erfolgt hierbei als Expertenschätzung. Hierzu ist gemäß der MEDIC- Bewertungsmethode vom Bewerter ein entsprechender Kriterien- bzw. Fragenkatalog für das betrachtete Attribut anhand von relevanten Normen und Regelwerken (z. B. NUREG 0700, KTA) zu entwickeln und anzuwenden. Im Rahmen der MEDIC-Bewertungsmethode wurden Kriterien zur Ermittlung des Erfüllungsgrades der eingeführten Attribute aus der NUREG 0700-Richtlinie /NUR 02/ abgeleitet.

Um eine einheitliche Verwendung der Methode und eine systematische Vorgehensweise bei der Anwendung der MEDIC-Bewertungsmethode zu ermöglichen, wurde ein Anwendungsleitfaden entwickelt, in dem die durchzuführenden Schritte bei der Anwendung der MEDIC-Bewertungsmethode spezifiziert sind. Wesentlich hierbei ist, dass die zu betrachtenden Beziehungen sowie die Attribute zur Charakterisierung der Beziehungen zwischen den Komponenten des MEDIC-Arbeitssystemmodells abhängig von der durchzuführenden Aufgabe an der MMS spezifiziert werden. Dies ermöglicht es, die MEDIC-Bewertungsmethode für verschiedene Typen von Arbeitssystemen anzuwenden.

Die Anwendbarkeit der MEDIC-Bewertungsmethode zur Bewertung von technischen Vorkehrungen gegen Personalfehlhandlungen an MMS konnte anhand von Beispielen demonstriert werden. Hierbei wurden MMS, die an typische MMS softwarebasierter Leittechniksysteme für Steuerungsaufgaben angelehnt sind, sowie MMS zur Durchführung von Wartungsaufgaben an einem Leittechnikschrank eines digitalen Leittechniksystems,

betrachtet. Als weiteres Anwendungsfeld wurde die Eignung der MEDIC-Bewertungsmethode zur nachträglichen Bewertung von MMS, die als ursächlich für Personalfehlhandlungen bei meldepflichtigen Ereignissen in Kernkraftwerken identifiziert wurden, erprobt. Es zeigte sich hierbei, dass die MEDIC-Bewertungsmethode dazu geeignet ist, fehlerverursachende Mängel von technischen Vorkehrungen zu erkennen.

Zur softwaregestützten Anwendung der MEDIC-Bewertungsmethode wurde im Rahmen des Vorhabens das MEDIC-Analysewerkzeug entwickelt, welches aus mehreren eigenständigen Softwaretools besteht. Im derzeitigen Entwicklungsstand setzt sich das MEDIC-Analysewerkzeug aus der Software MEDIC-Tool, dem Framework MEDIC-MMS sowie aus der Komponente MEDIC-AnTeS zusammen.

Mit dem Tool MEDIC-MMS können grafische Benutzeroberflächen, wie sie typischerweise in softwarebasierten Leittechniksystemen als MMS für Steuerungs- und Überwachungsaufgaben eingesetzt werden, entwickelt und anschließend bewertet werden.

MEDIC-AnTeS ist die Komponente des MEDIC-Analysewerkzeugs, mit der Arbeitssysteme für die Durchführung von Wartungs- und Instandhaltungsaufgaben an softwarebasierten Leittechniksystemen über typische hierfür verwendeten MMS mit den Komponenten des Moduls 1 „Reales Leittechniksystem“ des GRS-AnTeS entwickelt, spezifiziert und anschließend mit der MEDIC-Bewertungsmethode bewertet werden. Hierbei können sowohl neue als auch bereits vorhandene TXS-basierte Arbeitssysteme analysiert werden. Darüber hinaus können auch andere Arbeitssysteme für Wartungs- und Instandhaltungsaufgaben, welche auf anderen digitalen Leittechnikplattformen basieren, bei grundsätzlichem Vorliegen entsprechender Informationen unabhängig von MEDIC-AnTeS mit der MEDIC-Bewertungsmethode bewertet werden.

Das MEDIC-Tool wurde entwickelt, um den Nutzer der MEDIC-Bewertungsmethode systematisch durch die Bewertung von Arbeitssystemen mit der MEDIC-Bewertungsmethode zu führen. Es dient dazu, die Bewertung von technischen Vorkehrungen mit der MEDIC-Bewertungsmethode zu vereinfachen und die Reproduzierbarkeit der Ergebnisse zu verbessern. Nacheinander werden dem Nutzer des MEDIC-Tools in Bezug auf die Bewertungsaufgabe Einzelfragen bzw. zu prüfende Kriterien und Erläuterungen zur Frage bzw. zum Kriterium angezeigt. Der Nutzer kann dann die angezeigte Frage mit „Erfüllt“ oder „Nicht Erfüllt“ beantworten. Als Bewertungsgrundlage wird in der derzeitigen Softwareversion des MEDIC-Tools die NUREG 0700-Richtlinie /NUR 02/ aufgrund

ihres hohen Detaillierungsgrades in Bezug auf die Anforderungen zur Vermeidung von Personalfehlhandlungen an Mensch-Maschine-Schnittstellen herangezogen.

Bei der im Rahmen dieses Vorhabens entwickelten MEDIC-Bewertungsmethode zur Bewertung von technischen Vorkehrungen gegen Personalfehlhandlungen an MMS digitaler Leittechniksysteme wird der Einfluss des Menschen auf das Arbeitssystem nicht betrachtet. Dies diente dazu, die MMS zunächst in Bezug auf die realisierten technischen Vorkehrungen zur Vermeidung von Bedienfehlern zu bewerten. Die MEDIC-Bewertungsergebnisse sind demnach als Prognose hinsichtlich des Auftretens von Personalfehlhandlungen an MMS in Abhängigkeit von den vorhandenen technischen Vorkehrungen aufzufassen. Das Einbeziehen des Einflusses des Menschen auf das Arbeitssystem in die MEDIC-Bewertung ermöglicht es, MEDIC-Bewertungsergebnisse für eine MMS und tatsächlich beobachtete Bedienfehlern an dieser MMS in Abhängigkeit von den technischen Vorkehrungen zur Vermeidung von Fehlhandlungen an der MMS gegenüberzustellen und somit die MEDIC-Bewertungsmethode zu verifizieren und ggfs. anzupassen. Hierfür wäre das MEDIC-Arbeitssystemmodell so zu erweitern, dass der Einfluss des Menschen, welcher durch interne leistungsbeeinflussende Faktoren beschrieben wird, berücksichtigt werden kann. Die Klärung dieser Fragestellungen stellt einen möglichen Schwerpunkt für künftige Forschungsarbeiten z. B. im Rahmen eines Nachfolgevorhabens dar, um die MEDIC-Bewertungsmethode weiterzuentwickeln.

Literaturverzeichnis

/BAD 22/ https://www.bad-gmbh.de/glossar/show-term/arbeitssystem/, abgerufen am 23.02.2022

/BMU 15/ Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit: Sicherheitsanforderungen an Kernkraftwerke, 03. März 2015

/BOY 11/ Guy A. Boy (Hrsgb.): The Handbook of Human-Machine Interaction. A Human-Centered Design Approach, Ashgate Pub Co, 2011

/DIN 88/ DIN 66234-8, Bildschirmarbeitsplätze; Grundsätze ergonomischer Dialoggestaltung, 1988

/DIN 03/ DIN EN 60073 VDE 0199, Grund- und Sicherheitsregeln für die Mensch-Maschine-Schnittstelle: Kennzeichnung Codierungsgrundsätze für Anzeigegeräte und Bedienteile, 2003

/DIN 06/ DIN EN ISO 9241-110, Ergonomie der Mensch-System-Interaktion, 2006

/DIN 11/ DIN IEC 62508 VDE 0050-2:2011-05: Leitlinien zu den menschlichen Aspekten der Zuverlässigkeit, 2011

/DIN 15/ DIN IEC 62441 „Kernkraftwerke- Warte – Alarmfunktionen und ihre Darstellung“, 2015

/DIN 88/ DIN 66234 Teil 8 „Bildschirmarbeitsplätze. Grundsätze der Dialoggestaltung“, 1988

/EIC 22/ „Heuristische Evaluation“, Armin Eichinger, Universität Regensburg, Institut für Psychologie, https://www.uni-regensburg.de/Fakultaeten/phil_Fak_II/Psychologie/Doktoranden/absolventen/eichinger_armin/u-evaluation.html, abgerufen am 21.02.2022

/EPR 04/ EPRI, Human Factors Guidance for Control Room and Digital Human-System Interface Design and Modification, EPRI 1008122, November 2004

/FAS 94/ W. Faßmann, J. Beraha, J. Brummer, M. Kerksen, H. Rührmann, H. Schmidtke, Nutzbarmachung neuer Informationstechnologien zur Verbesserung der Mensch-Maschine-Schnittstelle insbesondere in Kernkraftwerkswarten, GRS-A-2138, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Köln, Mai 1994

/GAB 20/ https://wirtschaftslexikon.gabler.de/definition/softwarewerkzeug-43682/version-267009; Gabler Wirtschaftslexikon, abgerufen am 12.02.2020

/GRS 21/ C. Müller, E. Piljugin, P. Gebhardt, J. Shvab, AnTeS Entwicklung und Anwendung des Analyse- und Testsystems der GRS, GRS-648, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Köln, März 2021

/HAR 10/ Hartung, J., E. Piljugin: Entwicklung eines methodischen Ansatzes zur Bewertung menschlicher Zuverlässigkeit beim Einsatz softwarebasierter Leittechnik, GRS A – 3548, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Köln, Mai 2010.

/HER 18/ Software-Ergonomie., Theorien, Modelle und Kriterien für gebrauchstaugliche interaktive Computersysteme, De Gruyter, 2018

/HUN 22/ Oliver Hunziker, 10 Usability Heuristiken nach Jakob Nielsen – Usability erklärt, 3. März 2021, xeit gmbg, https://blog.xeit.ch/2021/03/10-usability-heuristiken-nach-jakob-nielsen-usability-erklart/, abgerufen am 21.02.2022

/IAE 21/ International Atomic Agency, Human Factors Engineering Aspects of Instrumentation and Control System Design, IAEA-Guide NR-T-2.12 2021

/IEC 20/ DIN EN IEC 62646, Kernkraftwerke – Warten – Rechnergestützte Prozeduren, 2020

/INL 19/ R. Lew, R.L. Boring, T.A. Ulrich, Computerized Operator Support System for Nuclear Power Plant Hybrid Main Control Room, Proceedings of the Human Factors and Ergonomics Society 2019 Annual Meeting, 28 October -1 November 2019, Seattle, Washington, USA

/INL 16/ R.L. Boring, D. Gertman, P-203: Human Reliability Analysis (HRA) Training Course, March 2016

/ISO 90/ ISO 9241, Part 10 (1990): Ergonomic Dialogue Design Criteria, Version 3, Committee Draft, December 1990

/ION 22/ https://www.ionos.de/digitalguide/websites/web-entwicklung/human-centered-design/, abgerufen am 23.03.2022

/KOC 91/ Manfred Koch, Harald Reiterer, A Min Tjoa, Software-Ergonomie, Gestaltung von EDV-Systemen - Kriterien, Methoden und Werkzeuge, Springer Verlag, 1991

/KTA 09/ Kerntechnischer Ausschuss, KTA 1203, Anforderungen an das Notfallhandbuch, 2009

/KTA 15/ Kerntechnischer Ausschuss, KTA 1201, Anforderungen an das Betriebshandbuch, 2015

/KTA 17a/ Kerntechnischer Ausschuss, KTA 1202, Anforderungen an das Prüfhandbuch, 2017

/KTA 17b/ Kerntechnischer Ausschuss, KTA 3904, Warte, Notsteuerstelle und örtliche Leitstände in Kernkraftwerken, 2017

/MSG 22/ msg Applied Research msg systems ag „Heuristische Evaluation“, https://www.user-experience-methods.com/evaluation/heuristic-evaluation.html, abgerufen am 21.02.2022

/MUR 87/ B. Murchner, R. Oppermann, M. Paetau, M. Pieper, H. Simm, I. Stellmacher, EVADIS - Ein Leitfaden zur softwareergonomischen Evaluation von Dialogschnittstellen, In: Schönpflug, W. & Wittstock, M. (Hrsg.), Software-Ergonomie '87: Nützen Informationssysteme dem Benutzer?. Stuttgart: B. G.Teubner. (S. 307-316)

/NIE 94/ Jakob Nielsen “Ten Usability Heuristics”, Heuristic Evaluation, 1994

/NUR 02/ U.S. Nuclear Regulatory Commission: Human-System Interface Design Review Guidelines, NUREG-0700, Rev. 2, 2002

/OEC 07/ OECD – HRP Summer School on Design and Evaluation of Human System Interfaces, Halden, Norwegen, 27. – 30. August 2007

/OPP 92a/ Reinhard Oppermann, Bernd Murchner, Harald Reiterer, Manfred Koch, Software-ergonomische Evaluation, Der Leitfaden EVADIS II (Mensch-Computer-Kommunikation, Band 5) De Gruyter; 2. neubearb. Aufl. 1992.

/OPP 92b/ Reinhard Oppermann, Harald Reiterer: Der Evaluationsleitfaden EVADIS II Ergonomie und Informatik, Bd. 15, S. 25-29, 1992

/OPP 92c/ Reinhard Oppermann, Harald Reiterer: Evaluation von Benutzerschnittstellen, In Wirtschaftsinformatik, 34 (1992), 3. -S. 283-293, 1992

/PYT 22/ https://www.python.org

/PYP 22/ https://pypi.org/project/PyQt5/

/REA 90/ James Reason: Human Error, Cambridge University Press, 1990

/TEC 22/ https://techterms.com/definition/framework

/TRI 02/ Usability und Software-Ergonomie, Proseminar Technikpsychologie I, Michael Trimmel, WS 2001/2002

/VDI 02/ VDI 4006, Blatt 1: Menschliche Zuverlässigkeit: Ergonomische Forderungen und Methoden der Bewertung, Beuth Verlag GmbH, Berlin, 2002

Abbildungsverzeichnis

Tabellenverzeichnis

A Anhang

A.1 Ergebnisse der Bewertung der MMS des Wassertanksystems mit der MEDIC-Bewertungsmethode

Nachfolgend werden die MEDIC-Bewertungsergebnisse der MMS des Wassertanksystems sortiert nach den betrachteten Wechselwirkungen und den diesen Wechselwirkungen zugeordneten Attributen dargestellt. Die Beschreibung des Wassertanksystems und seiner MMS finden sich in Kapitel 3.4.2.2.

MMS → Mensch:

Physische Zugänglichkeit:

- ➔ Bei der Darstellung der Füllstände ist die Anzeige der Füllstände gut lesbar.
- ➔ Alle Steuerelemente sind gleichzeitig sichtbar.
- ➔ Die Bedienung beschränkt sich hier auf Aktionen mit einer Computermaus, diese sind alle gut durchführbar.

- ➔ Positiv ist, dass die „Knöpfe“ eine farbliche Rückmeldung geben, die die getätigte Aktion kennzeichnet und die getätigten Handlungen dem Benutzer damit zugänglich sind.

Abb. A 1.1 Pumpen- und Ventilsteuerung

- ➔ Die Animation der Füllstände in der Übersicht ist schwer lesbar (schlecht zugänglich). Die Füllstände sind im Verhältnis zu den Wertebereichen nicht abzuschätzen. Markierungen in den Darstellungen, sowie eine leichtere lesbare Darstellung, z. B. durch eine Einfärbung der Fläche unter der Füllstandhöhe wären hilfreich, um die Zugänglichkeit zu verbessern (siehe Abb. A 2).

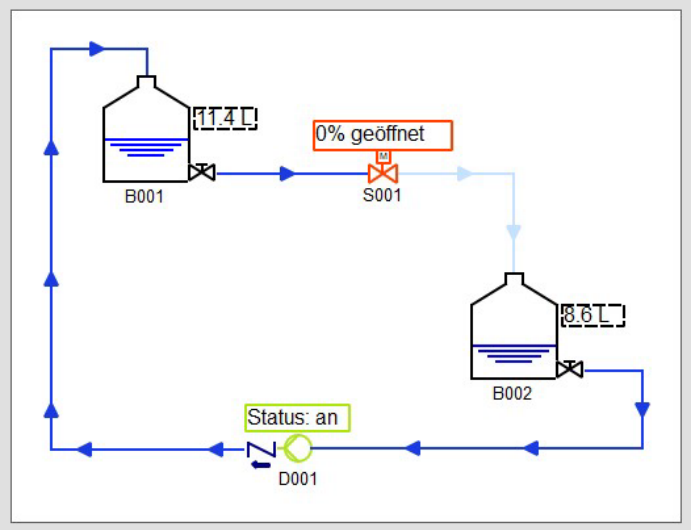

Abb. A 1.2 Verfahrenstechnische Darstellung des Wassertanksystems

➔ Ein Negativpunkt ist die Umsetzung des Hover-over-Tooltips in der Verfahrenstechnischen Darstellung. Das entsprechende Fenster ist so groß, dass es die verfahrenstechnische Darstellung überdecken kann und damit einen Abgleich zwischen dem Gelesenen und der Darstellung erschwert. Hier ist also die physische Zugänglichkeit nicht mehr gegeben, da die Darstellung des verfahrenstechnischen Prozesses des Systems für die Dauer der Einblendung des Tooltips nicht mehr sichtbar ist. Eine Veränderung des Systems in dieser Zeit würde der Mensch nicht merken. Dies ist in Abb. A 3 zu sehen, wo der Tooltip durch die Bewegung des Zeigers auf Behälter B001 (oben links) aufgerufen wurde, die Bezeichnung des Behälters, zusammen mit einem Großteil der verfahrenstechnischen Darstellung, aber nicht mehr zu sehen ist.

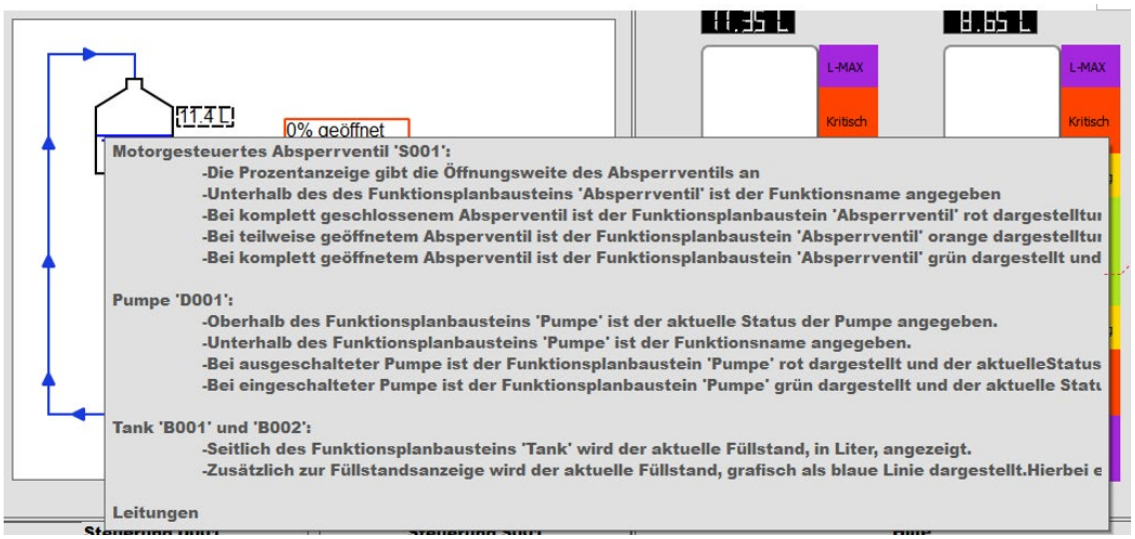

Abb. A 1.3 Hover-Over-Tooltip auf der MMS

Mentale Zugänglichkeit:

- ➔ Die MMS stellt keine besonderen Anforderungen, z. B. an das Gedächtnis des Benutzers durch das Verschwinden von Informationen oder Ähnliches.
- ➔ Die Erfüllung der „Korrespondenz“ fördert die mentale Zugänglichkeit des Systems beim Menschen.
- ➔ Zu erwähnen ist, dass der Warnton als Alarmsignal sehr penetrant und ablenkend ist, und ein konzentriertes Arbeiten erschwert und somit die mentale Zugänglichkeit zum System verschlechtert. Allerdings führt dieselbe Eigenschaft auch dazu, dass die Warnung selbst sehr gut wahrgenommen werden kann. Eventuell wäre die Möglichkeit, die Warnung temporär zu deaktivieren sinnvoll, um den kritischen Zustand des Systems nicht vergessen zu können und ein konzentriertes Arbeiten an der Normalisierung des Zustandes zu ermöglichen.

Unterlagen → Mensch

Physische Zugänglichkeit:

- ➔ Dass die Existenz von weiterführenden Hilfetexten neben der initialen Anzeige nicht zugänglich ist, ist ein Kritikpunkt. Hier ist, bis man zum Ende des initialen Textes scrollt, nicht ersichtlich, dass es noch weiterführende Erklärungen gibt.
- ➔ Auch beim Lesen der Texte ist immer nur ein Ausschnitt des Textes verfügbar.

Mentale Zugänglichkeit:

➔ Die physischen Einschränkungen in der Darstellung führen prinzipiell zu einer erhöhten Anforderung an das Gedächtnis des Benutzers, allerdings hält sich dieser Effekt durch die Einfachheit und den übersichtlichen Umfang der Anwendung in Grenzen.

System → Mensch

Physische Zugänglichkeit:

➔ In der Simulation des verfahrenstechnischen Prozesses wurde der physische Zugang zum System nicht berücksichtigt, da ein solcher für die Überwachungs- und Steuerungsaufgabe nicht erforderlich ist. Das Attribut wird deshalb nicht betrachtet bzw. nicht bewertet.

Mentale Zugänglichkeit:

➔ Das System ist in klar definierte Teilkomponenten aufgeteilt, deren Funktion verständlich ist.
➔ Die verfahrenstechnische Darstellung in der Bedienoberfläche erleichtert dem Menschen das Systemverständnis.

MMS ←→ MMS

Konsistenz:

➔ Die Elemente, mit denen die Pumpe und das Ventil dargestellt sind, entsprechen den üblichen Symbolen in verfahrenstechnischen Diagrammen. Damit sind sie konsistent mit den üblichen Konventionen.

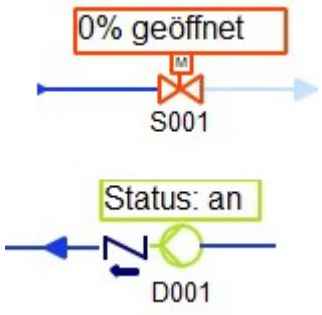

Abb. A 1.4 Darstellung der Elemente einer Pumpe und eines Ventils

➔ Farblich sind die Anzeigen im verfahrenstechnischen Diagramm nicht konsistent mit denen der Pumpensteuerung, dort wird eine angeschaltete Pumpe durch eine rote Leuchte angezeigt, während die Farbe „Rot“ im Diagramm eine ausgeschaltete Pumpe anzeigt.

Abb. A 1.5 Anzeigen einer eingeschalteten Pumpe auf der MMS

➔ Die Farben im Hover-Over-Tooltip der absoluten Füllstandsanzeige oben rechts sind invers zur weiteren Farbgebung.

Korrektheit:

➔ Es wurden keine inkorrekt implementierten Elemente gefunden.

Übersichtlichkeit:

➔ Durch die Darstellung des Hover-Over-Tooltips der verfahrenstechnischen Darstellung auf der MMS in einem einzigen Fenster ist es schwer, gezielt Informationen zu den einzelnen Elementen zu ermitteln.

Eindeutigkeit und Unterscheidbarkeit:

➔ Die Kennzeichnung der Pumpe und des Ventils (D001, S001) könnten durch prägnantere Namen unterscheidbarer gemacht werden. Da nur wenige Elemente vorhanden sind, ist eine Codierung der Kennzeichnungen nicht zwingend notwendig, um eine eindeutige Unterscheidung zu gewährleisten.

➔ Bei der Steuerung fällt auf, dass die Knöpfe zur Ventil- und Pumpensteuerung zwar unterschiedliche Funktionen haben (gedrückt Halten zum Öffnen/Schließen des Ventils, einmaliges Drücken zum Starten/Stoppen der Pumpe), optisch aber nicht voneinander getrennt sind. Dadurch ist die die Funktion nicht eindeutig durch die Darstellung der Knöpfe gekennzeichnet.

Abb. A 1.6 Pumpen- und Ventilsteuerung auf der MMS

➔ In der Darstellung der Füllstandsanzeige oben rechts sind die verschiedenen Zustände durch die Verwendung von Farben gut unterscheidbar.

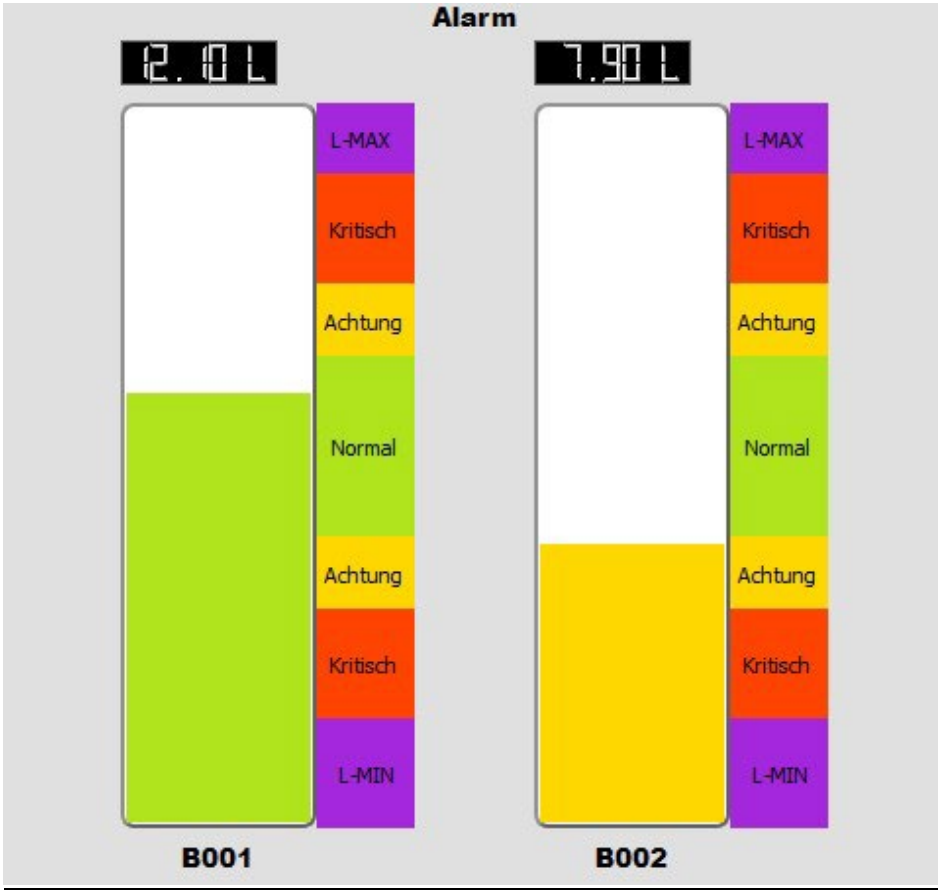

Abb. A 1.7 Darstellung der Behälterfüllstände auf der MMS

➔ Es werden dieselben Farben in dem verfahrenstechnischen Diagramm zur Anzeige von Pumpen- und Ventilstatus verwendet. Eine andere farbliche Darstellung eines der Elemente könnte hier zur Eindeutigkeit beitragen.

Vorhandensein:

➔ Positiv ist, dass die Knöpfe eine farbliche Rückmeldung geben, welche die getätigte Aktion kennzeichnet und damit die Rückmeldung zur Handlung vorhanden ist.

Unterlagen ←→ MMS

Konsistenz:

➔ Gut ist, dass in der Beschreibung der Steuerungsbausteine die gleichen Symbole wie in der verfahrenstechnischen Darstellung verwendet werden, was die Identifikation der Bausteine in der verfahrenstechnischen Darstellung erleichtert.

➔ In der Systembeschreibung werden neben den Bezeichnungen S001 und D001 von Pumpe und Ventil teilweise die Worte „Förderpumpe“ und „Absperrventil“ verwendet. Auf der MMS hingegen sind nur die Bezeichnungen S001 und D001 vorhanden.

Korrespondenz:

➔ Gut ist die farbliche Abhebung der Anweisungen von denen der normalen Hilfetexten. Hier korrespondiert die Farbgebung mit dem Alarmzustand (Abbildung A1.6).

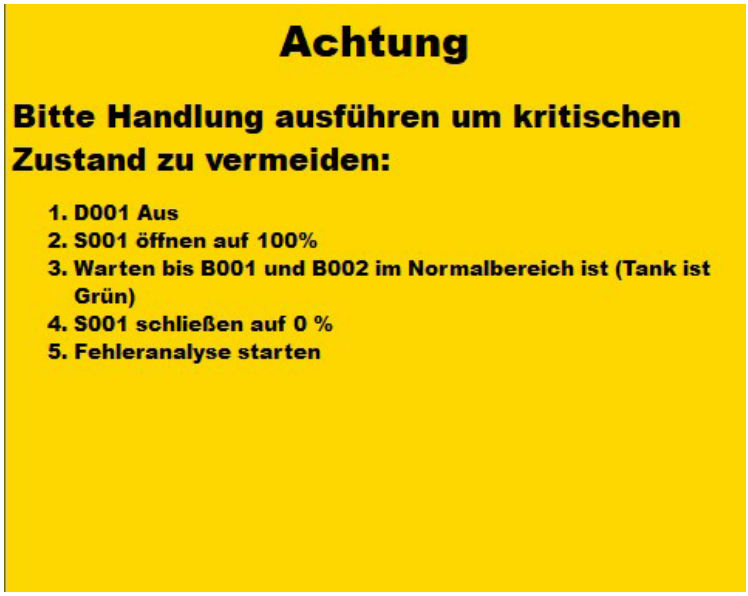

Abb. A 1.8 Handlungsanweisung bei Alarmzustand

Vollständigkeit:

➔ Die Anweisungen sind bei kritischen Systemzuständen nicht vollständig, da die Freigabe der Steuerung nicht in der Anweisung enthalten ist.

System←→MMS

Konsistenz:

➔ Dadurch, dass kein System als solches vorhanden ist, entfallen die entsprechenden Vergleiche.

Korrespondenz:

➔ Die Darstellungen der Behälter auf der MMS sind gut als solche zu erkennen. Die Anordnung der verfahrenstechnischen Darstellung spiegelt die Höhenverhältnisse im System wider.

➔ Positiv ist die Darstellung der Fließwege. Hier wird eine optische Rückmeldung gegeben, wenn in einem Abschnitt Wasser fließt, sowie die Flussrichtung angezeigt.

➔ Positiv ist auch, dass nicht nur die Steuerelemente, sondern auch der tatsächliche Zustand, insbesondere der Pumpe, angezeigt werden. Das ermöglicht die Erkennung einer Störung, ohne die Reaktion des Systems mit der Erwartung

bei der Steuerung abgleichen zu müssen (unter der Annahme, dass alle Störungen erkannt werden).

Vollständigkeit:

➔ Die MMS bietet die Möglichkeit, jeden Systemzustand darzustellen.

Unterlagen ←→ Unterlagen

Konsistenz:

➔ Innerhalb der Unterlagen werden teilweise inkonsistente Bezeichnungen verwendet (Behälter ←→ Tanks, Pumpe ←→Förderpumpe).

Korrektheit:

➔ Die Unterlagen beschreiben die Systemfunktion und die Steuerung in korrekter Weise.

Übersichtlichkeit:

➔ Die Texte könnten präziser formuliert werden, indem unnötige Teile weggelassen werden. Vor allem die Teile „gehen sie wie folgt vor“. Dazu würde auch beitragen, wenn Handlungsbeschreibungen im Hilfetext in imperativer Form vorliegen würden. Dies ist in der Handlungsanweisung bei kritischem Zustand besser gelöst, aber auch dort ließe sich der Text noch präziser ausführen (Streichen des „Bitte“ in „Bitte Handlung ausführen …“).
➔ Aufzählungen sind jeweils durch entsprechende Kennzeichnungen strukturiert.
➔ Die Absätze in der allgemeinen Systembeschreibung wirken teilweise etwas lang.

Eindeutigkeit:

➔ Aus den Beschreibungen und Anweisungen in den Unterlagen geht stets hervor, welche Elemente oder Tätigkeiten gemeint sind.

Vorhandensein:

➔ Die Erweiterung des reinen Textes um Hover-Over-Tooltips ist ein guter Weg, um Informationen korrespondierend mit der MMS darzustellen.

System ←→ System

Konsistenz:

➔ Es konnten keine Inkonsistenzen im Systemdesign gefunden werden.

Korrektheit:

➔ Das System bietet die Möglichkeit, die Füllstände der beiden Behälter zu kontrollieren.

Übersichtlichkeit:

➔ Das System besteht aus Komponenten mit klar definierten, voneinander abgegrenzten Funktionen.

Eindeutigkeit:

➔ Die Systemunktionen werden jeweils eindeutig durch bestimmte Komponenten übernommen.

Vorhandensein:

➔ Eine automatische Fehlererkennung der Pumpe liegt vor.

A.2 Ergebnisse der Bewertung der Arbeitsanweisung des Arbeitssystems „MMS-Schrank“ für den Austausch einer Prozessorbaugruppe mit anschließendem Hochladen der Software im Modul1 von AnTeS (Teleperm XS)

Nachfolgend sind die Ergebnisse der MEDIC-Bewertung der Arbeitsanweisung des Arbeitssystems „MMS-Schrank“ sortiert nach den betrachteten Wechselwirkungen und den diesen Wechselwirkungen zugeordneten Attributen dargestellt. Die Beschreibung des Arbeitssystems „MMS-Schrank“ ist in Kapitel 3.4.2.4 nachzulesen

Unterlagen ←→ Unterlagen

Konsistenz:

Das Attribut „Konsistenz“ ist erfüllt:

- ➔ Einheitliche Formatierung (Schriftart, Schriftgröße, Hervorhebungen der Tätigkeitsblöcke) in allen drei Unterlagen der Arbeitsanweisung.
- ➔ Einheitliche Bezeichnung der Abbildungen in allen drei Unterlagen der Arbeitsanweisung.
- ➔ Einheitliche Kennzeichnung der für die Durchführung der Aufgabe relevanten Informationen (Seriennummer, Position von Schaltern und Tastern etc..) in den Abbildungen.

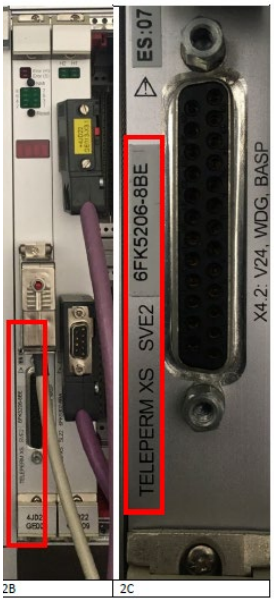

Abb. A 1.9 Auszug aus der detaillierten Arbeitsanweisung

Hier: Abbildung zur Lokalisierung der Seriennummer der Prozessorbaugruppe (rote rechteckige Umrandung).

Übersichtlichkeit:

Das Attribut „Übersichtlichkeit“ ist nur zum Teil erfüllt:

- ➔ Übersichtliche Darstellung der Anweisungen in den Unterlagen. Das Kriterium erfüllt durch die Checkliste zur Arbeitsanweisung. Erledigungsvermerke in der Checkliste fördern die Übersichtlichkeit.
- ➔ Eine sparsame Verwendung von Fließtexten wird empfohlen. Das Kriterium ist nicht erfüllt, da die Arbeitsanweisungen als Fließtext formuliert sind (siehe Abb. A 1.10).
- ➔ Hinweise und Erläuterungen zu den Anweisungen sollen von den Anweisungen unterschieden werden und als solche gekennzeichnet werden. Das Kriterium ist nicht erfüllt, da Hinweise und Erläuterungen in einem gemeinsamen Fließtext verfasst sind (siehe Abb. A 1.10).

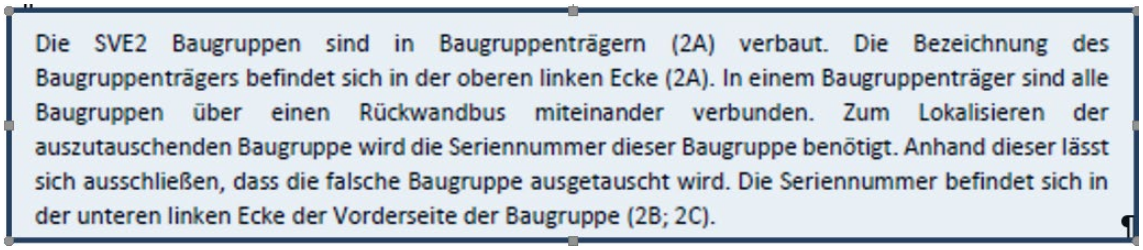

Abb. A 1.10 Auszug aus der detaillierten Arbeitsanweisung

➔ Verwendung von drei Unterlagen zur Durchführung der Aufgabe ist hinsichtlich der Übersichtlichkeit nicht fördernd. Zudem erschwert dies auch die physische Zugänglichkeit.

Eindeutigkeit

Das Attribut Eindeutigkeit trifft nicht zu:

➔ Unterschiedliche Bezeichnungen für die Baugruppenträger werden für identische Tätigkeitsblöcke in den Unterlagen verwendet. Es werden die Begriffe „Baugruppenträger“ und „Baugruppenracks“ verwendet.

Unterlagen → System

Korrespondenz

Das Attribut „Korrespondenz“ ist erfüllt:

➔ Die in den Unterlagen enthaltenen Abbildungen zur Erläuterung der jeweiligen Arbeitsschritte entsprechen den Gegebenheiten vor Ort im Leittechnikschrank und an den Baugruppen.

Unterlagen → MMS

Vollständigkeit

Das Attribut „Vollständigkeit“ ist nicht erfüllt:

➔ Zur Durchführung von einigen Arbeitsschritten sind Handwerkzeuge notwendig. Es sind keine Angaben oder Hinweise in den Unterlagen über die zu verwendenden Handwerkzeuge vorhanden.

➔ Zur Durchführung von Arbeitsschritten sind relevante Angaben notwendig wie z. B Aufstellort des Leittechnikschranks (Raumnummer), Öffnungsseite (vorne/hinten) sowie –richtung (links und rechts) des Leittechnikschranks. Diese Angaben fehlen.

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 978-3-949088-65-0