Entwicklung und Einsatz von Analysemethoden zur Beurteilung softwarebasierter leittechnischer Einrichtungen in deutschen Kernkraftwerken

GRS - 355

Gesellschaft für Anlagen-
und Reaktorsicherheit
(GRS) gGmbH

Entwicklung und Einsatz von Analysemethoden zur Beurteilung softwarebasierter leittechnischer Einrichtungen in deutschen Kernkraftwerken

Robert Arians
Simone Arnold
Stefanie Blum
Marcel Buchholz
André Lochthofen
Claudia Quester
Dagmar Sommer

März 2015

Anmerkung:

Das diesem Bericht zugrunde liegende FE-Vorhaben 3610R01361 wurde im Auftrag des Bundesministeriums für Umwelt, Naturschutz, Bau und Reaktorsicherheit (BMUB) durchgeführt.

Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Auftragnehmer.

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

GRS - 355
ISBN 978-3-944161-36-5

Deskriptoren

Ausfallmechanismen, Auswertung, Betriebserfahrung, digitale Leittechnik, Elektroleittechnik, Leittechniksysteme, Messumformer, programmierbare und rechenbasierte Komponenten, Sicherheitsleittechnik, Softwarefehler

Kurzfassung

Im vorliegenden Bericht werden die Ergebnisse und Daten der Auswertungen von Ereignissen unterhalb der Meldeschwelle programmierbarer oder rechnerbasierter leittechnischer Komponenten dargestellt. Da programmierbare oder rechnerbasierte Komponenten im Vergleich zu nicht programmierbaren oder rechnerbasierten Komponenten unterschiedliche Ausfallmechanismen sowie unterschiedliche Fehlerursachen aufweisen können, ist eine Auswertung der Betriebserfahrung notwendig, um zu untersuchen, ob die bisherigen Abläufe zur Bewertung der Zuverlässigkeit dieser Komponenten beibehalten werden können oder angepasst werden müssen. Es wurde die Betriebserfahrung unterhalb der Meldeschwelle ausgewertet, um Informationen über betriebliche Komponenten zu erhalten. Die Daten wurden von drei Doppelblockanlagen zur Verfügung gestellt, wodurch die Kernkraftwerkstypen Siedewasserreaktor der Baulinie 69, Siedewasserreaktor der Baulinie 72, Druckwasserreaktor der 2. Generation, Druckwasserreaktor der 3. Generation (Vor-Konvoi-Anlage) und Druckwasserreaktor der 4. Generation (Konvoi-Anlage) abgedeckt wurden. Der Betrachtungszeitraum, in dem die Betriebserfahrung ausgewertet wurde, beträgt für jede Anlage mindestens 8 Jahre. Darüber hinaus wurde der entsprechende Stand von Wissenschaft & Technik sowohl national als auch international dargestellt.

Abstract

In this report, results and data from examinations concerning software-based I&C components are evaluated. As failure modes of software-based components and failure causes differ fundamentally from non-software-based components, an evaluation of the operating experience of such components was carried out. This evaluation should show whether or not existing approaches for non-software-based components can be directly transferred to software-based components, or if a different approach has to be developed. The state of the art and science was gathered and is described for the national as well as the international situation. To include failures in non-safety systems, events not fulfilling the incident reporting criteria of German authorities were also included in this evaluation. The data provided by licensees of six German NPPs (different Boiling Water Reactors and Pressurized Water Reactors) was recorded for at least 8 years. The software-based components used in the NPPs are identified and their oper-

ating experience is analyzed in order to identify relevant failure modes and to establish a knowledge base for future failure rating.

Inhaltsverzeichnis

1 Einleitung

Die leittechnischen Komponenten in deutschen Kernkraftwerken sind seit vielen Jahren Gegenstand umfangreicher Modernisierungsmaßnahmen. Dies beruht zum einen auf der zunehmend erschwerten Ersatzteilbeschaffung bei den bisher eingesetzten konventionellen leittechnischen Komponenten, zum anderen aber auch auf der durch den Einsatz programmierbarer oder rechnerbasierter Komponenten realisierbaren Prozessoptimierung. In diesem Zusammenhang haben programmierbare oder rechnerbasierte leittechnische Komponenten eine wachsende Bedeutung gewonnen. So sind mittlerweile in nahezu allen deutschen Kernkraftwerken solche Komponenten eingesetzt. Aufgrund der sich verschlechternden Ersatzteilversorgung für konventionelle leittechnische Komponenten ist in den nächsten Jahren ein zunehmender Umfang an programmierbaren oder rechnerbasierten leittechnischen Komponenten sowohl in betrieblichen als auch in sicherheitstechnisch wichtigen Systemen zu erwarten. Da sich die programmierbare oder rechnerbasierte Technik – beispielsweise in ihrem Ausfallverhalten und in ihrer Struktur sowie der Mensch-Maschine-Schnittstelle – wesentlich von der konventionellen Technik unterscheidet, ist es erforderlich, die entsprechenden Komponenten insbesondere hinsichtlich ihres Ausfallsverhaltens näher zu untersuchen. Diese Untersuchung kann unter Umständen als Grundlage für eine Bewertung der Zuverlässigkeit dieser programmierbaren oder rechnerbasierten Komponenten herangezogen werden.

Für die Untersuchung des Ausfallsverhaltens wurden im Rahmen des hier beschriebenen Vorhabens für sechs deutsche, kerntechnische Anlagen ermittelt, welche programmierbaren oder rechnerbasierten leittechnischen Komponenten in welchem Umfang eingesetzt sind. Bezüglich dieser Komponenten wurden insbesondere Wartungs- und Instandhaltungsvorgänge über einen längeren Betrachtungszeitraum ausgewertet. Hiermit wurden u. a. Erkenntnisse über Ausfallverhalten und Ausfallhäufigkeiten der erfassten leittechnischen Komponenten ermittelt.

Für die Untersuchung hat die GRS Daten herangezogen, die ihr von folgenden kerntechnischen Anlagen zur Verfügung gestellt wurden:

- Siedewasserreaktor (SWR) der Baulinie 69
- Siedewasserreaktor (SWR) der Baulinie 72
- Druckwasserreaktor (DWR) der 2. Generation

- Druckwasserreaktor (DWR) der 3. Generation (Vor-Konvoi-Anlage)
- Druckwasserreaktor (DWR) der 4. Generation (Konvoi-Anlage)

Eine detaillierte Aufarbeitung und Dokumentation des für das Vorhaben relevanten Standes von Wissenschaft und Technik erfolgt in Kapitel 2. Dabei wird in Abschnitt 2.1 zunächst auf die in nationalen und internationalen Regelwerken enthaltenen Anforderungen an die Auslegung von rechnerbasierten oder programmierbaren leittechnischen Systemen in der Sicherheitsleittechnik eingegangen. In Abschnitt 2.2 werden der GRS bekannte Umrüstungsmaßnahmen auf programmierbare oder rechnerbasierte leittechnische Komponenten in deutschen und internationalen Kernkraftwerken beschrieben. Neben geplanten und bereits abgeschlossenen Umrüstungsmaßnahmen wird hierbei auch auf Neubauprojekte von Kernkraftwerken mit programmierbaren oder rechnerbasierten leittechnischen Komponenten eingegangen. In Abschnitt 2.3 werden die dabei verwendeten programmierbaren oder rechnerbasierten Leittechniksysteme beschrieben.

In Kapitel 3 wird die Vorgehensweise beschrieben, wie die in den sechs ausgewählten kerntechnischen Anlagen eingesetzten programmierbaren oder rechnerbasierten leittechnischen Komponenten und die zugehörigen Ereignisse ermittelt wurden. Es wird darauf eingegangen, wie für jede der sechs Anlagen die Wartungs- und Instandhaltungsvorgänge sowie Ereignisse unterhalb der Meldeschwelle, die an diesen programmierbaren oder rechnerbasierten leittechnischen Komponenten aufgetreten sind, für die hier durchgeführten Auswertungen verarbeitet werden. Unterhalb der Meldeschwelle bedeutet in diesem Fall, dass die Ereignisse nach der Atomrechtlichen Sicherheitsbeauftragten- und Meldeverordnung (AtSMV) nicht meldepflichtig sind.

Eine Auswertung der erfassten und aufgearbeiteten Daten erfolgt in Kapitel 4. Für die eingesetzten programmierbaren oder rechnerbasierten betrieblichen und sicherheitstechnisch wichtigen leittechnischen Komponenten, werden über den jeweiligen Betrachtungszeitraum die Wartungs- und Instandhaltungsvorgänge sowie die Ereignisse unterhalb der Meldeschwelle hinsichtlich unterschiedlicher Kriterien ausgewertet. Zudem wird ein Vergleich mit den im Bericht „Analyse zum Einsatz und Betrieb elektrotechnischer Einrichtungen“ /GRS 15/ erfassten Daten vorgenommen.

In Kapitel 5 werden die Erkenntnisse aus Kapitel 4 genutzt, um eine vertiefte Analyse der Daten durchzuführen. Hierbei wird insbesondere auf die spezifischen Fragestellun-

gen eingegangen werden, die sich im Rahmen der Bearbeitung von Kapitel 1 ergeben haben. Des Weiteren werden auffällige Ereignisse gesondert betrachtet und vertieft ausgewertet.

Eine Zusammenfassung der erzielten Ergebnisse und ein daraus resultierendes Fazit werden in Kapitel 6 gegeben.

2 Stand von Wissenschaft und Technik

Der für dieses Vorhaben relevante Stand von Wissenschaft und Technik enthält einerseits eine Zusammenstellung der in nationalen und internationalen Regelwerken enthaltenen Anforderungen an das Design von programmierbaren und rechnerbasierten leittechnischen Systemen in der Sicherheitsleittechnik (siehe Abschnitt 2.1). Andererseits werden Umrüstungsmaßnahmen auf programmierbare oder rechnerbasierte leittechnische Komponenten in deutschen und internationalen Kernkraftwerken beschrieben, wobei neben geplanten und bereits abgeschlossenen Umrüstungsmaßnahmen auch auf Neubauprojekte von Kernkraftwerken mit programmierbaren oder rechnerbasierten leittechnischen Komponenten eingegangen wird (siehe Abschnitt 2.2). Die dabei eingesetzten programmierbaren oder rechnerbasierten Leittechniksysteme werden anschließend näher beschrieben (siehe Abschnitt 2.3).

2.1 Internationale und nationale Anforderungen an die Auslegung von programmierbaren und rechnerbasierten Leittechniksystemen in der Sicherheitsleittechnik

Die Wahrscheinlichkeit, dass gemeinsam verursachte Fehler in programmierbaren und rechnerbasierten Leittechniksystemen auftreten, ist momentan ebenso wie Maßnahmen zur Beherrschung eines auftretenden CCF sowohl national als auch international in Diskussion. Im Folgenden werden die Anforderungen verschiedener Behörden und TSOs bezüglich Vorbeugung und Beherrschung eines CCF in der Sicherheitsleittechnik von Kernkraftwerken dargestellt.

2.1.1 IAEA

In der Sicherheitsrichtlinie NS-G-1.3 der Internationalen Atomenergie-Organisation IAEA mit dem Titel „Instrumentation and Control Systems Important to Safety in Nuclear Power Plants“ /IAE 02/ werden Anforderungen an die Auslegung von leittechnischen Systemen gestellt. Es werden folgende Aussagen gemacht:

- Designmerkmale wie Fehlertoleranz sowohl gegen Zufallsfehler als auch gegen gemeinsam verursachte Fehler, fehlersicheres Design, Unabhängigkeit von Systemen, Nutzung von qualitativ hochwertigem Equipment, Testbarkeit und Wartbarkeit sollten in geeigneter Weise berücksichtigt werden.

- Diversität bietet Schutz gegen gemeinsam verursachte Fehler, ergänzt das Defence-in-depth-Prinzip und erhöht die Wahrscheinlichkeit, dass sicherheitstechnisch wichtige Aufgaben bei deren Anforderung ausgeführt werden.
  Genannte Arten von Diversität sind menschliche Diversität, Design Diversität, Software Diversität, funktionale Diversität, Signal Diversität, Diversität der Ausrüstung und System Diversität.

- Wenn der notwendige Nachweis der Zuverlässigkeit des Systems nicht erbracht werden kann, sollte zusätzlicher Konservatismus zur Anwendung kommen. Dies kann zum Beispiel der Fall sein, wenn die Zuverlässigkeit eines mehrfach redundanten Systems durch Faktoren wie gemeinsam verursachte Fehler oder Unsicherheiten im Design limitiert wird. Beim Nachweis der Zuverlässigkeit eines rechnerbasierten Systems können beispielsweise besondere Probleme auftreten. Die Nutzung von Diversität ist eine Möglichkeit Konservatismus anzuwenden, um die Schwierigkeiten beim Nachweis des notwendigen Grades der Zuverlässigkeit zu kompensieren.

Bezüglich eines CCF in programmierbaren und rechnerbasierten leittechnischen Systemen werden in dem technischen Bericht „Protection against Common Cause Failures in Digital I&C Systems of Nuclear Power Plants“ /IAE 09/ der IAEA weitere Anforderungen gegeben. Folgende Maßnahmen bezüglich des Designs von leittechnischen Systemen zur Verhinderung eines CCF sind in diesem Bericht genannt:

- Minimierung von Fehlern im Aufbau, in Systemen und in Komponenten
- Vermeidung von systematischen Fehlern
- Vermeidung von gleichzeitiger Aktivierung
- Vermeidung der Ausbreitung von Fehlern
- Vermeidung gemeinsam verwendeter Teilsysteme
- Fehlertoleranz

Die Minimierung von Fehlern erfolgt durch die Vermeidung von Fehlern während der Planung und Entwicklung und der Fehlererkennung und Fehlerentfernung während der Verifizierung und Validierung im Entwicklungsprozess. Bezüglich der Vermeidung systematischer Fehler sind in /IAE 09/ folgende Aussagen getroffen worden:

- Trotz der getroffenen Maßnahmen zur Beseitigung von Fehlern in leittechnischen Systemen wird unterstellt, dass einige Fehler nicht entdeckt werden und verbleiben. Für angeblich voneinander unabhängige Systeme ist es entscheidend sicherzustellen, dass systematische Fehler nicht existieren oder nicht zur gleichen Zeit in allen Systemen ausgelöst werden. Diversität ist das bevorzugte Mittel, mit dem dies erreicht wird.

In /IAE 09/ werden menschliche Diversität, funktionale Diversität und Design-Diversität als Diversitätsmerkmale genannt.

- Unter menschlicher Diversität wird die Beschäftigung mehrerer Personen mit unterschiedlichen Ausbildungen, Erfahrungen usw. verstanden, die alle an der Lösung eines Problems arbeiten.

- Unter funktionaler Diversität wird die Nutzung zweier Systeme verstanden, die nach unterschiedlichen physikalischen Prinzipien arbeiten und einen überlappenden Sicherheitseffekt haben.

- Unter Design Diversität versteht man den Gebrauch verschiedener Lösungsansätze zur Lösung des gleichen Problems. Das Grundprinzip der Design Diversität ist dabei die Annahme, dass die erhaltenen unterschiedlichen, voneinander unabhängigen Lösungen des Problems verschiedene Fehler und verschiedene Fehlermöglichkeiten haben. Dadurch wird die Wahrscheinlichkeit für einen systematisch verursachten Fehler reduziert.

Zusammenfassend wird in den Unterlagen der IAEA ausgesagt, dass eine einzelne Art von Diversität hilfreich ist, aber üblicherweise die Vermeidung systematischer Fehler nicht garantiert. Der Gebrauch mehrerer Arten von Diversität könnte laut Aussage der IAEA die wichtigste Vorgehensweise sein, mit dieser Einschränkung umzugehen.

2.1.2 U.S. NRC

Im Standard Review Plan (SRP) der Nuclear Regulatory Commission der USA werden in Kapitel 7 Richtlinien zur Bewertung von leittechnischen Systemen in Kernkraftwerken gegeben. In Kapitel 7.8 /NUR 07/ werden der Bewertungsprozess und die Nachweiskriterien für diversitäre Leittechniksysteme, die zum Schutz gegen potenzielle CCF in Sicherheitssystemen vorgesehen sind, beschrieben. Folgende Aussagen wurden gemacht:

- Falls ein unterstellter systematischer Fehler eine Sicherheitsfunktion blockieren kann, sollte ein diversitäres Mittel verwendet werden, welches entweder die gleiche Funktion [wie das für den systematischen Fehler anfällige Sicherheitssystems] oder eine andere Funktion [welche einen angemessenen Schutz liefert] ausführt. Dabei muss nachgewiesen werden, dass es unwahrscheinlich ist, dass das diversitäre Mittel von dem gleichen systematischen Fehler [wie das Sicherheitssystem] betroffen sein kann. Die diversitäre Funktion kann von einem nichtsicherheitstechnischem System ausgeführt werden, falls dieses System eine ausreichende Güte hat, um die notwendigen Funktionen unter den bei dem Ereignis auftretenden Bedingungen auszuführen.

Im Regulatory Guide 1.152 /NRC 11/ mit dem Titel „Criteria for use of Computers in Safety Systems of Nuclear Power Plants“ werden folgende Aussagen getroffen:

- Mit der Einführung digitaler Systeme in die Sicherheitssysteme von Kraftwerken sind Bedenken bezüglich der Möglichkeit aufgekommen, dass ein Fehler im Design der Software in redundanten Systemen des Sicherheitssystems zu einem systematischen Fehler in der Funktion des Sicherheitssystems führen kann. Es können Bedingungen vorhanden sein, bei denen eine Form von Diversität notwendig sein kann, um eine zusätzliche Sicherheit zu schaffen, welche über die durch die Qualitätssicherungsprozesse inklusive der Qualitätssicherung der Software erreichte Sicherheit hinausgeht. Dabei können funktionale Diversität, Design-Diversität, Diversität im Betrieb und Diversität innerhalb der vier Stufen des Defence-in-depth-Prinzips (Reaktorschutz, ESFAS, Steuerung und Überwachung des Leittechniksystems) als Vorsorge gegen systematische Fehler eingesetzt werden. Manuelle Betätigungen von Sicherheits- und Nichtsicherheitssystemen sind dabei akzeptabel, sofern die notwendigen diversitären Bedienelemente und Anzeigen die benötigte Funktion unter den bei dem Ereignis auftretenden Bedingungen innerhalb einer akzeptablen Zeit ausführen können.

- Die NRC unterstützt das Konzept quantitativer Zuverlässigkeitsziele als einzige Möglichkeit zur Einhaltung der Regelungen bezüglich der Zuverlässigkeit digitaler, rechnerbasierter Systeme in Sicherheitssystemen nicht. Die Anerkennung der Zuverlässigkeit von rechnerbasierten Systemen durch die NRC basiert auf deterministischen Kriterien für sowohl Hardware als auch Software. Eine quantitative Bestimmung der Zuverlässigkeit, bei der eine Kombination aus Analyse, Test und Be-

triebserfahrung verwendet wird, kann ein zusätzliches Vertrauensniveau für die zuverlässige Funktion von rechnerbasierten Systemen bieten.

In der Branch Technical Position (BTP) 7-19 /NRC 12/ der U.S. NRC mit dem Titel „Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems" sind weitere Richtlinien dargestellt:

- Es gibt zwei Designmerkmale die ausreichen, um eine Berücksichtigung von softwarebasierten oder softwarelogikbasierten systematischen Fehlern auszuschließen:
  - Diversität – Falls eine ausreichende Diversität in einem Sicherheitssystem vorhanden ist, kann das Potenzial für einen CCF mehrerer Stränge ohne weitere Maßnahmen als angemessen behandelt betrachtet werden.
    Beispiel: Ein Reaktorschutzsystem-Design mit vier Kanälen für jede Sicherheitsfunktion, wobei zwei Kanäle in einem digitalen Leittechniksystem und zwei Kanäle in einem dazu diversitären digitalen Leittechniksystem verarbeitet implementiert sind. Falls eine Analyse der beiden Leittechniksysteme gemäß den Richtlinien im NUREG/CR-6303 /NUR 94/ durchgeführt wurde, durch welche gezeigt wurde dass die beiden Leittechniksysteme keinem gemeinsam verursachten Fehler unterliegen können, ist in dem Sicherheitssystem keine weitere Form von Diversität mehr notwendig.
  - Testbarkeit – Ein System ist hinreichend einfach, so dass jede mögliche Kombination von Eingangssignalen und jede mögliche Sequenz von Gerätezuständen sowie alle Ausgangssignale für jeden Fall nachgewiesen werden können (100 % getestet).

Zusammenfassend lässt sich feststellen, dass für die U.S. NRC das alleinige Erreichen quantitativer Zuverlässigkeitsziele für digitale Leittechniksysteme, welche in sicherheitstechnisch wichtigen Systemen in Kernkraftwerken eingesetzt werden, nicht ausreicht, sondern dass auch deterministische Kriterien für Hardware und Software gefordert werden. Um die Möglichkeit eines CCF in rechnerbasierten oder programmierbaren Systemen nicht mehr berücksichtigen zu müssen, müssen die Systeme laut U.S. NRC eine ausreichende Diversität und Testbarkeit aufweisen. Bezüglich der Frage ob ein System eine ausreichende Diversität aufweist, fordert die U.S. NRC eine Analyse nach den Richtlinien des NUREG/CR-6303.

2.1.3 HSE (UK)

In dem Dokument „Generic Design Assessment – New Civil Reactor Build; Step 4, Control and Instrumentation Assessment of the EDF and AREVA UK EPR™ Reactor" /HSE 11/, des zur Health and Safety Executive (HSE) gehörigen Office for Nuclear Regulation (ONR) werden folgende Aussagen getroffen:

- Der Gebrauch verschiedener Arten von Diversität innerhalb eines Systems, welches sicherheitstechnisch wichtige Aufgaben ausführt, ist von wesentlicher Bedeutung, um das Risiko eines gemeinsam verursachten Fehlers in diesem System zu minimieren.
- Die Begutachtung der Diversität in Systemen, die Reaktorschutzfunktionen ausführen, wurde beendet. Die in dieser Begutachtung untersuchten Systeme waren das „Protection System (PS)" (Plattform: TXS) und das „Safety Automation System/Process Automation System (SAS/PAS)" (Plattform: Siemens SPPA-T2000). Die Begutachtung beinhaltete die Berücksichtigung verschiedener Arten von Diversität:
  - Diversität der Ausrüstung (inklusive Diversität der Plattform)
  - Diversität von Verifizierung und Validierung
  - Diversität des physischen Standortes (Trennung)
  - Software Diversität
  - Funktionale/Daten/Signal Diversität
  - Diversität von Design/Entwicklung
  - Diversität der Spezifikation

2.1.4 STUK (Finnland)

In der Präsentation der finnischen Atomaufsichtsbehörde STUK mit dem Titel „Safety and regulation of nuclear power plants – regulatory project management for a new build" /STU 12/ werden folgende Aussagen gemacht:

- Es ist nicht möglich, die Fehlerfreiheit eines software-basierten Systems durch Test oder Analyse zu zeigen, da software-basierte Systeme und Ausrüstung normalerweise zu kompliziert sind
- Die Möglichkeit, dass ein CCF mehrfach redundante, parallele Systeme beeinflusst, kann nicht durch den Einsatz von software-basierten Systemen ausgeschlossen werden.
  - Die Beschaffenheit von software-basierten Systemen macht das Auftreten eines CCF wahrscheinlicher, als es bei nicht-programmierbarer Technologie der Fall wäre
  - Die Reduzierung der Wahrscheinlichkeit des Auftretens eines CCF ist schwierig, da diese normalerweise latent vorhanden sind
  - CCFs werden durch auslösende Ereignisse aktiviert, welche normalerweise so komplex sind, das die Fehler in der Test- und Verifizierungsphase nur sehr schwer aufzufinden sind
    - Man muss eine hinreichende Diversität von Hardware und Software sicherstellen
    - Man muss eine hinreichende Trennung zwischen Systemen und redundanten Kanälen sicherstellen

2.1.5 Europa

In dem Bericht „Licensing of safety critical software for nuclear regulators – Common position of seven European nuclear regulators and authorised technical support organisations“ /ENR 10/, der von BEL V (Belgien), BfS (Deutschland), CSN (Spanien), ISTec (Deutschland), NII (Vereinigtes Königreich), SSM (Schweden) und STUK (Finnland) verfasst wurde, wird folgende Meinung der beteiligten Organisationen bezüglich der Diversität des Software Designs wiedergegeben:

- Um eine hohe Zuverlässigkeit zu erreichen, werden typischerweise redundante Systeme und Komponenten genutzt. Während Redundanz mit identischen Systemen und Komponenten einen effektiven Schutz gegen Zufallsausfälle von Hardware bietet, geht die Möglichkeit eines CCF aus systematischen Fehlern hervor, die beispielsweise in der Spezifikation, im Design, in der Implementierung und Feh-

lern in der Wartung liegen können. Die Einführung von Diversität kann einen Schutz gegen gemeinsam verursachte Ausfälle bieten.

- Eine Vorgehensweise, die typischerweise während des Architekturdesigns zum Schutz gegen die Möglichkeit eines CCF angewendet wird, ist den Gebrauch von multiplen, möglicherweise diversitären, Systemen in Betracht zu ziehen. Auch die Erwägung des Einsatzes von defence-in-depth, so dass ein Fehler in einer Ebene durch die übergreifende Systemarchitektur kompensiert wird, kann zur Notwendigkeit des Einsatzes von diversitären, möglicherweise softwarebasierten, Systemen führen.

- Die Anzahl der benötigten Systeme, Komponenten oder Kanäle, der Grad an Diversität zwischen ihnen, die vorgesehenen Zuverlässigkeitsziele und die Auswahl der Technologie der benötigten Systeme, Komponenten oder Kanäle muss bestimmt werden. Eine Vorgehensweise, die für 1v2-Systeme von denen eines ein rechnerbasiertes System ist genutzt werden kann, ist ein einfaches nichtrechnerbasiertes System als zweites System einzusetzen. Wenn mehrere rechnerbasierte Systeme, Kanäle oder Komponenten eingesetzt werden, muss der Einsatz von Software Diversität in Betracht gezogen werden.

2.1.6 Deutschland

In den „Sicherheitsanforderungen an Kernkraftwerke“ /BMU 12/, die vom Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit veröffentlicht wurden, werden folgende Aussagen getroffen:

- Redundante Sicherheitseinrichtungen, bei denen Möglichkeiten für Ausfälle infolge gemeinsamer Ursache identifiziert sind, sind dazu, soweit technisch sinnvoll, diversitär auszuführen.

- Das Kernkraftwerk ist mit zuverlässigen leittechnischen Einrichtungen mit Leittechnik-Funktionen auf der Sicherheitsebene 3, dem Reaktorschutzsystem, auszurüsten, deren Leittechnik-Funktionen bei Erreichen festgelegter Ansprechwerte Schutzaktionen auslösen. Diese Einrichtungen sind nach folgenden Grundsätzen auszulegen:

  - Redundante Auslegung von Komponenten, Baugruppen und Teilsystemen
  - Diversität

- Räumlich getrennte Installation entsprechend dem Wirkungsbereich möglicher versagensauslösender Ereignisse
- Selbsttätige Überwachung auf einen Ausfall hin
- Anpassung der Komponenten an die möglichen Umgebungsbedingungen
- Einfache Struktur der Software
- Begrenzung des Funktionsumfangs von Hard- und Software auf das sicherheitstechnisch notwendige Maß
- Einsatz fehlervermeidender, fehlerentdeckender und fehlerbeherrschender Maßnahmen und Einrichtungen

- Es sind Vorkehrungen gegen systematisches Versagen zur Minderung von dessen Eintrittswahrscheinlichkeit derart zu treffen, dass es auf der Sicherheitsebene 3 nicht mehr unterstellt werden muss.

In den Interpretationen zu den Sicherheitsanforderungen an Kernkraftwerke /BMU 13/ werden folgende Aussagen getroffen:

- Bei der Auslegung der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind Vorkehrungen gegen systematische Ausfälle der leittechnischen Einrichtungen zur Minderung der Eintrittswahrscheinlichkeit derart zu treffen, dass ein systematischer Ausfall auf der Sicherheitsebene 3 nicht mehr unterstellt werden muss. Kann für rechnerbasierte oder programmierbare leittechnische Einrichtungen diese Nachweisführung nach dem Stand von Wissenschaft und Technik nicht erfolgen, sind Vorkehrungen derart zu treffen, dass ein systematischer Ausfall von Hardware und Software auf der Sicherheitsebene 3 beherrscht wird.

- Beim Einsatz rechnerbasierter oder programmierbarer Leittechnik sind grundsätzlich diversitäre leittechnische Einrichtungen unter Beachtung der folgenden Bedingungen zu verwenden. Es bestehen keine Vorgaben hinsichtlich des Einsatzes diversitärer Einrichtungen, wenn für die jeweils auszuführende Leittechnik-Funktion ein aktiver systematischer Ausfall sicherheitsgerichtet ist. Beim Einsatz von rechnerbasierter oder programmierbarer Leittechnik ist für Schutzaktionen, die nicht für jeden Anlagenzustand sicherheitsgerichtet sind, in Abhängigkeit von den Auswirkungen von passiven oder aktiven systematischen Ausfällen in den leittechnischen

Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, eine zweifache oder dreifache diversitäre Ausführung der software-basierten Leittechnik einzusetzen. Eine mindestens zweifache diversitäre Ausführung ist einzusetzen,

- wenn mit den noch verfügbaren Sicherheitseinrichtungen der Störfall beherrscht wird oder
- wenn jede der beiden diversitären leittechnischen Einrichtungen für sich alleine die erforderliche Schutzaktion auslöst.

Trifft beim Einsatz von rechnerbasierter oder programmierbarer Leittechnik eine der beiden genannten Voraussetzungen für den Einsatz einer zweifach diversitären Ausführung nicht zu, ist eine dreifach diversitär ausgeführte Leittechnik einzusetzen.

Der VdTÜV hat eine „Stellungnahme zu den erforderlichen Vorsorgemaßnahmen gegen systematisches Versagen von digitalen leittechnischen Einrichtungen in kerntechnischen Anlagen, die Leittechnikfunktionen der Kategorie 1 ausführen“ /VdT 08/ abgegeben. In dieser werden folgende Aussagen getroffen:

- Die grundsätzlich zu treffenden Vorsorgemaßnahmen umfassen nach dem Stand von Wissenschaft und Technik sowohl das gesamte Spektrum der fehlervermeidenden Maßnahmen als auch der fehlerbeherrschenden Maßnahmen.
- Es werden ausschließlich die fehlerbeherrschenden Maßnahmen im Hinblick auf eine dissimilare leittechnische Auslegung von redundanten Kanälen oder Strängen oder Teilsystemen behandelt. Unter dissimilarer Technik wird hier eine in der Summe hinreichend unähnliche bzw. unterschiedliche Hardware, Software, Entwicklungswerkzeuge, Entwicklungsteams, Fertigung, Test und Instandhaltung verstanden, so dass das systematische Versagen von zueinander dissimilaren Einrichtungen hinreichend unwahrscheinlich ist.
- Für Ereignisabläufe, die ausschließlich eindeutig sicherheitsgerichtete Schutzaktionen beinhalten, ist eine zweifache dissimilare Auslegung der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie 1 ausführen, dann erforderlich, wenn ein Störfall oder ein Ereignis bei passivem systematischem Versagen nicht in Sicherheitsebene 3 beherrscht wird.
- Für Ereignisabläufe, die nicht für jeden Anlagenzustand sicherheitsgerichtete Aktionen beinhalten, ist in den leittechnischen Einrichtungen, die Leittechnik-

Funktionen der Kategorie 1 ausführen, eine zweifache oder dreifache dissimilare Auslegung vorzusehen.

2.1.7 Fazit

Bezüglich der internationalen und nationalen Anforderungen an das Design von rechnerbasierten oder programmierbaren Leittechniksystemen, welche in Sicherheitssystemen genutzt werden, lässt sich feststellen, dass die Forderung von Diversität für rechnerbasierte oder programmierbare Systeme von allen hier dargestellten Behörden und TSOs in unterschiedlicher Deutlichkeit als Schutz gegen gemeinsam verursachte Fehler gesehen wird. Vor allem die U.S. NRC, die STUK, der VdTÜV und die Interpretationen zu den Sicherheitsanforderungen an Kernkraftwerke /BMU 13/ fordern Diversität für rechnerbasierte oder programmierbare leittechnische Systeme. Dabei wird eine wirksame Diversität gefordert, welche meist nicht nur durch das Vorhandensein eines Diversitätsmerkmals, sondern durch das Zusammenwirken mehrerer Arten von Diversität, erzielt wird. Eine weitere Untersuchung der Diversitätsmerkmale von leittechnischen Systemen ist erforderlich, um zu zeigen, ob die Diversität einen wirksamen Schutz gegen gemeinsam verursachte Fehler liefert.

2.2 Nationaler und internationaler Stand der Umrüstungsmaßnahmen

In Kernkraftwerken unterscheidet man bei den leittechnischen Einrichtungen zwischen betrieblicher Leittechnik (Leittechnik der Kategorie C sowie nicht kategorisierte leittechnische Einrichtungen /DIN 10/) und Sicherheitsleittechnik (Leittechnik der Kategorien A und B /DIN 10/). Dabei bezeichnet Sicherheitsleittechnik die leittechnischen Einrichtungen des Sicherheitssystems und der anderen Systeme mit sicherheitstechnischer Bedeutung /RSK 97/.

Bei der Modernisierung von Kernkraftwerken im Ausland wird bereits programmierbare oder rechnerbasierte Leittechnik für Einrichtungen bis zur Kategorie A eingesetzt. Neue Reaktoranlagen im Ausland wurden in den letzten Jahren mit programmierbarer oder rechnerbasierter Leittechnik für praktisch alle Automatisierungsaufgaben ausgelegt und errichtet.

In deutschen Kernkraftwerken hingegen kommt programmierbare oder rechnerbasierte Leittechnik bisher in betrieblichen Systemen sowie in der Sicherheitsleittechnik der Kategorie B zum Einsatz, z. B.

- Prozessrechner zur Beurteilung des Betriebszustandes und zur Aufzeichnung der Prozessparameter,
- Regelungs- und Begrenzungseinrichtungen für die Durchführung des bestimmungsgemäßen Betriebes der Anlage,
- digitale Messeinrichtungen,
- Steuerung der Brennelementlademaschine sowie
- Steuer- und Schutzsysteme der Turbine.

Aufgrund des Beschlusses zur Beendigung der Nutzung der Kernenergie und der bereits stattgefundenen Abschaltung einiger Anlagen, die zuvor Umrüstungspläne verfolgten (wie beispielsweise das Kernkraftwerk Unterweser (KKU)), liegen in Deutschland derzeit keine Anträge zur Umrüstung der Sicherheitsleittechnik auf programmierbare oder rechnerbasierte Systeme mehr vor. Es gibt allerdings Anlagen, in denen bereits Teile der Sicherheitsleittechnik (nicht Reaktorschutz) auf programmierbare oder rechnerbasierte Systeme umgerüstet wurden (siehe Abschnitt 2.2.1).

In ausländischen Anlagen, auch grenznahen Anlagen wie z. B. das Kernkraftwerk Gösgen, finden derartige Umrüstungen weiterhin statt, beziehungsweise sind geplant.

Im Folgenden wird zunächst auf die Umrüstungsmaßnahmen der betrieblichen Leittechnik sowie Sicherheitsleittechnik in deutschen Kernkraftwerken eingegangen (siehe Abschnitt 2.2.1). Danach wird eine Übersicht über den internationalen Stand bereits durchgeführter (siehe Abschnitt 2.2.3) und derzeit geplanter Umrüstungsmaßnahmen (siehe Abschnitt 2.2.2) im Bereich der Sicherheitsleittechnik gegeben.

2.2.1 Abgeschlossene Umrüstungsmaßnahmen in Deutschland

Neben abgeschlossenen Umrüstungsmaßnahmen auf programmierbare oder rechnerbasierte leittechnische Einrichtungen werden im Folgenden auch bereits begonnene Projekte zur Umrüstung genannt.

2.2.1.1 Kernkraftwerk Philippsburg 1 und 2 (KKP)

In beiden Blöcken des Kernkraftwerks Philippsburg kommen seit entsprechenden Umrüstungsmaßnahmen in den vergangenen Jahren programmierbare oder rechnerbasierte leittechnische Einrichtungen zum Einsatz /BFS 03/, /HAG 10/.

Zunächst wurde 1999 der Turbinenschutz von Block 1 komplett ausgetauscht. Seit 2001 ist die Umrüstung des Unabhängigen Sabotage- und Störfallschutzsystems (USUS) zur Beherrschung äußerer Einwirkungen im Kernkraftwerk Philippsburg 1 abgeschlossen. Laut /VGB 08/ wurde vor Realisierung der Umrüstungsmaßnahmen die Software des Leittechniksystems TELEPERM XS der Firma Areva NP auf den Anlagenschulungssimulator übertragen. Die Ergebnisse der damit durchgeführten Tests flossen zurück in die Projektierung /ABB 03/, /ANP 02/. Auch das Kernüberwachungssystem in KKP 1 ist seit 2002 mit dem Leittechniksystem TELEPERM XS realisiert. Dieses System enthält Module zur Überwachung des minimalen Abstandes zur Siedeübergangsleistung, zur Kernstabilitätsmessung, zur Überwachung der maximalen linearen Stableistung und zur Sammeleinfahrkontrolle /BEN 03/.

Im Block 2 des Kernkraftwerks Philippsburg (KKP 2) wurde 2009 die Umrüstung des Reaktorleistungsbegrenzungssystems abgeschlossen. Eingesetzt wird auch hier das Leittechniksystem TELEPERM XS /NEI 09/. Laut /VGB 08/ sind inzwischen auch die Reaktorregelungen mit TELEPERM XS realisiert. Der Genehmigungsumfang für die Umrüstung der Reaktorleistungsleittechnik auf das Leittechniksystem TELEPERM XS aus dem Jahr 2007 umfasst folgende Funktionen: Reaktorleistungsbegrenzung (RELEB), Steuerstabfahrbegrenzung (STAFAB), Kühlmittelmassen-, -druck und -temperaturgradientenbegrenzung (MADTEB), Reaktorleistungsregelung und Primärkreisregelung sowie das Kern-Innenmesssystem /UMB 07/.

Genauere Informationen hierzu liegen der GRS derzeit nicht vor.

2.2.1.2 Kernkraftwerk Neckarwestheim 1 und 2 (GKN)

Auch in der Anlage Neckarwestheim 1 wurden Teile der Leittechnik auf programmierbare oder rechnerbasierte Einrichtungen umgerüstet. Seit dem Jahr 1998 wird in der Reaktorleistungsbegrenzung, Reaktorregelung und Stabsteuerung das Leittechniksystem TELEPERM XS bzw. TELEPERM XP der Firma Areva NP bzw. der Firma

Areva/Siemens eingesetzt /BFS 03/, /HAG 10/, /GKN 99/. Auch die Generatorleistungsbegrenzung und -regelung ist mit TELEPERM XS realisiert. Zu den in TELEPERM XS ausgeführten Begrenzungs- und Regelungseinrichtungen zählen beispielsweise folgende leittechnische Funktionen: Druckhalter-Füllstandsregelung, KMT-Begrenzung, Leistungsverteilungsregelung und Generatorleistungsregelung /GKN 00/. Im Jahr 2005 wurde der bis dahin eingesetzte Sättigungsabstandsrechner durch eine in TELEPERM XP realisierte Rechenschaltung ersetzt /GKN 05/. 2007 wurde das Neutronenflussmesssystem gegen das digital arbeitende Messsystem TK 250 der Firma Merion (vormals MGP Instruments, siehe Bericht „Analyse zum Einsatz und Betrieb elektrotechnischer Einrichtungen“ /GRS 15/) ausgetauscht /GKN 07/.

In der Anlage Neckarwestheim 2 ist ein redundant aufgebauter Turbineneinsatzrechner zur automatischen Leistungssollwertvorgabe mit dem Leittechniksystem TELEPERM XS realisiert /ANP 03/. TELEPERM XP wird seit 2003 im Bereich der Prozessrechneranlage und des Kugelmessrechners eingesetzt /GKN 03/. In den Jahren 2012 und 2013 wurden die Leittechnik des Kühlturms sowie die Leittechnik der Kühlturmzusatzwasseraufbereitung ertüchtigt. Eingesetzt wird nun Simatic S7 der Firma Siemens /GKN 12/.

Genauere Informationen hierzu liegen der GRS derzeit nicht vor.

2.2.1.3 Kernkraftwerk Isar 1 und 2 (KKI)

In KKI 1 wurden Teile der Regelungen und Begrenzungen auf programmierbare oder rechnerbasierte Leittechnik umgerüstet. Von den Umrüstungsmaßnahmen betroffen waren beispielsweise die Reaktordruckbehälter-Füllstandsregelung, die Kondensatregelung, die Speisewasserbehälter-Druckregelung und die Blockleistungsregelung, die alle in den Jahren 1998 bis 2001 erneuert wurden /HOF 10/. Ebenfalls in programmierbare oder rechnerbasierte Leittechnik realisiert sind die Turbinenregelung und die Leistungsverteilungsüberwachung einschließlich Steuerstabfahrfolgesteuerung /WLN 06/. Eingesetzt wird das Leittechniksystem SYMPHONY MELODY von ABB. Auch in der Neutronenfluss- und Leistungsdichteerfassung kommen programmierbare oder rechnerbasierte leittechnische Einrichtungen zum Einsatz /BFS 03/. Zusätzlich wurde eine Wartenumgestaltung vorgenommen, so dass nun ein Bedien- und Beobachtungssystem mit Großbildleinwänden die Funktionen zur Anzeige und Bedienung der oben genannten Regelungen und Begrenzungen übernimmt. Dieses System übernimmt des

Weiteren auch Meldefunktionen für die in SYMPHONY MELODY realisierten Systeme /TÜV 01/.

Im Kernkraftwerk Isar 2 wird das rechnergestützte Prüfsystem GREVER K zur Prüfung der Referenzspannungen der Grenzsignalgeber und Vergleicher des Reaktorschutzsystems eingesetzt /KKI 09/.

Genauere Informationen hierzu liegen der GRS derzeit nicht vor.

2.2.1.4 Kernkraftwerk Gundremmingen B und C (KRB-II B und C)

Im Kernkraftwerk Gundremmingen wird seit der Umrüstung von Teilen der betrieblichen Leittechnik ebenfalls das Leittechniksystem SYMPHONY MELODY von ABB verwendet. Umgerüstet wurde beispielsweise die Kühlturmzusatzwasseraufbereitungsanlage /HOF 10/. Im Abwasseraufbereitungssystem kommt das Leittechniksystem SPPA-T2000 der Firma Siemens zum Einsatz /KRB 12/. Laut Hersteller HIMA wird das Prozessleitsystem HIMAX in der Pumpensteuerung des Kernkraftwerks Gundremmingen eingesetzt /HIM 12/. Des Weiteren wird programmierbare oder rechnerbasierte Leittechnik im Leistungsverteilungs-Überwachungssystem, bei der Brennelementlademaschine, beim Steuerstabfahrrechner und bei der Reaktorfüllstandsmessung eingesetzt /TÜV 08/.

Genauere Informationen hierzu liegen der GRS derzeit nicht vor.

2.2.1.5 Kernkraftwerk Biblis A und B (KWB)

In beiden Blöcken des Kernkraftwerks Biblis wird das Leittechniksystem TELEPERM XS der Firma Areva NP in den Reaktorregelungen eingesetzt. Zudem ist in beiden Blöcken ist die Turbinenregelung seit 2003 mit TELEPERM XP/XS realisiert /KWB 03/.

In den Jahren 2002 und 2003 wurde ein Teil der Lüftungsanlagen von Block A auf TELEPERM XP der Firma Areva/Siemens umgerüstet /KWB 02/. Im Block A kommen programmierbare oder rechnerbasierte leittechnische Einrichtungen zusätzlich zu den oben genannten Bereichen beim Prozessrechner, den Brandmeldeanlagen, der Anlagensicherung, bei Prüfsystemen, beim Sekundär-Einspeisesystem, der Brennelement-

lademaschine und beim vorrangigen Aggregateschutz der Notstromdiesel zum Einsatz /TÜV 09/.

Im Block B sind zusätzlich zu den oben genannten Reaktorregelungen auch die Reaktorbegrenzungen und die Stabsteuerung mit TELEPERM XS realisiert. Im Bereich der Instrumentierung werden ebenfalls programmierbare oder rechnerbasierte leittechnische Einrichtungen eingesetzt /ME 11/. Im Jahr 2009 wurde die Leittechnik der Lüftungsanlagen von Block B erneuert, zum Einsatz kam TELEPERM XP/XS /KWB 09/. Zudem werden programmierbare oder rechnerbasierte leittechnische Einrichtungen in Block B im Neutronenflussmesssystem, im vorrangigen Aggregateschutz der Notstromdiesel und in der Steuerung der Brennelementlademaschine eingesetzt /TÜV 10/.

Genauere Informationen hierzu liegen der GRS derzeit nicht vor.

2.2.1.6 Kernkraftwerk Unterweser (KKU)

Ein weiteres Beispiel für den Einsatz programmierbarer oder rechnerbasierter leittechnischer Einrichtungen in deutschen Kernkraftwerken ist die Reaktorleistungsbegrenzung und -regelung im Kernkraftwerk Unterweser /HAG 10/, für die seit einigen Jahren das Leittechniksystem TELEPERM XS der Firma Areva NP eingesetzt wird /BFS 03/, /KKU 98/.

Genauere Informationen hierzu liegen der GRS derzeit nicht vor.

2.2.1.7 Kernkraftwerk Grohnde (KWG)

Im Jahr 2004 wurde im Kernkraftwerk Grohnde die Leistungsverteilungsüberwachung auf das Leittechniksystem TELEPERM XS der Firma Areva NP umgerüstet /KWG 04/. Die Neutronenflussintrumentierung wurde im Jahr 2009 auf programmierbare oder rechnerbasierte Leittechnik umgerüstet /NMU 11/. Im Jahr 2013 wurde die Umrüstung der Reaktorregelungen auf das Leittechniksystem TELEPERM XS abgeschlossen /KWG 13/. Im Jahr 2012 wurde die Umrüstung der Excore-Instrumentierung auf TELEPERM XS beantragt. Diese wurde nach Kenntnisstand der GRS bisher noch nicht in Betrieb genommen.

Genauere Informationen hierzu liegen der GRS derzeit nicht vor.

2.2.1.8 Kernkraftwerk Emsland (KKE)

Im Kernkraftwerk Emsland wurden Reaktorleistungsregelungen und Regelungen des Primärkreises von den Systemen Iskamatic A und B sowie TELEPERM ME der Firma Siemens auf das Leittechniksystem TELEPERM XS der Firma Areva NP umgerüstet. Die Umrüstung betrifft im Einzelnen die Kühlmittel-Druck-Regelung und Aufbereitung, die Druckhalter-Füllstands-Regelung und Aufbereitung, die Regelungsanalogsignal-Auswahl und Verteilung, die Kühlmittel-Temperatur-Regelung, die D-Bank-Stellungs-Regelung, die D-Bank-Reaktivitätsregelung, die Bor-/Deionat-Mengen-Regelung, die Volumenausgleichs-Behälter-Regelung, die Leistungs-Verteilungs-Regelung, die Mitte-Loop-Regelung. Die Druckhalter-Füllstands-Regelung und die HD-Kühler-Temperatur-Regelung. Zusätzlich wurde der Prozessrechner PRISCA durch das Prozessrechner-system OM 690 von Siemens ersetzt, welches das System TELEPERM XP der Firma Areva/Siemens beinhaltet. /KKE 09/

Genauere Informationen hierzu liegen der GRS derzeit nicht vor.

2.2.1.9 Kernkraftwerk Brokdorf (KBR)

Im Kernkraftwerk Brokdorf wurden im Jahr 2008 die Reaktorregelungen auf das Leit-techniksystem TELEPERM XS der Firma Areva NP umgerüstet /KBR 08/. Die Leit-technikplattform SPPA-T2000 der Firma Siemens mit OM 690 wird für den Prozess-rechner eingesetzt /KBR 09/. Für die Kältemaschinen ist AC 160 von ABB im Einsatz. Simatic S7 Steuerungen der Firma Siemens werden im Bereich der Brennelement-wechseleinrichtung eingesetzt /KBR 03/.

Genauere Informationen hierzu liegen der GRS derzeit nicht vor.

2.2.1.10 Kernkraftwerk Krümmel (KKK)

Im Kernkraftwerk Krümmel ist das Leittechniksystem TELEPERM XS der Firma Areva NP im Bereich des Turbinenschutzes eingesetzt /KKK/.

Genauere Informationen hierzu liegen der GRS derzeit nicht vor.

2.2.1.11 Kernkraftwerk Brunsbüttel (KKB)

Im Kernkraftwerk Brunsbüttel kommt das Leittechniksystem TELEPERM XS beim Turbinenschutz zum Einsatz. Simatic S5 Steuerungen der Firma Siemens werden beispielsweise im Bereich des Fahrwerks der Brennelementwechselbühne eingesetzt /WLN 04/. Bei der Strahlenmesstechnik werden Komponenten des Systems TK 250 der Firma Merion (vormals MGP Instruments, siehe dazu auch Bericht „Analyse zum Einsatz und Betrieb elektrotechnischer Einrichtungen“ /GRS 15/) verwendet /TÜV 07/.

Genauere Informationen hierzu liegen der GRS derzeit nicht vor.

2.2.1.12 Kernkraftwerk Grafenrheinfeld (KKG)

Während der Revision 2009 wurde im Kernkraftwerk Grafenrheinfeld die Leittechnik der Reaktorregelung und der Turbinenregelung auf programmierbare oder rechnerbasierte Leittechnik umgerüstet. /EON 09/, /ATW 10/.

Genauere Informationen hierzu liegen der GRS derzeit nicht vor.

2.2.2 Sicherheitsleittechnik: Abgeschlossene Umrüstungsmaßnahmen und Neubauprojekte im Ausland

Neben Projekten zur Umrüstung auf programmierbare oder rechnerbasierte Sicherheitsleittechnik wird bei dem folgenden Überblick auch auf den Einsatz von programmierbarer oder rechnerbasierter Sicherheitsleittechnik beim Neubau von Reaktoren eingegangen. Die für diese Zusammenstellung ausgewählten Projekte sind dabei nach bereits abgeschlossenen Projekten (dieser Abschnitt) und geplanten Projekten (Abschnitt 2.2.3) gruppiert. Innerhalb dieser Gruppen sind die einzelnen Projekte chronologisch nach Abschlussdatum bzw. geplantem Abschlussdatum aufgeführt.

2.2.2.1 Darlington 1 und 2, Kanada

Die Blöcke 1 und 2 der kanadischen Anlage Darlington waren die ersten CANDU-Reaktoren (CANDU: CANada Deuterium Uranium), die mit vollständig programmierbare oder rechnerbasierte leittechnischen Einrichtungen in Betrieb genommen wurden

/NUR 10/. Die beiden Reaktoren mit je 878 MW elektrischer Leistung gingen 1990 bzw. 1992 in Betrieb.

Jeder Block besitzt zwei Schnellabschaltsysteme (Shutdown System SDS1 und SDS2), die funktional voneinander unabhängig und physikalisch getrennt aufgebaut sind:

- SDS1 der Steuerstabeinwurf
- SDS2 die Boreinspeisung

Die Sensoren sind jeweils nur einem System zugeordnet, d. h. jedes System besitzt eigene Messeinrichtungen. Teilweise werden für dieselben Parameter diversitäre Messungen verwendet. Zusätzlich verwenden die beiden Systeme für einige Ereignisabläufe diversitäre Anregekriterien.

Jedes Schnellabschaltsystem ist dreifach redundant aufgebaut. Das SDS1 löst bei 2v3-Auslösesignalen aus den Redundanzen eine Reaktorschnellabschaltung (RESA) aus, wobei es keine Rolle spielt, ob die Anregekriterien übereinstimmen, d. h. RESA wird ausgelöst, sobald aus zwei von drei Redundanzen eines der RESA-Auslösesignale vorliegt. Das SDS2 löst ebenfalls bei 2v3-Auslösesignalen aus den Redundanzen RESA aus, allerdings muss hier das Anregekriterium übereinstimmen, d. h. in mindestens zwei Redundanzen muss dasselbe RESA-Auslösesignal vorliegen.

Für die Leittechnik der SDS1 und SDS2 wurden unterschiedliche Systeme verwendet. Die eingesetzten Rechner unterscheiden sich bezüglich Hersteller, Chipfamilie und Board Layout. Weiterhin unterscheiden sich die Systeme durch die bei der Entwicklung eingesetzten Compiler, Programmiersprachen, Entwicklungssoftware und Programmierer. SDS1 verwendet General Automation (GA) Model 220 Rechner (GA-16/220 Mikroprozessoren) sowie in FORTRAN und GA Assembler programmierte Anwendungssoftware. SDS2 verwendet Digital Equipment Corporation Programmed Data Processor Rechner (LSI- 11/23 Mikroprozessoren) sowie in Pascal und MACRO Assembler programmierte Anwendungssoftware.

2.2.2.2 Sizewell B, Großbritannien

Bei der Anlage Sizewell B handelt es sich um den bislang einzigen Druckwasserreaktor in Großbritannien. Der Block B ging 1995 in Betrieb und besitzt eine elektrische Leistung von 1188 MW. Bereits bei Inbetriebnahme wurde in der Anlage programmierbare oder rechnerbasierte Leittechnik implementiert. /NUR 10/

Die Leittechniksysteme in Sizewell B umfassen ein primäres Schutzsystem (Primary Protection System (PPS)) und ein sekundäres Schutzsystem (Secondary Protection System (SPS)). Das PPS umfasst die RESA und weitere Sicherheitsfunktionen, die zur Beherrschung von Auslegungsstörfällen notwendig sind. Das SPS dient als diversitäres Backup-System und ist nur zur Beherrschung ausgewählter auslösender Ereignisse (angenommene Ereigniseintrittshäufigkeit > 10^{-3} pro Jahr) vorgesehen. Beide Systeme sind vierfach redundant aufgebaut und die Auslösung einer Schutzaktion erfolgt nach 2v4-Auswahl. /NUR 10/

Für das PPS wird das programmierbare oder rechnerbasierte Westinghouse Integrated Protection System eingesetzt /NUR 04/. In jeder der vier Redundanzen sind zwei funktional diversitäre Teilsysteme realisiert, die auf der Grundlage verschiedener Anregekriterien arbeiten. Eines der Teilsysteme ist für die Bildung von RESA-Auslösesignalen verantwortlich, das andere für die Bildung von Auslösesignalen für andere Schutzaktionen. /NUR 10/

Das SPS nutzt die Laddic Technologie /USP 70/ von British Energy/GEC, die auf festverdrahteten Magnetkern-Logikelementen basiert /NUR 10/.

2.2.2.3 Chooz 1, Frankreich

Der Block 1 der französischen Anlage Chooz, der seit 2000 in Betrieb ist, ist der erste Druckwasserreaktor vom Typ N4. Chooz-B2 sowie Civaux 1 und 2 sind Blöcke desselben Typs. Alle vier besitzen 1500 MW elektrische Leistung und seit Inbetriebnahme die gleiche programmierbare oder rechnerbasierte Sicherheitsleittechnik /POU 09/. In der Sicherheitsleittechnik gibt es ein primäres Sicherheitssystem für die RESA und Notkühlfunktionen und diversitär dazu ein Backup-System für ausgewählte auslösende Ereignisse (angenommene Ereigniseintrittshäufigkeit > 10^{-3} pro Jahr). /NUR 10/

Das primäre Sicherheitssystem der N4-Anlagen nutzt das Leittechniksystem Système de Protection Intégré Numérique (SPIN). Das N4-SPIN-System basiert auf Motorola 68000 Mikroprozessoren. Die Anwendungssoftware wurde in der Programmiersprache C programmiert. Das System besitzt vier redundante Kanäle für Messwerterfassung und Signalverarbeitung. In jedem Kanal werden die Signale von Erfassungseinheiten erfasst und auf Funktionseinheiten verteilt, von denen die Auslösesignale gebildet werden. Diese Signale dienen als Eingangssignale für die Logic Safeguard Units (ULS), die eine 2v4-Auswahl vornehmen. /NUR 10/

Das diversitäre Backup-System wurde unter Verwendung des Leittechniksystems Contronic-E von Hartmann und Braun realisiert. Dieses System basiert auf Intel 80286 Mikroprozessoren (mit Intel 80287 Co-Prozessor). Für die Anwendungssoftware wurde eine proprietäre graphische Programmiersprache genutzt. /NUR 10/

2.2.2.4 Beznau 1 und 2, Schweiz

Bei den beiden Blöcken des schweizerischen Kernkraftwerks Beznau handelt es sich um Druckwasserreaktoren mit je 365 MW elektrischer Leistung, die seit 1969 bzw. 1971 in Betrieb sind. In den Jahren 2000 und 2001 wurde das analoge Reaktorschutz- und Regelungssystem durch ein programmierbares oder rechnerbasiertes Sicherheitsleittechniksystem ersetzt. /HAN 05/

Die neue Leittechnik für das Reaktorschutz- und Regelungssystem wurde basierend auf dem Leittechniksystem TELEPERM XS der Firma Areva NP realisiert. Auf den Rechnern des Reaktorschutzsystems werden die Prozesssignale erfasst, digitalisiert und verarbeitet sowie die Auslösesignale für Schutzaktionen entsprechend der Vorgaben aus der verfahrenstechnischen Aufgabenstellung gebildet. Die gebildeten Schutzsignale werden als binäre Einzelsignale an eine in Relaistechnik aufgebaute Voter-Ebene übergeben. Über diese Voter-Ebene werden die einzelnen Schutzaktionen ausgelöst. /HAN 05/

Das Regelungssystem ist zweifach redundant aufgebaut. Ebenfalls zwei redundante Rechner sind für die Bildung und Weiterleitung von Messungen sowie als Schnittstelle zum Servicegerät und zum Anlageninformationssystem vorhanden. Diese beiden Rechner sind jeweils über getrennte Datenbusse mit dem Rechner einer Diversitätsgruppe verbunden. /HAN 05/

Das Kernkraftwerk Beznau verfügt über ein Notstandsschutzsystem, das als Backup-System für das programmierbare oder rechnerbasierte Reaktorschutz- und Regelungssystem dient. Dieses Notstandsschutzsystem verfügt über eine eigene Messwerterfassung und -verarbeitung. Bei diesem Notstandsschutzsystem handelt es sich um ein unabhängiges, weitgehend redundantes Not- und Nachkühlsystem. /HSK/

Genauere Informationen über dieses Backup-System liegen der GRS derzeit nicht vor.

2.2.2.5 Temelín 1 und 2, Tschechische Republik

Bei beiden Blöcken der tschechischen Anlage Temelín handelt es sich um den russischen Druckwasserreaktor-Typ WWER-1000 (WWER: Wasser Wasser Energie Reaktor), wobei beide eine elektrische Leitung von jeweils 963 MW haben. Block 1 ist seit 2002 in Betrieb und Block 2 seit 2003. Die Anlage befand sich bereits seit 1982 in Bau. Vor Fertigstellung wurde ein Modernisierungsprogramm durchgeführt, in dessen Rahmen auch die ursprüngliche analoge Leittechnik des Reaktorschutzsystems durch ein programmierbares oder rechnerbasiertes Leittechniksystem ersetzt wurde. /NUR 10/

Ähnlich wie in Sizewell B (siehe Abschnitt 2.2.2.2) besitzen die Blöcke in Temelín je ein primäres Reaktorschutzsystem (Primary Reactor Protection System (PRPS)) und ein diversitäres Schutzsystem (Diverse Protection System (DPS)) mit reduziertem Funktionsumfang. Das primäre Reaktorschutzsystem umfasst die RESA und die Schutzfunktionen (Engineered Safety Feature Actuation System (ESFAS)). /NUR 10/

Das PRPS basiert auf dem Westinghouse Integrated Protection System und ist mittels der Westinghouse Eagle 2000 Plattform implementiert. Die Eagle 2000 Plattform nutzt Intel 80486 Mikroprozessoren. Die Anwendungssoftware ist in einer Kombination aus PL/M-86 und ASM86 programmiert /WAA 09/. Das PRPS ist dreifach redundant aufgebaut. Jede Redundanz übermittelt die innerhalb der Redundanz gebildeten Auslösesignale an die anderen beiden Redundanzen. In jeder Redundanz erfolgt eine 2v3-Auswahl über Mikroprozessoren. Nachfolgend erfolgt für die Redundanzen eine 2v3-Auswahl über einen Relais-Voter. /NUR 10/

Das DPS dient für ausgewählte auslösende Ereignisse (angenommene Ereigniseintrittshäufigkeit > 10^{-3} pro Jahr) als Backup-System zum PRPS. Das DPS nutzt das System Ovation der Firma Emerson, welches auf Motorola 68000 Mikroprozessoren ba-

siert. Die Anwendungssoftware wurde in ADA geschrieben. Wie das PRPS ist auch das DPS dreisträngig aufgebaut und besitzt zwei 2v3-Auswahlebenen. /NUR 10/

2.2.2.6 Uljin 5 und 6, Südkorea

Die südkoreanische Anlage Uljin besteht aus 6 Druckwasserreaktoren mit elektrischen Leistungen zwischen 940 und 995 MW. Die Blöcke 5 und 6, die seit 2004 bzw. 2005 in Betrieb sind, sind mit programmierbarer oder rechnerbasierter Leittechnik ausgestattet.

Die Sicherheitsleittechnik beinhaltet ein primäres System (u. a. Plant Protection System (PPS) und Engineered Safety Feature Actuation System-Auxiliary Cabinet (ESFAS-AC)) und ein diversitäres Backup-System (Diverse Protection System (DPS)) für ausgewählte auslösende Ereignisse (angenommene Ereigniseintrittshäufigkeit $> 10^{-3}$ pro Jahr). /NUR 10/

Das PPS beinhaltet Reaktorschnellabschalt- und Schutzfunktionen. Das PPS besteht aus vier redundanten Kanälen zur Messwerterfassung und Signalverarbeitung. Vor Auslösung einer RESA oder einer anderen Schutzaktion erfolgt eine 2v4-Auswahl im Local Coincidence Logic Prozessor. Die vom PPS gebildeten Signale für Schutzaktionen werden an das ESFAS-AC übergeben. Dort ist eine zweifach redundante zusätzliche 2v4-Auswahllogik für die Anregung von Schutzaktionen realisiert. Das PPS und das ESFAS-AC nutzen Advant Controller 160 (AC160) von ABB mit Motorola CPU. /NUR 10/

Das DPS dient zur Beherrschung von ATWS-Störfällen (ATWS: Anticipated Transient without Scram). Es umfasst die RESA und die Anregung der Notbespeisung der Dampferzeuger. Das DPS nutzt den Modicon PLC (Programmable Logic Controller), d. h. Intel CPU. Das System besitzt zwei Kanäle und benutzt eine 2v2-Auswahl vor der Auslösung einer RESA oder Notbespeisung der Dampferzeuger. /NUR 10/

Zusätzlich stehen festverdrahtete Handmaßnahmen für die Anregung von RESA oder Schutzfunktionen zur Verfügung /NUR 10/.

2.2.2.7 Dukovany 3, Tschechische Republik

Die tschechische Anlage Dukovany besteht aus vier WWER-440 Blöcken. Die Blöcke gingen in den Jahren 1985 bis 1987 in Betrieb. Seit 2002 läuft ein Modernisierungsprogramm für alle vier Blöcke, das auch die Umrüstung der Sicherheitsleittechnik auf programmierbare oder rechnerbasierte leittechnische Einrichtungen umfasst. Seit 2005 sind die Umrüstungsmaßnahmen für Dukovany 3 abgeschlossen. /NUR 10/

Das neue digitale Reaktorschutzsystem (Digital Reactor Protection System (DRPS)) wurde mit SPINLINE 3 der Firma Rolls Royce realisiert. DRPS umfasst die RESA, Schutzfunktionen und Begrenzungen. Das System ist dreifach redundant aufgebaut. Innerhalb jeder Redundanz gibt es zwei separate Lines of Protection (LOP A und LOP B), die auf unterschiedlichen Teilsystemen basieren. LOP A und LOP B verwenden diversitäre Signale, d. h. für jedes auslösende Ereignis sollen laut /NUR 10/ mindestens zwei Anlagenparameter als Kriterien zur Verfügung stehen, die dann in verschiedenen Lines of Protection verarbeitet werden. Die ggf. in einer LOP gebildeten Auslösesignale werden über Glasfaserverbindungen an die jeweils korrespondierende LOP in den beiden anderen Redundanzen übertragen. Getrennt für die beiden LOPs wird in jeder Redundanz eine 2v3-Auswahl vorgenommen. Für die drei Redundanzen erfolgt danach eine 2v3-Auswahl über Relais-Voter. /NUR 10/

Bei der Implementierung von RESA, Schutzfunktionen, Begrenzungen und Regelungen mit SPINLINE 3 in Dukovany 3 sollen unterschiedliche Eingabewerte und Verarbeitung dieser Werte mit verschiedenen Softwareanwendungen die funktionale Diversität der Teilsysteme sicherstellen /NUR 10/.

Informationen zu einem ggf. vorhandenen Backup-System für das DRPS liegen der GRS derzeit nicht vor.

2.2.2.8 Tianwan 1 und 2, Volksrepublik China

Die Blöcke 1 und 2 der chinesischen Anlage Tianwan sind seit ihrer Errichtung mit programmierbarer oder rechnerbasierter Sicherheitsleittechnik ausgestattet. Bei Tianwan 1 und 2 handelt es sich um WWER-1000 /IAE 08/. Block 1 ist im Mai 2007 in Betrieb gegangen und Block 2 im August desselben Jahres. Tianwan ist die erste chinesi-

sche Anlage, die mit programmierbarer oder rechnerbasierter Sicherheitsleittechnik ausgestattet wurde /XU 10/.

In Tianwan wird das Leittechniksystem TELEPERM XS der Firma Areva NP eingesetzt /NUC 10/. Für jedes auslösende Ereignis wurden laut /XU 10/ bereits in der Planungsphase zwei unterschiedliche physikalische Kriterien definiert. In der Sicherheitsleittechnik des Reaktorschutzsystems sind unter Verwendung von TELEPERM XS zwei Teilstränge A und B realisiert. Die Rechner der beiden Teilstränge arbeiten nicht synchron. Es gibt auch keinen Datenaustausch zwischen den beiden Teilsträngen A und B. Zusätzlich zum Reaktorschutzsystem gibt es für die RESA ein festverdrahtetes Backup System. Zur Beherrschung von ATWS-Störfällen wurde zusätzlich zu dem in TELEPERM XS realisierten Design noch eine zusätzliche Funktionalität im TELEPERM XP-System der Firma Areva/Siemens realisiert, welche eine diversitäre Möglichkeit zur Abschaltung der Turbine und zum Start des zusätzlichen Speisewassersystems bietet. /XU 10/

2.2.2.9 Tomari 3, Japan

Der Block 3 der japanischen Anlage Tomari ist seit seiner Errichtung mit programmierbarer oder rechnerbasierter Sicherheitsleittechnik ausgestattet. Bei Tomari 3 handelt es sich um einen 3-Loop Druckwasserreaktor mit einer Leistung von 866 MW. Die Anlage ist seit Ende 2009 in Betrieb.

Die leittechnischen Einrichtungen des Sicherheitssystems von Tomari 3 umfassen das RPS (Reactor Protection System) für die RESA und das ESFAS (Engineered Safety Features Actuation System) für die Anregung von Schutzaktionen /KON 10/.

Das RPS beinhaltet neben dem primären programmierbaren oder rechnerbasierten System noch ein festverdrahtetes Backup-System. Die leittechnischen Einrichtungen des primären Systems sind vierfach redundant aufgebaut. Ausgewählte Anlagenparameter werden überwacht und die erfassten Messsignale werden von jeder Redundanz verarbeitet. Sobald es in einer Redundanz zur Bildung eines RESA-Auslösesignals kommt, werden die beiden zu dieser Redundanz gehörenden Trennschalter in der Energieversorgung der Steuerstabantriebe geöffnet. Die Trennschalter sind so angeordnet, dass bei einem anstehenden RESA-Auslösesignal in 2v4 Redundanzen die Energieversorgung komplett unterbrochen ist und RESA ausgelöst wird. /KON 10/

Das festverdrahtete Backup-System ist dem primären programmierbaren oder rechnerbasiertem System nachgeordnet. Es wurde installiert, um bei einem CCF der oben genannten Trennschalter im Anforderungsfall RESA auszulösen. /KON 10/

Das ESFAS besitzt auf der Verarbeitungsebene vier redundante Kanäle für die Signalverarbeitung. Zwei redundante Voter führen auf der nachfolgenden Rechnerebene eine 2v4-Auswahl für die in diesen Kanälen gebildeten Auslösesignale durch und lösen ggf. eine ESFAS-Schutzaktion aus. /KON 10/

Beide Systeme wurden mit dem MELTAC-System der Firma Mitsubishi realisiert /NRC 08/, /MIT 07/.

2.2.2.10 Ringhals 1, Schweden

Bei Ringhals 1 handelt es sich um den ältesten von vier Reaktorblöcken am schwedischen Standort Ringhals. Der Siedewasserreaktor mit einer elektrischen Leistung von 855 MW ist seit 1976 in Betrieb. In den Jahren 2005 – 2009 wurden umfassende Modernisierungen durchgeführt. Unter anderem wurde das bisherige, auf analoger Relais-Technik basierende Reaktorschutzsystem um programmierbare oder rechnerbasierte leittechnische Einrichtungen ergänzt. Seit Juli 2010 sind die Umrüstungsmaßnahmen im Reaktorschutzsystem abgeschlossen. /ARE 10/

Das jetzige Reaktorschutzsystem besteht aus zwei räumlich und funktional voneinander getrennten Teilen. Ein Teil ist im OPS (Original Plant Section) realisiert und der andere im DPS (Diversified Plant Section) /AUT 10/.

- OPS: Das OPS umfasst die Anlage mit dem bisherigen Reaktorschutzsystem in weitgehend unveränderter Form. Einige Funktionen des ursprünglichen OPS, wie beispielsweise Systeme zur Druckentlastung und zur Kernkühlung, werden nun vom DPS übernommen.
- DPS: Die programmierbaren oder rechnerbasierten leittechnischen Einrichtungen des DPS erfüllen Funktionen im Rahmen von Energieversorgung und Messtechnik sowie im Reaktorschutzsystem und bei der Ausführung von Sicherheitsfunktionen.

Die Funktionen des OPS sind unabhängig von den Funktionen des DPS. Sowohl OPS als auch DPS können Ereignisse, die den Ausfall des jeweils anderen Teils (z. B. durch Erdbeben, Brand oder CCF) beinhalten, beherrschen.

Das DPS wurde mit dem Leittechniksystem TELEPERM XS der Firma Areva NP realisiert. Die leittechnischen Einrichtungen von TELEPERM XS sind dreifach redundant aufgebaut. Die drei leittechnischen Redundanzen sind jeweils räumlich getrennt ausgeführt. Jede Redundanz des TELEPERM XS-Systems besteht aus Einrichtungen zur Messwerterfassung und -aufbereitung, zur Signalverarbeitung, zur Grenzwertüberwachung und zur Bildung von Auslösesignalen sowie zur Ansteuerung der Stellglieder. Auf der Ebene der Messwerterfassung und -aufbereitung werden Prozesssignale erfasst und digitalisiert. Auf den Rechnern der Signalverarbeitung werden über Abgleich der Prozesssignale mit vorgegebenen Grenzwerten ggf. Schutzauslösesignale gebildet. Diese Signale dienen als binäre Eingangssignale für Relais-Voter, die nach erfolgter Auswahl (1v2, 2v2, 2v3, 2v4 etc.) die Schutzfunktionen auslösen /AUT 10/.

2.2.2.11 Gösgen, Schweiz

Im Kernkraftwerk Gösgen wurde die Regelungs- und Begrenzungstechnik auf das System TELEPERM XS der Firma Areva NP umgerüstet. Laut /GÖS 14/ wurde in der Jahresrevision 2014 die Leittechnik modernisiert. Das Projekt umfasste eine größere Zahl von Steuerungs-, Regelungs- und Begrenzungseinrichtungen. Insgesamt wurden 32 Leittechnikschränke ersetzt. Diese Regelungs- und Begrenzungssysteme sind Bestandteil der Sicherheitsleittechnik und stellen die Steuerung und Überwachung des Kraftwerks sicher.

Genauere Informationen hierzu liegen der GRS derzeit nicht vor.

2.2.2.12 Oconee 1, 2 und 3, USA

In der US-amerikanischen Anlage Oconee wurde in allen drei Blöcken die festverdrahtete Sicherheitsleittechnik auf programmierbare oder rechnerbasierte Sicherheitsleittechnik umgerüstet. Alle drei Blöcke sind Druckwasserreaktoren mit einer Leistung von jeweils 885 MW. Die Genehmigung für die Umrüstungsmaßnahmen wurde Anfang 2010 erteilt /NRC 10/, die Umrüstung erfolgte in den folgenden Revisionen.

Die Sicherheitsleittechnik in Oconee umfasst das Reactor Protection System (RPS) und das Engineered Safety Protection System (ESPS), welches dem üblicherweise in US-Anlagen verwendeten Engineered Safety Feature Actuation System (ESFAS) entspricht. Für die rechnerbasierte Sicherheitsleittechnik ist der Einsatz der rechnerbasierten Leittechnikplattform TELEPERM XS der Firma Areva NP geplant. /NEI 10a/

Das RPS überwacht ausgewählte Anlagenparameter für den sicheren Anlagenbetrieb und führt ggf. Reaktorschnellabschaltfunktionen aus. Das RPS besteht aus vier redundanten Kanälen, die elektrisch unabhängig und physikalisch separiert aufgebaut sind. Jeder Kanal besteht aus zwei Leittechnikschränken, die die Einrichtungen für die Signalverarbeitung, die Stromversorgung und die Verarbeitung der Logikfunktionen sowie die 2v4-Relais-Logik für die RESA und die Kommunikationsfunktionen enthalten. Jeder RPS-Kanal hat seinen eigenen Messwertumformer. Die RPS-Kanäle tauschen die Prozessvariablen über Glasfaserverbindungen aus. Ein fünfter RPS-Kanal führt keine RESA, sondern nicht sicherheitsrelevante Überwachungsfunktionen aus. /DUK 08/

Das ESPS besteht aus zwei redundanten sicherheitsrelevanten Subsystemen. Die Messwerterfassung wird von beiden Subsystemen gemeinsam genutzt. Jedes Subsystem umfasst drei Eingangskanäle und je acht Anregekanäle. Diese Anregekanäle werden den jeweiligen beiden Votern zugeordnet. Die Auslösung von Sicherheitsfunktionen erfolgt nach einer 2v3-Auswahl. Jedes der Subsysteme kann die erforderlichen Sicherheitsfunktionen auslösen. /DUK 08/

Die U.S. NRC gibt in /NUR 10/ die zwei Designattribute „Diversität“ und „Testbarkeit“ für Leittechniksysteme an, die laut U.S. NRC ausreichen, um einen CCF in der Leittechnik ausschließen zu können. In der Genehmigung für das programmierbare oder rechnerbasierte RPS/ESPS-System von Oconee kommt die U.S. NRC zu dem Schluss, dass das vorgeschlagene System beide Kriterien nicht erfüllt und daher ein CCF nicht ausgeschlossen werden kann. Daher wurden in der Anlage Oconee aufgrund der Forderungen der U.S. NRC folgende diversitäre Systeme eingerichtet:

- Ein diversitäres Anregesystem für die Niederdruckeinspeisung für die Beherrschung des Software CCF bei einem postulierten großen Leck.
- Ein diversitäres Anregesystem für die Hochdruckeinspeisung für die Beherrschung des Software CCF bei einem postulierten kleinen Leck.

Beide Systeme nutzen konventionelle analoge Grenzwertgeber und eine 2v3-Logik für die Anregung über den Primärkreisdruck. Die Systeme beinhalten je drei analoge Grenzwertgeber und Entkopplungsrelais /DUK 08/.

Zusätzlich wird bei der Einrichtung des programmierbaren oder rechnerbasierten RPS/ESPS-Systems von bereits existierenden diversitären Systemen Kredit genommen:

- Das ATWS Mitigation System für die Beherrschung von ATWS-Störfällen mit gleichzeitig unterstelltem Verlust des Hauptspeisewassers.
- Das Diverse Scram System für die diversitäre Anregung der RESA.

Diese beiden Systeme basieren auf der Technik eines anderen Herstellers (Programmable Logic Controllers der Firma Schneider) als das programmierbare oder rechnerbasierte RPS/ESPS-System /DUK 08/.

2.2.2.13 Weitere abgeschlossene Projekte

Zu Umrüstungsmaßnahmen in weiteren Kernkraftwerken sind der GRS nur Informationen in geringem Umfang bekannt. Ausgewählte Umrüstungsmaßnahmen werden nachfolgend kurz beschrieben.

Für die Umrüstung der Sicherheitsleittechnik der schwedischen Anlage Oskarshamn 1 wurde das Westinghouse Atom Advant System mit Advant Controllern 160 (AD160) von ABB gewählt /IAE 05/. Die Umrüstmaßnahmen waren 2002 abgeschlossen /NUR 10/.

In allen vier Blöcken der slowakischen Anlage Bohunice wurden Teile der Sicherheitsleittechnik auf programmierbare oder rechnerbasierte Sicherheitsleittechnik umgerüstet. Dabei wurde das Leittechniksystem TELEPERM XS der Firma Areva NP eingesetzt /YAS/. Die Umrüstungsmaßnahmen fanden in den Jahren 1997-2000 für die Blöcke 1 und 2 und in den Jahren 2004-2008 für die Blöcke 3 und 4 statt /LIN 09/.

In Frankreich wurden in den Jahren 1984-1991 in allen 20 Blöcken vom Typ P4, d. h. in Belleville 1 und 2, Cattenom 1 bis 4, Flamanville 1 und 2, Golfech 1 und 2, Nogent 1 und 2, Paluel 1 bis 4, Penly 1 und 2, sowie in St. Alban 1 und 2, eine teilweise Umrüs-

tung auf programmierbare oder rechnerbasierte Leittechnik vorgenommen. Bei diesen Umrüstungen war auch der Reaktorschutz enthalten. In den Anlagen vom Typ P4 wird das Leittechniksystem SPIN genutzt. Die Anlagen Fessenheim 1 und 2 sowie die Blöcke 2 bis 5 des Kernkraftwerks Bugey wurden auf programmierbare oder rechnerbasierte Sicherheitsleittechnik umgerüstet, beginnend im Jahr 2000. Eingesetzt wird in diesen Anlagen das Leittechniksystem SPINLINE 3 von Rolls-Royce /ELS 02/, /BFS 03/, /ROL 10/.

Die ungarische Anlage Paks setzt seit den Umrüstungsmaßnahmen zwischen 1999 und 2002 ebenfalls in allen vier Blöcken programmierbare oder rechnerbasierte Sicherheitsleittechnik auf Basis des Leittechniksystems TELEPERM XS der Firma Areva NP ein /NUC 10/.

In der Volksrepublik China wird in den beiden Blöcken der Anlage Qinshan Phase III seit Inbetriebnahme in den Jahren 2002 und 2003 programmierbare oder rechnerbasierte Sicherheitsleittechnik eingesetzt (beides CANDU-Reaktoren mit 700 MW elektrischer Leistung). In den Blöcken 1 bis 4 der Anlage Qinshan Phase II wird das Leittechniksystem SPINLINE 3 von Rolls Royce eingesetzt /ROL 10/. In Qinshan 1 wurden die leittechnischen Einrichtungen des Reaktorschutzsystems ausgetauscht. Der Druckwasserreaktor mit 288 MW elektrischer Leistung ist seit 2008 wieder am Netz. Im Reaktorschutz wird nun das Leittechniksystem TELEPERM XS der Firma Areva NP eingesetzt /ARE /.

In der Ukraine wurde in den Jahren 1998 bis 2009 das Reaktorschutzsystem in den Anlagen Saporischschja 1 bis 3, Chmelnyzkyj 1, Riwne 1 bis 3 sowie die Blöcke 1 und 2 des Kernkraftwerks Süd-Ukraine auf programmierbare oder rechnerbasierte Leittechnik umgerüstet. Zusätzlich sind die Anlage Chmelnyzkyi 2 sowie der Block 4 des Kernkraftwerks Riwne seit der Inbetriebnahme im Jahr 2004 mit programmierbarer oder rechnerbasierter Sicherheitsleittechnik ausgestattet /YAS 07/, /BFS 03/, /RAD 10/. Zum Einsatz kommt hier auf FPGA (Field Programmable Gate Array) basierende Leittechnik der Firma Radiy /RAD 10/.

Auch die beiden Blöcke 3 und 4 der russischen Anlage Kalinin (WWER-1000) sind seit der Inbetriebnahme 2004 bzw. 2011 mit programmierbarer oder rechnerbasierter Sicherheitsleittechnik ausgestattet /IAE 08/. Eingesetzt wird das Leittechniksystem TPTS, welches auf TELEPERM ME der Firma Siemens basiert und im russischen Forschungsinstitut VNIIA hergestellt wird /VNI/. Zudem wurde die Leittechnik des Blocks 1

in Zusammenarbeit mit Tecnatom modernisiert /SIV 11/. Dies umfasste nach Angaben des Herstellers auch eine Modernisierung der Warte /TEC 08/. Die Leittechnik des Reaktorschutzsystems der russischen Anlage Kola 3 wurde in Zusammenarbeit mit Areva NP ersetzt. Die Modernisierung der Sicherheitsleittechnik der Blöcke 1 und 2 der russischen Anlage Balakovo wurde in Zusammenarbeit mit DS&S durchgeführt. /SIV 11/

In Japan wurde programmierbare oder rechnerbasierte Sicherheitsleittechnik in vollem Umfang erstmalig in den Blöcken 6 und 7 des Kernkraftwerks Kashiwazaki-Kariwa eingesetzt /KUK 09/, /KUN 06/. Die beiden ABWR-Blöcke (Advanced Boiling Water Reactor) gingen 1996 bzw. 1997 in Betrieb /KON 10/. Die später gebauten ABWR Hamaoka 5 (in Betrieb seit 2005) und Shika 2 (in Betrieb seit 2006) besitzen ebenfalls programmierbare oder rechnerbasierte leittechnische Einrichtungen im Reaktorschutz /KUN 06/. In den DWR Blöcken 1 und 2 des Kernkraftwerks Ikata wurde 2009 auf programmierbare oder rechnerbasierte Sicherheitsleittechnik umgerüstet, zum Einsatz kommt hier das Leittechniksystem MELTAC der Firma Mitsubishi. /JAI 09/, /MIT 07/

In der litauischen Anlage Ignalina 2 wurde ein diversitäres Abschaltsystem programmierbarer oder rechnerbasierter Leittechnik realisiert. Eingesetzt wird das Leittechniksystem SPINLINE 3 von Rolls Royce. /ROL 10/

2.2.3 Sicherheitsleittechnik: Geplante Projekte im Ausland

2.2.3.1 Loviisa 1 und 2, Finnland

In der finnischen Anlage Loviisa sind zwei Reaktoren vom Typ WWER-440 mit je einer elektrischen Leistung von 488 MW seit 1977 bzw. 1981 in Betrieb. Umfassende Umrüstungsmaßnahmen für die gesamten leittechnischen Einrichtungen waren für die Jahre 2008-2012 geplant. Die zunächst geplante Umrüstung der gesamten Sicherheitsleittechnik auf TELEPERM XS der Firma Areva NP wird nach /NEI 14/ nicht weiter verfolgt. Stattdessen wurde die Firma Rolls Royce mit der Modernisierung der Sicherheitsleittechnik der Blöcke 1 und 2 beauftragt /NEI 14/. Daher soll die neue Sicherheitsleittechnik auf Basis des Leittechniksystems SPINLINE 3 erfolgen. Neben diesem programmierbaren oder rechnerbasierten System soll das bisherige festverdrahtete System in Teilen erhalten bleiben.

2.2.3.2 Olkiluoto 3, Finnland

Derzeit in Bau befindet sich der Block 3 der finnischen Anlage Olkiluoto. Hier entsteht ein EPR (European Pressurized Water Reactor) mit einer elektrischen Leistung von 1600 MW. Die Sicherheitsleittechnik ist überwiegend programmierbar oder rechnerbasiert.

Die geplante programmierbare oder rechnerbasierte Sicherheitsleittechnik basiert auf dem System TELEPERM XS der Firma Areva NP und SPPA-T2000 der Firma Siemens /NUR 10/. Die Architektur der Leittechnik umfasst ein primäres Sicherheitssystem, ein digitales Backup-System mit reduziertem Funktionsumfang und ein sog. „hardwired“ Backup-System, das auf FGPA-Bausteinen basiert. Die Reaktorschnellabschaltfunktion und andere Schutzaktionen sind im Reaktorschutzsystem realisiert. Die vier Redundanzen dieses Schutzsystems nutzen das TELEPERM XS -System, welche auf AMD K6-E2 Mikroprozessoren basiert. In jeder Redundanz sind funktional diversitäre Teilsysteme (A und B) vorhanden, die auf unterschiedliche Anlagenparameter zugreifen. Jede Redundanz besitzt fünf Erfassungs- und Verarbeitungseinheiten, die jeweils dem Teilsystem A oder dem Teilsystem B zugeordnet sind. Über Glasfaserverbindungen werden die gebildeten Auslösesignale der Erfassungs- und Verarbeitungseinheiten in einem Teilsystem an die korrespondierenden Teilsysteme in den anderen drei Redundanzen übertragen. Jedem Teilsystem innerhalb einer Redundanz sind zwei Logikeinheiten zugeordnet, die redundant eine 2v4-Auswahl vornehmen. Innerhalb der Logik für die Auslösung von Schutzaktionen sind diese Voter mit einem ODER verknüpft, um auch dann eine Schutzaktion auslösen zu können, wenn ein Voter versagt. Im Fall der Logik für die Auslösung einer RESA sind die Voter mit einem UND verknüpft, um eine unberechtigte RESA zu vermeiden. Die RESA-Auslösesignale der einzelnen Redundanzen öffnen unterschiedliche Schalter in der Energieversorgung der Steuerstäbe. /NUR 10/

Die leittechnischen Einrichtungen, die keine direkte Sicherheitsfunktion erfüllen, nutzen das SPPA-T2000-System der Firma Siemens. Innerhalb dieses Reaktorschutzsystems dient das zweifach redundant ausgeführte Safety Automation System als Backup für das Schutzsystem für die Auslösung von Schutzaktionen bei ausgewählten auslösenden Ereignissen. /NUR 10/

Das zusätzliche „hardwired“ Backup-System kann alle Schnellabschaltfunktionen erfüllen. Dieses festverdrahtete System verwendet dieselben Anlagenparameter wie das

Schutzsystem, nutzt allerdings redundante Messungen dieser Parameter. Darüber hinaus sind festverdrahtete Handmaßnahmen als weiteres Backup vorhanden. /NUR 10/

2.2.3.3 Flamanville 3, Frankreich

In der französischen Anlage Flamanville befindet sich derzeit der dritte Block, ein EPR mit einer elektrischen Leistung von 1600 MW, im Bau. Flamanville 3 soll 2017 den kommerziellen Betrieb aufnehmen /EDF 10/. Flamanville 3 soll vollständig programmierbarer oder rechnerbasierter Leittechnik und einer bildschirmbasierten Warte ausgestattet werden.

Für die Realisierung der leittechnischen Einrichtungen ist der Einsatz des Systems TELEPERM XS der Firma Areva NP im Reaktorschutzsystem und SPPA-T2000 der Firma Siemens für das automatisierte Sicherheitssystem geplant /POU 09/, /GAS 10/. Die Autorité de Sureté Nucléaire (ASN) kommt in ihrer Bewertung der vorgesehenen Architektur der programmierbaren oder rechnerbasierten Leittechnik in der geplanten Anlagen zu dem Schluss, dass die Diversität zwischen diesen beiden Plattformen zwar ausreichend ist, bislang aber kein Nachweis erbracht wurde, dass das System SPPA-T2000 den Vorgaben für die geforderten Sicherheitsklassen entspricht. /ASN 10/

Weitere Informationen liegen der GRS derzeit nicht vor.

2.2.3.4 Weitere geplante Projekte

Zu weiteren geplanten Umrüstungsmaßnahmen liegen der GRS derzeit nur wenige Informationen vor. Diese werden nachfolgend aufgeführt.

In Südkorea sollen die Blöcke 1 und 2 der Anlage Shin-Kori sowie die beiden Blöcke der Anlage Shin-Wolsong mit programmierbarer oder rechnerbasierter Leittechnik ausgestattet werden. Shin-Kori 1 und 2 sowie Shin-Wolsong 1 wurden in den Jahren 2010 bzw. 2012 mit dem Netz synchronisiert, Shin-Wolsong 2 ist derzeit (November 2014) noch nicht fertiggestellt. Auch die Blöcke 3 und 4 der Anlage Shin-Kori, die bis 2016 in Betrieb gehen sollen, sollen ein vollständig programmierbares oder rechnerbasiertes Reaktorschutzsystem erhalten. /KIN/

Die schweizerische Anlage Leibstadt plant eine komplette Umrüstung der Leittechnik. Hierbei soll ein Leittechniksystem der Firma Westinghouse zum Einsatz kommen. Das Projekt soll 2018 abgeschlossen sein. /BFS 03/, /HUR 07/

In den beiden Blöcken der US-amerikanischen Anlage Diablo Canyon wurden in den letzten Jahren einige Leittechniksysteme auf programmierbare oder rechnerbasierte Leittechnik umgerüstet, darunter beispielsweise Regelungen für Turbine und Speisewassersystem. Eine Umrüstung des Reaktorschutzes ist ebenfalls geplant. /NUC 07/

In der Russischen Föderation soll ein Block der Anlage Novovoronezh II mit dem Leittechniksystem TELEPERM XS der Firma Areva NP ausgestattet werden. Der Block vom Typ WWER-1200 soll bis 2016 in Betrieb gehen. /NEI 10/

In China werden die derzeit in Bau befindlichen Anlagen Hongyanhe sowie Ningde mit dem Leittechniksystem SPINLINE 3 von Rolls Royce ausgestattet. Die Blöcke 1 und 2 beider Anlagen gingen in den Jahren 2012 – 2014 in Betrieb. Bei allen vier Blöcken handelt es sich um CPR-1000 (Chinesischer Druckwasserreaktor). /ROL 10/

In Japan ist geplant, die vier Blöcke der Anlage Takahama sowie die vier Blöcke der Anlage Ohi auf programmierbare oder rechnerbasierte Leittechnik umzurüsten. In allen Blöcken kommt für das Reaktorschutzsystem das Leittechniksystem MELTAC der Firma Mitsubishi zum Einsatz. Der Einsatz dieses Systems ist auch für die in Planung befindlichen Blöcke 3 und 4 der Anlage Tsuruga vorgesehen. /MIT 07/

2.3 Überblick über programmierbare oder rechnerbasierte Leittechniksysteme

In diesem Abschnitt wird ein Überblick über programmierbare oder rechnerbasierte Leittechniksysteme gegeben, die bereits in deutschen oder ausländischen Kernkraftwerken eingesetzt werden. In der Tabelle 2.1 wird für jedes dieser Leittechniksysteme aufgeführt, in welchen Anlagen es nach derzeitigem Kenntnisstand der GRS eingesetzt wird. Dabei wird zusätzlich nach der Art der leittechnischen Funktion, für die das Leittechniksystem vorgesehen ist, unterschieden.

Tab. 2.1 Übersicht über eingesetzte Leittechniksysteme (Quellen siehe Abschnitt 1.2, wenn nicht anders angegeben)

Leittechniksystem	Leittechnische Funktion	Kernkraftwerk
TELEPERM XS	Leittechnische Einrichtungen einschließlich Reaktorschutz	Beznau 1 und 2 (Schweiz)
		Ringhals 1 (Schweden)
		Qinshan 1 (Volksrepublik China)
		Tianwan 1 und 2 (Volksrepublik China)
		Paks 1 bis 4 (Ungarn)
		Bohunice (Slowakische Republik)
		Kozloduy 5 und 6 (Bulgarien)
	Leittechnische Einrichtungen einschließlich Reaktorbegrenzungen	Gösgen (Schweiz)
		Unterweser
		Philippsburg 2
		Neckarwestheim 1
		Biblis B
	Leittechnische Einrichtungen wie z. B. Reaktorregelungen, Mess- und Überwachungseinrichtungen, betrieblicher Schutz, Prozessrechner	Emsland
		Biblis A
		Grafenrheinfeld
		Neckarwestheim 2
		Brunsbüttel

Leittechnik-system	Leittechnische Funktion	Kernkraftwerk
		Grohnde
		Brokdorf
		Krümmel
	Leittechnische Einrichtungen einschließlich USUS	Philippsburg 1
OVATION	Leittechnische Einrichtungen einschließlich Reaktorschutz	Temelín 1 und 2 (Tschechische Republik)
	Leittechnische Einrichtungen wie z. B. Reaktorregelungen, Mess- und Überwachungs-einrichtungen, betrieblicher Schutz, Prozessrechner /WES 04/	South Texas 1 und 2 (USA)
		Point Beach 1 und 2 (USA)
		Surry 1 und 2 (USA)
		Braidwood 1 und 2 (USA)
		Byron 1 und 2 (USA)
		Vandellos 2 (Spanien)
		Almaraz 1 und 2 (Spanien)
		Ascó 1 und 2 (Spanien)
		Leningrad (Russische Föderation)
		Ringhals 2 (Schweden)
		Kozloduy 5 und 6 (Bulgarien)
		Shin-Kori 1 und 2 (Südkorea)
		Shin Wolsong 1 und 2 (Südkorea)
SPINLINE 3	Leittechnische Einrichtungen einschließlich Reaktorschutz /ROL 12/	Belleville 1 und 2 (Frankreich)
		Cattenom 1 bis 4 (Frankreich)
		Flamanville 1 und 2 (Frankreich)
		Golfech 1 und 2 (Frankreich)
		Nogent 1 und 2 (Frankreich)
		Paluel 1 bis 4 (Frankreich)
		Penly 1 und 2 (Frankreich)
		St. Alban 1 und 2 (Frankreich)

Leittechnik-system	Leittechnische Funktion	Kernkraftwerk
		Fessenheim 1 und 2 (Frankreich)
		Bugey 2 bis 5 (Frankreich)
		Dukovany 3 (Tschechische Republik)
		Kozloduy (Bulgarien)
		Qinshan Phase II 1 bis 4 (Volksrepublik China)
		Tihange (Belgien)
		Ignalina (Litauen)
SYMPHONY MELODY	Leittechnische Einrichtungen wie z. B. Reaktorregelungen, Mess- und Überwachungs-einrichtungen, betrieblicher Schutz, Prozessrechner	Isar 1
		Gundremmingen B und C
HIMAX	Leittechnische Einrichtungen wie z. B. Reaktorregelungen, Mess- und Überwachungs-einrichtungen, betrieblicher Schutz, Prozessrechner	Gundremmingen B und C
MELTAC	Leittechnische Einrichtungen einschließlich Reaktorschutz /MIT 14/	Tomari 3 (Japan)
		Ikata 1 und 2 (Japan)
		Mihama 3 (Japan)
		Takahama 1 bis 4 (Japan)
		Ohi 1 bis 4 (Japan)

Nachfolgend werden die Leittechniksysteme, wie sie vom Hersteller üblicherweise angeboten werden, im Einzelnen beschrieben. Dabei wird mit Blick auf die Herstellerunterlagen vor allem auf die Auslegung, die Architektur und die eingesetzten Baugruppen eingegangen.

2.3.1 TELEPERM XS-System

Das Leittechniksystem TELEPERM XS der Firma Areva NP wird z. B. im Reaktorschutz- und Regelsystem des Kernkraftwerks Beznau 1 und 2 (Schweiz), im

Reaktorschutz des Kernkraftwerks Tianwan (Volksrepublik China), im Reaktorschutz des Kernkraftwerkes Ringhals 1 (Schweden), in der Reaktorleistungsbegrenzung und -regelung des Kernkraftwerkes Unterweser (Deutschland) sowie laut Hersteller /ARE 06/ in verschiedenen Anlagen in der Neutronenflussmessung, der Kernüberwachung und der Stabstellungsüberwachung eingesetzt. Da die Anwendungen des Systems in ausländischen Kernkraftwerken auch im Bereich des Reaktorschutzes und der ESFAS-Funktionen liegen, wurden bei der Systemauslegung besondere Anforderungen an die Zuverlässigkeit, die Fehlervermeidung und die Fehlerbeherrschung gestellt. Zur Erfüllung dieser Forderungen sind laut Hersteller /ARE 06/ beim TELEPERM XS-System folgende Möglichkeiten gegeben:

- Redundante Strukturen
- Fehlererkennung durch Selbstüberwachung
- Entkopplung redundanter Teilsysteme über Lichtwellenleiter
- Verhindern der Fehlerausbreitung durch intelligente Signal-Statusverarbeitung
- Behandlung des Vorrangs zwischen Systemen unterschiedlicher Sicherheitsklassen

Durch eine Trennung in Erfassungs- und Ansteuerebene (d. h. Erfassungsrechner lesen die Gebersignale ein und stellen diese dann allen Redundanzgruppen bereit) soll die Fehlauslösung beim Ausfall einzelner oder mehrerer Geber vermieden werden. In TELEPERM XS werden standardmäßig folgende Architekturen angeboten /ARE 06/:

- Master-Checker-Konfiguration mit parallelgeschalteten, sich gegenseitig überwachenden Verarbeitungseinheiten
- Voter-Konfigurationen mit redundanten Master-Checker-Paaren (2 x (2v2))
- Hot-Standby-Rechnerpaare mit automatischer Umschaltung im Fehlerfall

Die Unabhängigkeit redundanter Teilsysteme soll durch den Einsatz von Lichtwellenleitern für die Busverbindungen sowie durch nachfolgend beschriebene softwaretechnische Maßnahmen realisiert werden. Alle eingehenden Telegramme werden auf Lesbarkeit, gültige Identifikation und Gültigkeit der Daten geprüft. Nur gültige Informationen werden weiter verwendet, wobei aus redundanten Signalen per Mehrheitsauswahl ein validiertes Signal gewonnen oder ggf. ein Ersatzwert aufgeschaltet

wird. So soll laut Hersteller /ARE 06/ selbst bei massiven Störungen ein spezifikationsmäßiges Verhalten sichergestellt werden.

Die Selbstüberwachung erfolgt z. B. durch die zyklische Prüfung der Programmspeicher, die Überwachung der Kommunikation, die Selbstprüfung der Eingänge der Eingabebaugruppen und das automatische Rücklesen der Ausgänge der Ausgabebaugruppen. Außerdem erfolgen eine Überwachung der internen Versorgungsspannung und eine Drahtbruchüberwachung der Ausgangssignale. Durch einen stündlich durchgeführten Selbsttest werden RAM (Random Access Memory; Speicher mit direktem Zugriff), ROM (Read Only Memory; Nur-Lese-Speicher) und die Ausgänge auf mögliche Fehler untersucht. Bei erkannten Fehlern werden die Ausgänge in einen definierten Zustand gebracht, um ein gerichtetes Ausfallverhalten zu erzielen und die Verarbeitungseinheit wird abgeschaltet. /ARE 06/

In Abbildung 2.1 ist eine typische Aufteilung eines TELEPERM XS-Systems anhand des Reaktorschutzsystems für Tianwan 1 und 2 gezeigt. TELEPERM XS-Systeme sind in der Regel aus folgenden Komponenten aufgebaut /ARE 06/:

- Rechner
- Ein-/Ausgabebaugruppen
- Kommunikationsbaugruppen
- Schnittstellen zum Feld
- Baugruppenträger
- Gateway-Schnittstelle

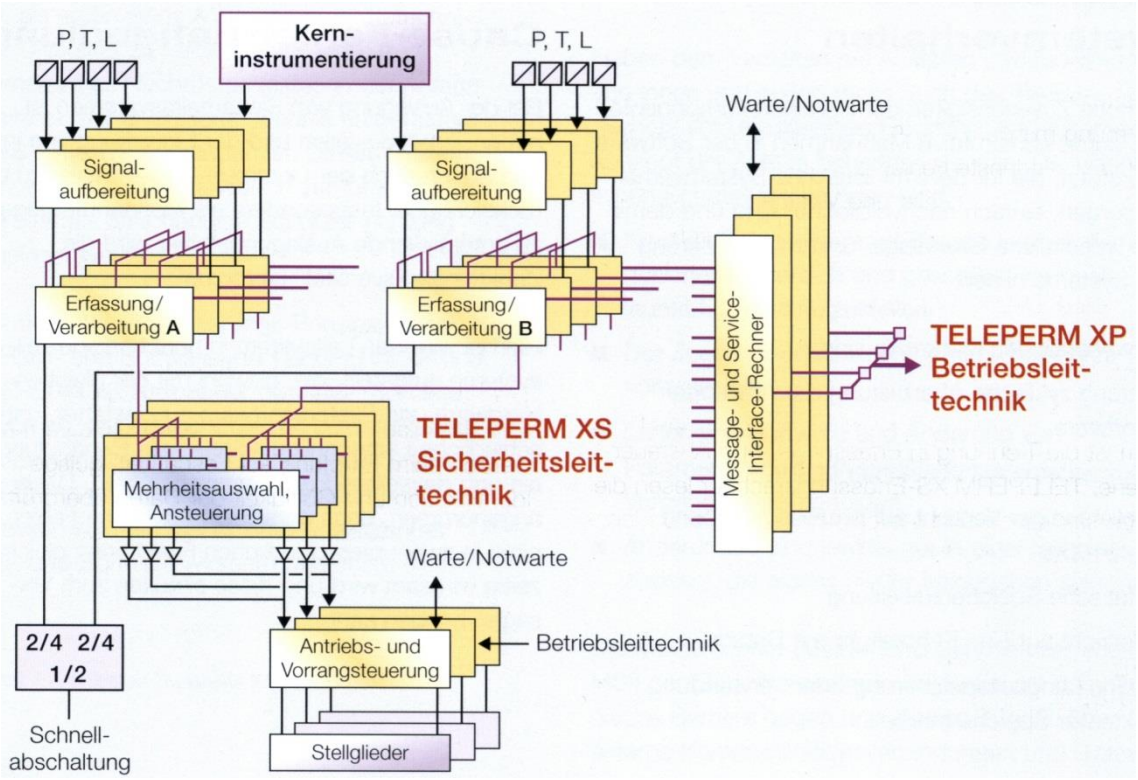

Abb. 2.1 Typische Aufteilung eines TELEPERM XS-Systems in Signalaufbereitung, Erfassungs- und Verarbeitungsebene, Ansteuerrechner und Antriebs-/ Vorrangebene anhand des Reaktorschutzsystems für Tianwan 1 und 2 /ARE 06/

Rechner:

Der strukturelle Aufbau des Rechnersystems besteht aus verteilten, lose gekoppelten Einzelrechnern, die folgende Funktionen erfüllen:

- Erfassungs- und Verarbeitungsrechner
- Ansteuerrechner bzw. Voter
- Melderechner

Die Erfassungsrechner haben die Aufgabe, ankommende Signale aus der Anlage zu erfassen, diese Daten vorab zu bearbeiten und dann an die Verarbeitungsrechner weiterzugeben. In den Verarbeitungsrechnern werden die Signale aufbereitet, gefiltert und logisch verarbeitet. Nach der aufgabenbezogenen Verarbeitung werden die Ausgabesignale über die Ansteuerrechner bzw. Voter ausgegeben und somit über die Ausgabebaugruppen und die Vorrangebene zu den Komponenten ausgegeben. Der Melderechner hat die Aufgabe, Prozesszustände und Störungen zu melden und stellt

somit in jedem Strang das Bindeglied zwischen den im Auslösepfad liegenden Erfassungsrechnern und dem gemeinsamen, strangübergreifenden Netzwerk dar.

Ein-/Ausgabebaugruppen:

Die Ein-/Ausgabebaugruppen dienen zur Erfassung von Standardsignalen. Alle Baugruppen besitzen eine galvanische Trennung zwischen dem Signalkreis und der Schnittstelle zum Systembus, die über Optokoppler realisiert ist. Die Baugruppen sind durchweg mit Mikrocontrollern realisiert, deren Firmware streng zyklisch abläuft (Zykluszeit: typischerweise 50 ms, einstellbar zwischen 5 ms und 1600 ms). Neben der Ein-/Ausgabefunktion wird auch eine zyklische Selbstprüfung der Ein-/Ausgabekanäle und der Verbindung zur Verarbeitungseinheit vorgenommen.

Kommunikationsbaugruppen:

Innerhalb eines Baugruppenträgers erfolgt die Kommunikation über den TELEPERM XS Systembus. Zusätzlich werden der TELEPERM XS PROFIBUS und das TELEPERM XS Ethernet als serielle Bussysteme verwendet. Der TELEPERM XS PROFIBUS basiert auf dem PROFIBUS-Standard DIN/EN 19245 und wird mit einer Datenrate von 12 Mbit/s betrieben. Er kann mit elektrischer oder optischer Verbindung ausgeführt werden und dient zur systeminternen Datenübertragung, also zum Datenaustausch zwischen den einzelnen Rechnern eines TELEPERM XS-Systems. Das TELEPERM XS Ethernet basiert auf dem Standard-Ethernet gemäß IEEE 802.3 und benutzt das LLC (Logical Link Control)-Protokoll, die Übertragungsrate beträgt 10 Mbit/s. Es kann ebenfalls mit elektrischer oder optischer Verbindung ausgeführt werden und dient zum Anschluss externer Rechner mit handelsüblichen Ethernet-Schnittstellen wie z. B. Gateways, WinCC-Bedienstationen, TELEPERM XS Servicegerät oder TELEPERM XS Qualified Display System. Die Verbindungen zwischen unabhängigen Teilsystemen erfolgt mittels Lichtwellenleitern, um eine energetische Entkopplung zu erreichen und elektromagnetische Störungen auszuschließen.

Schnittstellen zum Feld:

Feldsignale mit 0/4 – 20 mA-Schnittstelle werden über die TELEPERM XS Geber- und Aufbereitungsbaugruppen erfasst. Anschließend können die Signale über Trennverstärker oder eine Gateway-Lösung an niedriger klassifizierte Systeme verteilt werden. Sind die Schutz- und Überwachungsfunktionen unmittelbar in der Schaltanlage integriert, wird die Schaltanlage direkt angebunden und die erforderlichen Überwachungs- und Steuerfunktionen werden im TELEPERM XS Rechner umgesetzt. In anderen Fällen ist eine Antriebssteuerebene notwendig. Bei von der Betriebs- und

Sicherheitsleittechnik gemeinsam genutzten Stellgliedern muss zusätzlich der Vorrang zwischen den einzelnen Befehlen sichergestellt werden. Die hierzu vorhandene Antriebssteuer- und Vorrangbaugruppe nimmt diese Funktionen wahr.

Baugruppenträger:
Die einzelnen Baugruppen werden auf sog. Baugruppenträgern aufgebracht. In der Grundausführung verfügt dieser Baugruppenträger über 21 Steckplätze und einen durchgehenden Systembus. Je nach Anforderung werden aber auch andere Konfigurationen, wie beispielsweise geteilte Baugruppenträger mit zwei kleineren, unabhängigen Rechnern und jeweils 10 Steckplätzen mit eigenen Lüftern und eigener Stromversorgung oder eine Mischkonfigurationen unterstützt. Zum Aufbau der TELEPERM XS-Systeme kommen üblicherweise Leittechnikschränke zum Einsatz, die für seismische Beanspruchungen ausgelegt sind und in welche die Baugruppenträger, TELEPERM XS Rechner und alle weiteren Baugruppen eingebaut werden können.

Gateway-Schnittstelle:
Zur Anbindung an die Betriebsleittechnik oder zum Prozessrechner kommt anstatt Einzeldrahtverbindungen eine Gateway-Schnittstelle auf Basis eines Industrie-PCs zum Einsatz. Diese bringt die vom TELEPERM XS-System bereitgestellten Daten in das von der Betriebsleittechnik oder vom Prozessrechner benötigte Datenformat. Vorzugsweise werden industrielle Standard-Bussysteme verwendet, üblicherweise TCP/IP über Industrial Ethernet.

Als zusätzliches Arbeitsmittel steht ein Servicegerät für im Betrieb anfallende Tätigkeiten zur Verfügung. Dieses bietet Unterstützung bei der Fehlerdiagnose, indem die über Funktionspläne spezifizierten Überwachungsmechanismen wie auch die Diagnosemeldungen der Systemsoftware abgefragt und angezeigt werden können. Außerdem können mit Hilfe des Servicegerätes im Betrieb veränderbare Einstellwerte ausgelesen, geändert und verifiziert oder wiederkehrende Prüfungen durchgeführt werden. Das Servicegerät ist in die TELEPERM XS Systemarchitektur eingebunden und kann über das Ethernet und die Melderechner mit den Automatisierungsrechnern verbunden werden. Durch den Zugriff auf die Projektdatenbank kann stets ein komplettes Abbild des Systems auf das Servicegerät geladen werden.

2.3.2 OVATION-System

Das OVATION-System der Firma Emerson (ehemals Westinghouse) wurde für die Kraftwerksindustrie entwickelt. Es wird z. B. in den Kernkraftwerken Temelín 1 und 2 (Tschechische Republik) in der Sicherheitsleittechnik eingesetzt. Die Prozessleittechnik ist skalierbar und erfüllt die Funktionen zur Prozessführung und Überwachung eines Kraftwerkes (Messen, Steuern, Regeln, Überwachen) /EME/. Die eingesetzten Komponenten wie Hardware, Betriebssystem und Software sind kommerziell verfügbare Standardprodukte und keine Sonderentwicklungen. Wesentliche Kernkomponenten von OVATION sind redundant ausgeführt.

Das OVATION-System ist typischerweise aus folgenden Komponenten aufgebaut:

- Controller
- Ein-/Ausgabebaugruppen
- Netzwerk

Controller:
Der Controller führt Ablaufsteuerungen sowie einfache und komplexe Regelstrategien aus und übernimmt Funktionen zur Datenerfassung. Außerdem bildet er die Schnittstelle zum Netzwerk. Die Controller sind mit Intel-Prozessoren ausgerüstet. Eine Regelungsaufgabe besteht aus dem Lesen des Eingangs, dem Ausführen des Regelungsschemas und dem Schreiben des Ausgangs. Ein Regelungsschema besteht aus so genannten Regelmodulen (Control Sheets = Funktionspläne) die aus Standardalgorithmen zusammengesetzt sind. Von einem Controller können dabei mehr als 1000 Regelmodule abgearbeitet werden. Dem Controller können bis zu fünf Zykluszeiten für die Bearbeitung einer Regelungsaufgabe zugewiesen werden, wobei die Zykluszeit zwischen 10 ms und 30 s liegen muss. Der Controller führt auch alle im Zusammenhang mit dem Datenerfassungssystem stehenden Funktionen wie die Grenzwertbildung und die Alarmverarbeitung aus. Der Status aller dem Controller zugewiesenen Punkte wird dabei aktualisiert und dem Netzwerk sekündlich gesendet. Der Controller kann je nach Anforderung mit mehreren Redundanzstufen für wichtige Komponenten wie Netzwerkschnittstelle, Prozessor, Stromversorgung und Ein-/Ausgangsschnittstellen arbeiten, d. h. es können entweder einige benötigte Komponenten oder bei vollständiger Redundanz alle Komponenten mehrfach ausgeführt werden. In der Standard-Hardwarekonfiguration sind der primäre Controller und der Backup-

Controller auf einer passiven Bus-Leiterplatte installiert. Die redundante Stromversorgung wird an diese Bus-Leiterplatte angeschlossen und auf die Controller verteilt. Jeder Controller besteht aus zwei Modulen, von denen ein Modul Prozessor, Speicher, Netzwerk und weitere Netzwerkverbindungen bereitstellt und das andere als Schnittstelle zu lokalen Ein-/Ausgangsbaugruppen und als interne Stromversorgung dient. In vollständig redundanten Controllern sind alle Komponenten (Prozessor, Netzwerkschnittstellen, Stromversorgung, Ein-/Ausgangsschnittstellen) doppelt vorhanden. Jeder der beiden redundanten Controller führt dann dasselbe Applikationsprogramm aus, aber nur einer läuft im Steuermodus. Der im Steuermodus laufende primäre Controller greift auf die Ein-/Ausgangsbaugruppen zu und führt alle Regelungsfunktionen aus. Außerdem überwacht der primäre Controller den Status des Backup-Controllers. Der Backup-Controller läuft im Sicherungs-, Konfigurier- oder Offline-Modus. Im Sicherungsmodus überwacht der Backup-Controller den Status des primären Controllers und pflegt die Daten durch Abfrage des Datenspeichers des primären Controllers. Falls der im Steuermodus laufende primäre Controller einen Fehler aufweist, übernimmt der Backup-Controller automatisch den Steuermodus. Zu dem Konfigurier- und Offline-Modus liegen keinen näheren Informationen vor.

Ein-/Ausgabebaugruppen:

Für das OVATION-System stehen verschiedene Ein-/Ausgabebaugruppen zur Verfügung. Hierzu gehören z. B. für analoge Messungen HART-Eingangsbaugruppen (Highway Addressable Remote Transducer; standardisiertes Kommunikationssystem zum Aufbau industrieller Feldbusse mit der Möglichkeit digitaler Kommunikation mehrerer Teilnehmer über einen gemeinsamen Datenbus) mit einer Auflösung von 14 Bit oder klassische 4 – 20 mA Baugruppen mit einer Auflösung von 13 Bit. Angeschlossene 2-Leiter Messumformer werden aus der Karte heraus gespeist. Alle Kanäle sind galvanisch voneinander getrennt und in Bezug auf Kurzschluss, Fühlerbruch und Messbereichsgrenzwerte vom Leitsystem überwacht. Für den Anschluss weiterer analoger Messgeräte (z. B. Widerstandsthermometer, Thermoelemente, Strom- und Spannungsmessgeräte) stehen Karten mit Auflösungen von 13 oder 14 Bit zur Verfügung. Die Auflösung analoger Ausgänge beträgt 12 Bit bei Standardausführung und 16 Bit bei HART-Baugruppen.

Zur Integration der an das Prozessleitsystem angeschlossenen Feldgeräte können Kommunikationsprotokolle wie HART, FOUNDATION FIELDBUS (digitales, serielles, Zwei-Wege-Kommunikationssystem) und PROFIBUS DP (Process Field Bus Dezentrale Peripherie; Standard für Feldbus-Kommunikation in der Automatisierungstechnik,

verwendet zur Ansteuerung von Sensoren und Aktoren durch eine zentrale Steuerung) verwendet werden. Dabei sind viele der erhältlichen HART-Geräte bereits in der Software von OVATION integriert. Die Handhabung der Software ist im Wesentlichen an der „Microsoft Windows“-Darstellung und -Funktionalität orientiert.

Netzwerk:

Das Netzwerk von OVATION bietet die Möglichkeit mittels Ethernet Kontakt zu allen angeschlossenen Baugruppen herzustellen. Sind mehrere, unabhängig voneinander arbeitende OVATION-Prozessleitsysteme vorgesehen, werden diese über eine Mehrfach-Netzwerk-Struktur (Verbindung der einzelnen Prozessleitsysteme mit dem übergeordneten Netzwerk mittels redundanter Root Switches, Datenaustausch zwischen den einzelnen Prozessleitsystemen über redundante Core Switches, siehe Abbildung 2.2) miteinander verbunden. Ist nur ein OVATION-Prozessleitsystem vorgesehen, sind keine getrennten Netzwerke für die Prozess- und Bedienebene nötig (keine Client-Server-Architektur). Es entfällt somit der Aufwand zur Einrichtung von Netzwerkschnittstellen (Gateways). Das Netzwerk von OVATION kann redundant ausgelegt werden und sowohl Lichtwellenleiter als auch Kupferkabel als Übertragungsmedium nutzen. Zur Anbindung an das betreibereigene LAN (Local Area Network), WAN (Wide Area Network) oder Intranet sind laut Hersteller /EME/ keine kundenspezifischen Gateways oder Schnittstellen erforderlich. Durch das Netzwerkdesign soll laut Hersteller /EME/ die Datenübertragung in Echtzeit ohne Leistungsminderung oder Verzögerungen gewährleistet werden. Das Netzwerk wird gemäß dem Industriestandard IEEE 802.3 mit einer maximalen Datenübertragungsgeschwindigkeit von 100 Mbit/s betrieben.

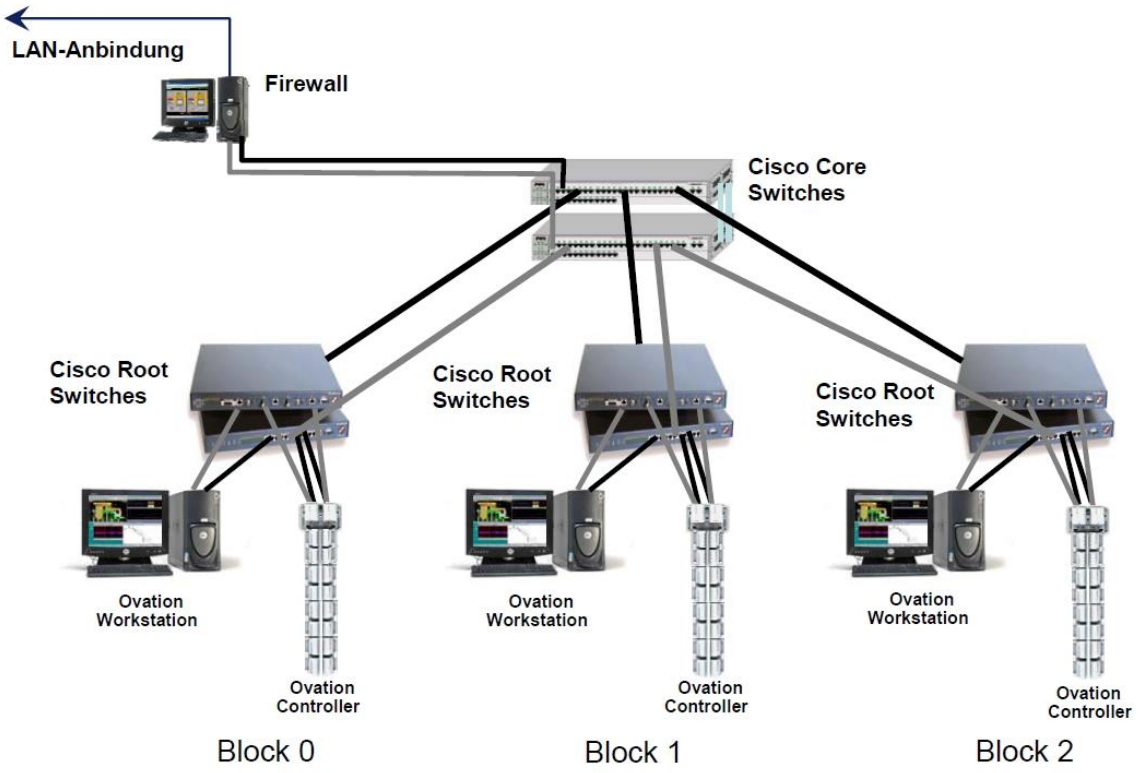

Abb. 2.2 Netzwerkarchitektur für drei Prozessleitsysteme /EME/

Zur Verwaltung des OVATION-Prozessleitsystems steht eine zentrale Engineering-umgebung zur Verfügung. Mit den zugehörigen Werkzeugen hat der Anwender Zugriff auf die Projektierungsdaten und somit die Möglichkeit zur Konfiguration der Knoten, Regelungen, Ablaufsteuerungen und Prozessbilder. Die Engineeringumgebung beinhaltet eine zentrale Systemdatenbank. Des Weiteren ist eine individuell erweiterbare Bibliothek mit vordefinierten Algorithmen zur Erstellung von Regel- und Steuerungsfunktionen vorhanden. Control Sheets (Funktionspläne) können durch Verknüpfung verschiedener Algorithmen erstellt und durch Eingabe von Analog- bzw. Binärwerten durch eine Simulation geprüft werden. Außerdem ist eine Systemdiagnose mit verschiedenen Diagnosefunktionen zur Erfassung des aktuellen Systemzustandes (z. B. Verfügbarkeit verschiedener Aggregate, Laufzeitmeldungen für Aktoren, Sensorüberwachung, Fühlerbruch, Kurzschluss) vorhanden. /EME/

Die Bedien- und Beobachtungsebene ist in einer hierarchischen Systematik von Anlagen- oder Fließbildern dargestellt, die sekündlich aktualisiert werden. Bei Störungsmeldungen wird der Bediener interaktiv zur entsprechenden Grafik mit detaillierten Informationen geführt. Zur Verdeutlichung der Priorität ist bei manchen Grafiken auch ein automatischer Aufruf möglich. Zur Analyse von Daten (historische Mess-

größen oder aktuelle Prozesswerte) können Kurvenbilder dargestellt werden. Ein Meldesystem mit Routinen zur Alarmanalyse und Meldeprioritäten sollen den Bediener über den Sicherheitszustand der Anlage informieren und Meldefluten vermeiden. /EME/

Zur Prozessdatenarchivierung und Protokollierung erfolgt mittels eines Scanners eine sekündliche Prüfung der Prozesspunkte auf Status und Änderung. Ändert sich ein Wert um einen vorher vom Anwender festgelegten Prozentsatz wird dieser Wert mit dem zugehörigen Zeitstempel und Status abgespeichert. Optional besteht auch die Möglichkeit der redundanten Ausführung der Prozessdatenarchivierung und Protokollierung mit zwei voneinander unabhängigen Scannern. Jeder Scanner besitzt die Möglichkeit der automatischen Zwischenspeicherung bei Ausfall der Datenbankanbindung. /EME/

2.3.3 SYMPHONY MELODY-System

Das System SYMPHONY MELODY der Firma ABB bietet laut Hersteller durch seinen modularen, flexiblen Aufbau die Möglichkeit, sich an unterschiedlichste Anlagentypen und -größen anzupassen /ABB 03/. Es besteht sowohl die Möglichkeit eines dezentralen Hutschienenaufbaus als auch der schrankorientierten Lösung, wobei beide Aufbautechniken untereinander kompatibel und bei Bedarf kombinierbar sind. Die Möglichkeit des redundanten Aufbaus für Versorgung, Kommunikation und Baugruppen ist gegeben /ABB 03/. SYMPHONY MELODY wird z. B. in den Kernkraftwerken Isar und Gundremmingen für Leittechnik-Funktionen der Kategorien B und C eingesetzt.

Die SYMPHONY MELODY Control-Stationen bestehen aus modularen Controllern und einer projektierbaren Anzahl von Prozessinterfacebaugruppen. Diese Control-Stationen arbeiten autark und erfüllen alle Funktionen für Messwerterfassung und -aufbereitung, Überwachung, Regelung und Steuerung von Aggregaten und Anlagen. Die SYMPHONY MELODY Control-Stationen sind typischerweise aus folgenden Komponenten aufgebaut:

- Controller
- Prozessinterfacebaugruppen
- Netzwerk

Controller:

Das Kernstück der SYMPHONY MELODY Control-Stationen bilden die AC 870P oder CMC70 Controller. Die Controller verarbeiten die analogen und/oder digitalen Ein-/Ausgangssignale und übernehmen Aufgaben der Überwachung, Regelung und Steuerung sowie komplexe Algorithmen wie z. B. Ablaufsteuerungen. Über Diagnoseroutinen wird zyklisch die ordnungsgemäße Funktion der Hard- und Firmware überprüft, im Fehlerfall wird eine Meldung generiert und gemeldet. Es besteht die Möglichkeit zu einem redundanten Aufbau, wobei dann auf zwei Baugruppen ständig eine parallele Verarbeitung stattfindet. Dadurch kann im Fehlerfall die redundante Baugruppe die Verarbeitung mit den aktuellen Algorithmen und Prozessdaten unterbrechungsfrei übernehmen. Der Controller bietet Kommunikation über eine Vielzahl von Schnittstellen (unter anderem integrierte, standardisierte, redundante PROFIBUS-Schnittstelle und standardisierte FDT/DTM-Schnittstelle (Field Device Tool/Device Type Manager; herstellerübergreifendes Konzept zur Parametrierung von Feldgeräten verschiedener Hersteller mit nur einem Programm)) zur Integration von Feldgeräten ohne Zusatz-Tools, wobei Automatisierungsschnittstellen immer redundant ausgelegt sind. Die Controller bieten laut Hersteller /ABB 03/ eine hohe Datensicherheit, indem die Firmware in Flash Memory, Konfigurationsdaten in doppelt batteriegepufferten RAMs und Fabrikationsdaten in NVRAMs (Non Volatile Random Access Memory; nicht flüchtiger Datenspeicher basierend auf RAM-Speichern, dessen Dateninhalt ohne externe Energieversorgung erhalten bleibt) hinterlegt werden.

Prozessinterfacebaugruppen:

Wesentliche Komponenten sind die Ein-/Ausgabebaugruppen und das Feldbussystem, die zusammen als Prozessinterface für die SYMPHONY MELODY Controller arbeiten. Die Ein-/Ausgabebaugruppen verarbeiten alle Eingangs- und Ausgangssignale von Feldgeräten und leiten diese dann mit einem Zeitstempel (Genauigkeit 1 ms) an den Controller weiter. Außerdem sind Funktionen wie Überwachung, Filterung und HART-Kommunikation direkt auf den Ein-/Ausgabebaugruppen implementiert.

Das serielle Feldbussystem ermöglicht eine zentrale oder verteilte Anordnung von Ein-/Ausgabebaugruppen. Es stehen verschiedene Ein-/Ausgabebaugruppen zur Verfügung, wie z. B. Analogeingabe, Temperatureingabe, Frequenzeingabe, Analogausgabe, Binäreingabe, Binärausgabe, Regler-/Steuerungs-Ausgaben und serielle Kommunikationsschnittstellen. Die einzelnen Baugruppen innerhalb eines Schrankes

werden durch eine modular aufgebaute Versorgung gespeist, die wahlweise auch redundant ausgeführt werden kann.

Netzwerk:

Das SYMPHONY MELODY-System bietet ein redundantes, serielles Netzwerk, wodurch eine systemweite Kommunikation sichergestellt werden soll. Das Netzwerk ist hierarchisch und funktionell unterteilt. Durch die hierarchische Staffelung in Stationen, Anlagenbereiche und Gesamtanlage erfolgt die Anpassung des Netzwerks an die Anlagengröße. Die hierarchische Gruppierung soll einen maximalen Datentransfer zwischen einzelnen Control-Stationen ermöglichen. Funktional wird das Netzwerk in Control- und Operation-Busse unterteilt. Die funktionale Verbindung zwischen mehreren Control-Stationen erfolgt über den Control-Bus (Cnet). Laut Hersteller /ABB 03/ ist ein systemweiter Signalaustausch einer Control-Station mit anderen Control-Stationen, dem zentralen Engineering-Tool sowie Bedien- und Management-Systemen unter Echtzeit-Bedingungen möglich. Die Kommunikation zwischen den Control-Stationen und den Prozessinterfacebaugruppen erfolgt über den redundanten seriellen Feldbus (Fnet) oder über den integrierten PROFIBUS. Alle Operationen zur Prozessvisualisierung, Konfiguration und Wartung des Systems werden über den Operation-Bus (Onet) rangiert. Durch diese Aufgabenteilung soll z. B. die Automatisierung nicht durch eine eventuell auftretende umfangreiche Anzahl von Meldungen behindert werden. Somit werden verschiedene Busse zur Kommunikation der Teilnehmer untereinander zur Verfügung gestellt:

- Cnet: Kommunikation zu anderen Control Stationen
- Onet: Kommunikation zur Process Portal Bedienstation und zum Composer für die Konfiguration und den Service
- Fnet: Kommunikation zu Ein-/Ausgabebaugruppen
- PROFIBUS DP: Kommunikation zu intelligenten Feldgeräten

Busverbindungen zwischen dem Messwert (Signal-Quelle) und allen nachfolgenden Verarbeitungsfunktionen (Signal-Senken) werden automatisch im gesamten System aufgebaut. Für jede aufgebaute Verbindung wird das aktive Signal zyklisch und spontan von jeder Signal-Quelle zur Signal-Senke übertragen.

Das Composer Engineering Tool soll die Konfiguration, Dokumentation, Inbetriebnahme und Wartung von Systemen auf der Basis von SYMPHONY MELODY Control-

Stationen ermöglichen. Durch Nutzung der Client-Server-Architektur können Mehrplatzsysteme mit Systemvernetzung realisiert werden. Das Composer Engineering Tool verfügt über ein Datenbankmanagementsystem zur Sicherstellung der Vollständigkeit aller Anlagendaten. Zur Projektierung von gewünschten Applikationen ist eine Bibliothek mit getesteten und laut Hersteller betriebsbewährten Funktionsblöcken verfügbar.

Das Mensch-Maschine-Interface Maestro UX soll die Überwachung, Steuerung und Optimierung des Prozesses sowie die Fehlerbeseitigung durch bedienerbezogene Merkmale und Funktionen erleichtern. Kundenspezifische Grafikbilder, Alarmübersichten und aktuelle oder historische Trenddarstellungen sollen einen schnellen Zugriff auf Prozessstatus und Bedieninformationen erlauben.

2.3.4 HIMAX-System

Das System HIMAX wird z. B. im Kernkraftwerk Gundremmingen für Leittechnik-Funktionen der Kategorie B eingesetzt. Das System bietet laut dem Hersteller HIMA /HIM/ eine flexible Plattform für sicherheitskritische Anwendungen, die kontinuierlich laufen müssen. Es basiert auf der XMR-Architektur, wobei XMR für „x-fach modulare Redundanz“ steht (x kann jeden Wert zwischen 1 und 4 annehmen). Das System kann laut Hersteller an verschiedenste Anforderungen (Anlagengröße, Reaktionszeit, Fehlertoleranz) angepasst werden und eignet sich für zentrale und dezentrale Anwendungen. Durch den modularen Aufbau, bei dem jedes Modul ein eigenes Gehäuse besitzt und mit EMV-Schutz (Elektromagnetische Verträglichkeit), mechanischem Schutz und einer Schutzbeschichtung versehen ist, soll der Schutz gegen Umgebungseinflüsse gegeben werden. Laut /HIM 10/ ermöglichen die Trennung zwischen Modul- und Anschlussebene, die automatische Hardwareerkennung, die Codierung zum Schutz vor Vertauschen und die Möglichkeit des Modulwechsels ohne Lösen der Feldverkabelung eine schnelle und einfache Installation. Das HIMAX-System bietet die Möglichkeit zur Nutzung von bis zu 4 Prozessormodulen (identische Prozessoren), die auf zwei Racks verteilt werden können. Diese beiden Racks können physisch getrennt voneinander installiert werden. Außerdem besteht die Möglichkeit der redundanten bzw. mehrfach redundanten Auslegung der Ein-/Ausgabemodule und die Möglichkeit der räumlichen Trennung von redundanten Komponenten. Über eine Eigendiagnose wird das HIMAX-System ständig auf seine Funktionsfähigkeit überprüft. Dabei wird beispielsweise getestet, ob alle Redundanzen zur Verfügung stehen, der

Systembus einwandfrei arbeitet, ein interner Fehler im System erkannt wurde oder ein Fehler im Feld vorliegt. Zur Gewährleistung der kontinuierlichen Operation können Soft- und Hardware während des Betriebes geändert, erweitert und gewartet werden. Die Änderung von Applikationsprogrammen selbst bei einkanaligen Modulen und das Upgrade vom Betriebssystem können ebenfalls während des Betriebes erfolgen. Das HIMAX-System ist typischerweise aus folgenden Komponenten aufgebaut:

- Systembusmodule
- Prozessormodule
- Kommunikationsmodule
- Ein-/Ausgangsmodule

Systembusmodule:

Das Systembusmodul des HIMAX-Systems organisiert die Kommunikation aller Module auf einer Base Plate, dem Basisträger auf dem alle Module montiert werden. Je nach Bedarf können bis zu zwei Systembusmodule auf einer Base Plate untergebracht werden. Die Übertragungsgeschwindigkeit auf dem Systembus beträgt 1 Gbit/s. Innerhalb der Base Plates existiert eine sternförmige Kommunikation zwischen den Modulen eines Systems. Das hat laut Hersteller /HIM/ den Vorteil, dass jedes Modul eines Systems mit jedem anderen Modul direkt kommunizieren kann, eine fehlerhafte Verbindung zu einem Modul aber keinen Einfluss auf die anderen Verbindungen hat. Werden zwei Systembusmodule verwendet, kann die Kommunikation zu dem Modul mit der fehlerhaften Verbindung über den redundanten Systembus aufrechterhalten werden /HIM/. Die Systembusmodule stellen auch die Kommunikation zwischen den Base Plates her. Zur Vernetzung verschiedener Base Plates dienen Ethernet-Ports, mit denen eine Distanz von bis zu 100 m mit Kupferkabeln überbrückt werden kann. Über spezielle Medienkonverter kann man die Daten auf Lichtwellenleiter umsetzen, mit denen dann eine Distanz von bis zu 1,5 km überbrückt werden kann.

Prozessormodule:

Das Prozessormodul dient der Abarbeitung des Anwenderprogramms und der Kommunikation mit den Ein-/Ausgabemodulen und externen Einheiten. Das Verhalten des Moduls kann beim Neustart (nicht im laufenden Betrieb) zwischen drei Optionen umgeschaltet werden. Die Option „Init“ lässt das Prozessormodul ausschließlich mit Fabrikeinstellungen für die Ethernet-Ports und das User Management starten. Bei Auswahl der Option „Stop“ lädt das Modul die Konfiguration aus dem Speicher, startet

jedoch nicht. Auch die Einstellungen für die Ethernet-Ports und das User Management werden aus dem Speicher genommen. Die Option „Run“ lädt die Konfiguration aus dem Speicher und startet das Anwenderprogramm.

Kommunikationsmodule:

Die Kommunikationsmodule dienen der Anbindung des HIMAX-Systems an Fremdsysteme. Dazu besitzt jedes Modul zwei Feldbus-Schnittstellen, vier Ethernet-Ports und kann bis zu sechs Protokolle verarbeiten.

Ein-/Ausgangsmodule:

Im HIMAX-System können verschiedene Ein-/Ausgangsmodule verwendet werden, wobei die Signalaufbereitung aller Feldsignale direkt in den Ein-/Ausgangsmodulen stattfindet. Dadurch können z. B. Analogwerte in der gleichen Zeit bearbeitet werden wie Digitalwerte. Es gibt verschiedene digitale Eingangsmodule mit der Möglichkeit der Auswertung von bis zu 16, 32 oder 64 digitalen Eingangssignalen, mit oder ohne Möglichkeit der schnellen Aufzeichnung von Ereignissen. Die analogen Eingangsmodule sind mit 32 Stromeingängen und einer kurzschlussfesten Speisung je Eingang ausgestattet, wiederum mit oder ohne Möglichkeit der schnellen Ereignisaufzeichnung. Das Zählermodul ist mit 24 Eingängen ausgestattet, die Frequenzen zwischen 0 und 20 kHz messen können. Die digitalen Ausgangsmodule besitzen 12, 24 oder 32 digitale Ausgänge und können einzelne Kanäle bei Überlast abschalten und zyklisch wieder aktivieren. Außerdem ist in den Ausgangsmodulen eine kanalweise Diagnose für Leitungsbruch und Leitungsschluss integriert. Das Relaismodul besitzt 12 potentialfreie Relaisausgänge für 250 V AC/DC. Sowohl die Schaltspiele als auch der dabei fließende Strom werden überwacht. Das analoge Ausgangsmodul ist mit 16 Stromausgängen bei einkanaliger Verschaltung und acht Stromausgängen bei redundanter Verschaltung ausgestattet, welche sich zum Anschluss von ohmschen, induktiven und kapazitiven Lasten eignen.

Auf den Base Plates werden auch so genannte Connector Boards zur Anbindung von Modulen an das Feld montiert. Durch die Aufteilung in eine Modulebene und eine Anschlussebene ist ein Lösen der Feldverdrahtung beim Austausch von Modulen nicht notwendig. Connector Boards können im laufenden Betrieb bestückt werden.

Für den Aufbau von sicherheitsgerichteten, verteilten Applikationen verwendet das HIMAX-System Netzwerktechnologie nach dem Ethernet-Standard mit einer Übertragungsrate von 100 Mbit/s. Jedes Prozessormodul und jedes Kommunikationsmodul

kann dabei seine eigenen Ethernet Einstellungen (z. B. IP-Adresse, Netzwerkmaske, Routen und Standardgateway) haben. Der Telegramminhalt sicherheitsgerichteter Kommunikation wird in den Prozessormodulen erstellt. Die physikalische Anbindung erfolgt über die Prozessormodule oder die Kommunikationsmodule. Die sicherheitsgerichtete Kommunikation kann sich ein Netzwerk mit anderen Protokollen teilen, wobei laut HIMA die Sicherheit nicht beeinflusst wird /HIM/. Zur Erhöhung der Verfügbarkeit ist auch ein redundanter Aufbau möglich.

Das Engineering Tool SILworX dient zur Konfiguration, Programmierung und Diagnose eines HIMAX-Systems. Das Andocken eines PCs mit SILworX ist an beliebigen Stellen im Netzwerk möglich. Es können bis zu 255 Steuerungen in einem Projekt bearbeitet werden. Die Konfiguration der Hardware wird von einem grafischen Editor unterstützt. Syntaktische Fehler bei der Programmierung werden erkannt und angezeigt und Parametrierungsfehler werden automatisch gemeldet. Die gesamte Ein-/Ausgabeebene kann ohne Anwenderprogramm getestet werden. So kann die komplette Verdrahtung der Anlage bereits getestet werden, während die Erstellung des Anwenderprogramms davon unabhängig zur gleichen Zeit durchgeführt werden kann. Durch die zur Verfügung stehende Offline-Simulation kann man Programme im Vorfeld ohne angeschlossene Steuerungen testen. Für Inbetriebnahme und Wartung stehen Online-Tests zur Verfügung, um aktuelle Werte und Zustände anzeigen zu lassen. Außerdem stehen Diagnosemöglichkeiten für Hardware und Kommunikation bereit.

2.3.5 SPINLINE 3-System

Das SPINLINE 3-System der Firma Rolls Royce, welches gemeinsam von Areva NP, EdF (Electricité de France) und DS&S (Data Systems and Solutions) entwickelt wurde, ist ein programmierbares oder rechnerbasiertes Leittechniksystem. Laut Hersteller /SCH 01/ werden von dem System alle sicherheitsrelevanten Funktionen abgedeckt, von der Messwerterfassung bis hin zur Steuerung der Stellglieder. Das System wird z. B. im Reaktorschutzsystem des Kernkraftwerkes Dukovany 3 (Tschechische Republik) eingesetzt.

Hardware:

Die Hardware des SPINLINE 3-Systems wurde speziell für den Einsatz in der Sicherheitsleittechnik von Kernkraftwerken entwickelt und ist mit einem Motorola 68040 32-Bit Prozessor mit einer Taktrate von 25 MHz und 2 MByte RAM ausgestattet. Die

Ein-/Ausgabekarten sind zuständig für die Ein- und Ausgabe von binären und analogen Daten, wie beispielsweise Daten aus der Neutroneninstrumentierung, der thermodynamischen Instrumentierung oder der Stellglied-Ansteuerung. Die Standard-Kommunikation erfolgt über ein internes Netzwerk im Token-Ring-Verfahren. Die Karten signalisieren Ausfälle mit LEDs und einer Meldung zum Prozessor. Bei Kartenausfällen werden die Ausgänge innerhalb eines vordefinierten Zeitintervalls der Ausgabekarten auf sicherheitsgerichtete, vordefinierte Werte gesetzt. Die Eingangskarten haben einen zusätzlichen Testeingang zum Anlegen eines externen Testsignals für jeden Prozessinput zur Durchführung von wiederkehrenden Prüfungen. Außerdem sind Schutzmaßnahmen gegen das Einstecken falscher Karten beim Austausch vorgesehen.

Software:

Die Software ist unterteilt in drei verschiedene Teile, die Systemsoftware, die Anwendersoftware und das Werkzeug-Set. Die Systemsoftware wird benötigt, um die Anwendersoftware ablauffähig zu machen, die Kommunikation zwischen dem Prozessor und den Ein-/Ausgabekarten zu bewerkstelligen und Aufgaben zur Selbstüberwachung wahrzunehmen. Die Systemsoftware erfüllt die Funktionen der Initialisierung und des Selbsttests, bildet die Schnittstellen zu den Ein-/Ausgabekarten und sorgt für die Steuerung und Überwachung der Zyklusdauer. Die Anwendersoftware implementiert die zu verwirklichende Funktionalität. Sie umfasst kundenspezifische Funktionspläne, deren Code mit Hilfe des Werkzeug-Sets automatisch erstellt wird. Das Werkzeug-Set ermöglicht die Beschreibung der Leittechnik-Architektur und der Hardwarestruktur des zu erstellenden Systems. Diese Beschreibung dient als Datenbasis zur automatischen Systemsoftwaregenerierung, der Netzwerkgenerierung (Netzwerk-Konfigurierung festlegen) und der Konfigurierung der Kommunikation (Telegramme im Netzwerk organisieren). Zur Erstellung der Anwendersoftware wird ein graphischer Editor verwendet, der das Erstellen der Funktionspläne ermöglicht. Der gesamte Code und die dazugehörige Dokumentation werden automatisch generiert. Anschließend wird der Code kompiliert und ins Zielsystem geladen.

Werkzeuge zur Bedienung und Wartung:

Mit Hilfe der Automatic Testing Unit können die Sicherheitssysteme online während des Betriebes oder offline während der Stillstandzeiten getestet werden. Dafür können bestimmte Testreihen definiert werden. Während des Tests werden die Daten graphisch dargestellt und die Testergebnisse können analysiert und archiviert werden.

Die Monitoring and Maintenance Unit dient zur kontinuierlichen Beobachtung, ob bestimmte Ergebnisse und Ausfälle aufgetreten sind. Es wird z. B. geprüft auf Ausfälle von Sensoren, Boards oder Netzteilen, offene Schranktüren oder Inkonsistenzen zwischen Signalen und Parametern redundanter Stränge. Mit der Parameter Management Unit können Parameter und Werte einzeln oder in Gruppen überprüft und gesetzt werden. Dies geschieht über ein gesichertes Protokoll, wobei die gewünschten Wertebereiche vorgegeben werden können.

2.3.6 MELTAC-System

Das MELTAC-System (MELTAC: Mitsubishi Electric Total Advanced Controller) der Firma Mitsubishi kommt z. B. im Kernkraftwerk Tomari 3 (Japan) im Reaktorschutzsystem und im ESFAS zum Einsatz. Es ist ein programmierbares oder rechnerbasiertes Leittechniksystem, welches laut Hersteller /MIT 07/ durch eine modulare Architektur vielfältige Konfigurationen erlaubt und die Möglichkeit bis zu 4-facher Redundanz bietet. Zur Übertragung von Daten von Geräten vor Ort zu den Leittechnikräumen und der Warte sowie zwischen den eingesetzten Leittechniksystemen werden Datenübertragungsnetzwerke im Multiplexverfahren genutzt. Das MELTAC-System ist typischerweise aus folgenden Komponenten aufgebaut:

- Controller (Steuereinheit)
- Sicherheitsbildschirm-Konsole
- Sicherheitsbildschirm-Prozessor
- Regelungsnetzwerk
- Datenverbindung
- Engineering Tool
- Wartungsnetzwerk

Der Controller besteht aus einem Prozessor und einem oder zwei Untersystemen. Jedes Untersystem ist aus mehreren Modulen aufgebaut, z. B. Spannungsversorgungs-, Regelungsnetzwerk-, Systemmanagement- und Bus-Master-Modulen. Die Kommunikation der Untersysteme mit dem Regelungsnetzwerk erfolgt über optische Signale. Des Weiteren können an den Controller mehrere Module zur Ein-/ Ausgabe angeschlossen werden. Der Controller ist mit einem 32-Bit Mikroprozessor

mit SRAM (Static Random Access Memory; flüchtiger, statischer Speicher mit der Möglichkeit beliebig langer Datenspeicherung bei vorhandener Betriebsspannung) und Cache ausgestattet. Mit ultraviolettem Licht löschbare PROMs (Programmable Read Only Memory; programmierbarer Nur-Lese-Speicher) werden zum Speichern der Basissoftware und Flash-EEPROMs (Electrically Erasable Programmable Read Only Memory; elektrisch löschbarer programmierbarer Nur-Lese-Speicher; nichtflüchtiger, elektronischer Speicherbaustein) zum Speichern der Anwendungssoftware (logische Verknüpfungen, Sollwerte und Parameter) genutzt. Interne Operationen und Datenübertragungen werden über Module wie das Bus-Master-Modul und das Regelungsnetzwerk-Modul mittels des Standards Futurebus+ (Bussystem zur Datenübertragung mit Datenbus-Breiten zwischen 32 und 256 Bit und Adressbus-Breiten von 32 und 64 Bit) durchgeführt.

Die von der Systemsoftware bearbeiteten Prozesse laufen deterministisch ab, was durch folgende Design-Prinzipien erreicht werden soll: Die Bearbeitung erfolgt zyklisch und es wird immer nur eine Aufgabe abgearbeitet (Single Task Processing), Interrupts werden nur für Fehlerbehandlungen und nicht für andere Aufgaben genutzt. Die Anwendungssoftware ist für funktionelle Algorithmen entworfen worden, indem simple Logikbefehle wie UND, ODER, NICHT kombiniert werden. Durch Kombination von graphischen Blockdiagrammen, welche Funktionsmodule repräsentieren, können vom Anwender Anwendungsprogramme erstellt werden, die automatisch in Ausführungsdaten umgewandelt werden. Diese werden direkt durch die Basissoftware ausgeführt. Die Basissoftware führt ihre Prozesse sequentiell entsprechend den Ausführungsdaten aus.

Das MELTAC-System sieht drei verschiedene Systemkonfigurationen vor. Die gewählte Konfiguration hängt von den Anforderungen des Anwenders ab. Jede der Konfigurationen kann als Sicherheitssystem genutzt werden /NUR 09/:

- Einzel-Controller-Konfiguration
  Der Controller beinhaltet ein Untersystem, das im Steuermodus arbeitet, d. h. das Untersystem steuert die Ausgänge zu den Kraftwerkskomponenten.
- Redundante-Parallele-Controller-Konfiguration
  Diese Konfiguration nutzt zwei Untersysteme, welche beide jeweils im Steuermodus arbeiten.

- Redundante-Standby-Controller-Konfiguration
  Diese Konfiguration beinhaltet ebenfalls zwei Untersysteme, von denen eines im Steuermodus arbeitet und das andere im Standby-Modus ist. Das Untersystem im Standby-Modus überwacht den Betrieb des Untersystems im Steuermodus einschließlich der Speicherzustände. Fällt das im Steuermodus betriebene Untersystem aus, wird das Untersystem im Standby-Modus automatisch in den Steuermodus geschaltet.

2.3.7 Siemens Simatic S7 Baugruppen und Software Step 7

Siemens S7 Baugruppen sind vielfach bei der Steuerung moderner Automatisierungslösungen im Einsatz. Mithilfe des Simatic Systems können verschiedene Aufgaben erfüllt werden. Hierzu gehören u. a. /SIE 06/:

- Kopplung von Automatisierungssystemen sowie einfacher Sensoren, Aktoren und Rechner
- Prozess- und Feldkommunikation der Automatisierungssysteme incl. Sensoren und Aktoren
- Datenkommunikation zwischen Automatisierungssystemen

Von den speicherprogrammierbaren Steuerungen der Simatic S7-Familie werden in den Anlagen hauptsächlich die Steuerungen Simatic S7-300 beziehungsweise S7-400 eingesetzt, welche eine CPU (Central Processing Unit) besitzen. Die moderneren Steuerungen S7-400 verfügen über zusätzliche Möglichkeiten, die den S7-300 noch nicht zur Verfügung stehen. So ist es bei der S7-400 im Gegensatz zu S7-300 beispielsweise möglich, die Baugruppen unter Spannung zu stecken und zu ziehen.

Im Folgenden werden die speicherprogrammierbaren Steuerungen S7-400 beschrieben. Für diese gibt es unterschiedliche Baugruppenträger und vier unterschiedliche Typen von Baugruppen /SIE 11/:

- Baugruppen für die Stromversorgung
- Digitalbaugruppen
- Analogbaugruppen
- Anschaltungsbaugruppen

Die Baugruppen der S7-Reihe können mit Hilfe der Software Step 7 programmiert werden. Es ist auch möglich Parametrierungen im laufenden Anlagenbetrieb zu ändern. Bei parametrierbaren Baugruppen können Diagnosemeldungen und Alarme ausgegeben werden. Die Freigabe dieser Meldungen muss mit der Software Step 7 programmiert werden. Darüber hinaus können die Baugruppen auch über ein Bussystem (PROFIBUS) programmiert werden und Diagnosedateien ausgelesen werden. Hierzu wird eine spezielle Anschlussbaugruppe (IM 467/IM 467 FO) benötigt.

Die Diagnosemöglichkeiten sind sehr umfangreich und detailliert. Die Diagnosedaten einer Baugruppe können bis zu 43 Bytes lang sein und stehen in den beiden Datensätzen 0 und 1. Der Datensatz 0 enthält 4 Bytes Diagnosedaten, die den aktuellen Zustand eines Automatisierungssystems beschreiben. Der Datensatz 1 enthält die 4 Bytes Diagnosedaten, die auch im Datensatz 0 stehen und bis zu 39 Bytes baugruppenspezifische Diagnosedaten.

Die Baugruppen können in ein sog. TIA-System (Totally Integrated Animation) integriert werden /SIE 11a/. Mit Hilfe eines solchen TIA-Systems werden alle Ebenen eines Produktionsprozesses (Unternehmensleitebene, Betriebsführungsebene, Steuerungsebene, Feldebene) in einem Konzept zusammengefasst (siehe Abbildung 2.3). Das ganze System bestehend aus verschiedenen automatisierungstechnischen Einzelkomponenten, Software-Tools und dazugehörigen Services wird einheitlich betrachtet, was zu Vereinfachung und Kosteneinsparung führt. Das ganze System kann zum Beispiel über Windows-Rechner gesteuert werden.

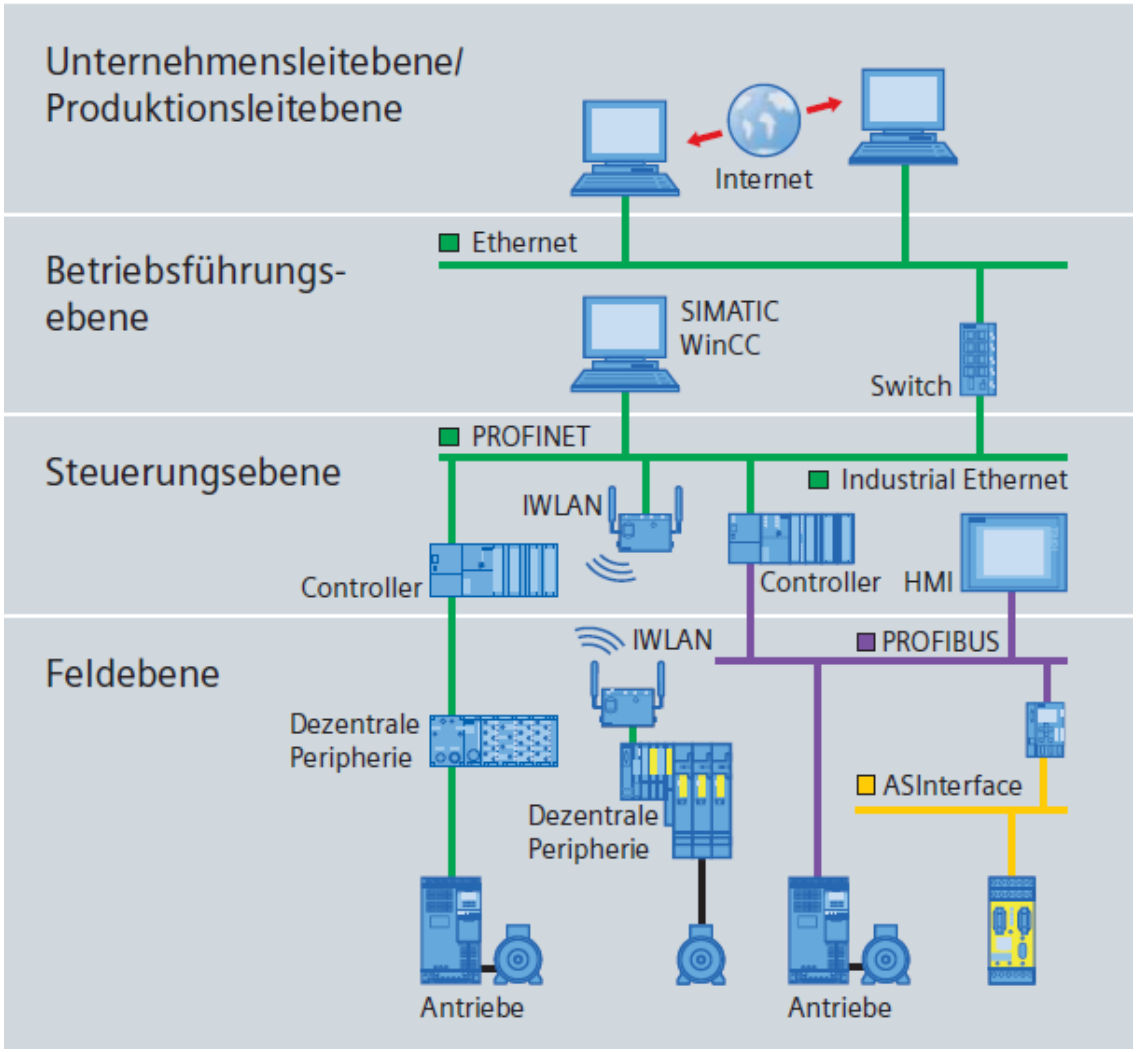

Abb. 2.3 TIA Prinzipbild /SIE 11a/

2.3.8 TELEPERM XP-System

Das Leittechniksystem TELEPERM XP der Firma Areva/Siemens wird in vielen kerntechnischen Anlagen im betrieblichen Teil eingesetzt. Darüber hinaus findet es breite Anwendung in konventionellen Kraftwerken. TELEPERM XP hat eine flexible Systemstruktur, die auf die Anlage angepasst werden kann. /SIE 02/

TELEPERM XP besteht aus folgenden Untersystemen /SIE 02/:

- AS 620 Automatisierungssystem
- OM 650 Prozesssteuerungs- und Managementsystem
- ES 680 Engineering-System

- DS 670 Diagnosesystem
- Kommunikations- und Bussystem

Die einzelnen Untersysteme werden im Folgenden kurz beschrieben.

AS 620

Das AS 620 Automatisierungssystem übernimmt grundlegende Aufgaben. Es nimmt Mess- und Zustandswerte von Feldgeräten auf, übernimmt Kontrollfunktionen und übermittelt aus den Kontrollfunktionen stammende Befehle an die Feldgeräte. Für verschiedene Anwendungsbereiche (Allgemeine Automatisierung, Sicherheitssysteme (konventionell), Turbine) gibt es spezielle Versionen des AS 620. Darüber hinaus ist das AS 620 die Schnittstelle zu anderen TELEPERM XP-Untersystemen. /SIE 02/

OM 650

Das OM 650 Prozesssteuerungs- und Managementsystem dient zur Implementierung einer Mensch-Maschine-Schnittstelle. Über das OM 650 werden Prozesse überwacht und gesteuert. Das OM 650 kann an die Größe der Anlage angepasst werden. /SIE 02/

ES 680

Das ES 680 ist das sogenannte Engineering-System und wird zur Konfiguration der vorhandenen Untersysteme verwendet. Mit dem ES 680 kann sowohl Software (Automatisierungs-, Prozesssteuerungs- und Informationssoftware) als auch die Kommunikation zwischen den Untersystemen sowie die Hardware des Leittechniksystems konfiguriert werden. Eine Option ist hier die sogenannte web4txp Technik. Mit Hilfe dieser Technik ist es möglich weltweit auf das TELEPERM XP-System zuzugreifen. /SIE 02/

DS 670

Das Diagnosesystem DS 670 verwendet UNIX PCs als Systemplattform. Das DS 670 dient der Schichtmannschaft zur Überwachung, zur Durchführung von Testfunktionen und zur Ermittlung detaillierter Informationen über den Status des Prozessleitsystems und ggf. zur Fehleranalyse. Es können sowohl automatische als auch dialogbasierte Diagnosen durchgeführt werden. /SIE 02/

Kommunikations- und Bussysteme

Die Kommunikation der Server Untersysteme läuft über einen Terminalbus. Im Falle von TELEPERM XP sind Systembus und Terminalbus identisch (SIMATIC NET) und

erfüllen internationale Standards für Industrial Ethernet. Die Kommunikation mit externen Netzwerken verläuft z. B. über offene Schnittstellen (z. B. CM Kommunikationsmodul). Diese Schnittstellen können über Windows-Rechner angesprochen werden. /SIE 02/

Wichtige Module des TELEPERM XP-Systems sind die sogenannte Funktionsmodule (FUM) und Signalmodule (SIM). FUM sind speziell auf die Eigenschaften von Kraftwerken zugeschnittene Module. Über das ES 680 können FUM parametrisiert werden und es können auch Signalsimulationen zu Testzwecken durchgeführt werden. Für die verschiedenen Steuerungsaufgaben gibt es unterschiedliche FUM. /SIE 02/

SIM werden für die Signalaufnahme und -abgabe verwendet. SIM werden zu sogenannten ET 200 Stationen gruppiert und sie sind SIMATIC S7 Komponenten (ET 200M Produktlinie). Jede ET 200 Station verfügt über Busmodule, womit die SIM an ein PROFIBUS-System angeschlossen werden kann. Für unterschiedliche Aufgaben gibt es unterschiedliche SIM. /SIE 02/

3 Bestandsaufnahme der in deutschen Kernkraftwerken eingesetzten programmierbaren oder rechnerbasierten leittechnischen Komponenten

Ziel der Arbeiten ist eine Auswertung der anlagenspezifischen Betriebserfahrung von programmierbaren oder rechnerbasierten leittechnischen Komponenten (Leittechnik-Komponenten). Dazu werden insbesondere Ereignisse unterhalb der sog. Meldeschwelle ausgewertet. Unterhalb der Meldeschwelle bedeutet in diesem Fall, dass die Ereignisse nach der Atomrechtlichen Sicherheitsbeauftragten- und Meldeverordnung (AtSMV) nicht meldepflichtig sind. Zu Beginn der Arbeiten wurde daher eine Bestandsaufnahme der in deutschen Kernkraftwerken eingesetzten Leittechnik-Komponenten durchgeführt. Hierfür wurden Kernkraftwerke ausgewählt, in denen die aktuell eingesetzten programmierbaren oder rechnerbasierten leittechnischen Komponenten ermittelt wurden. Für die Auswahl der Komponenten sind die folgenden Kriterien zugrunde gelegt worden:

- Die Komponenten sollen bereits über eine gewisse Betriebsdauer verfügen, d. h. die auszuwählenden Komponenten sollten Einsatzzeiten von mindestens 3 Jahren in der Anlage aufweisen.
- Die Komponenten sollen einen Softwareanteil und ggf. eine Schnittstelle besitzen, über die die Software von außen geändert werden kann.
- Die Komponenten sollen in einer für statistische Auswertungen geeigneten Stückzahl eingesetzt sein.

Aufgrund dieser Kriterien haben die Fachleute der ausgewählten Kernkraftwerke die von der GRS benötigten Daten zu den entsprechenden Komponenten zur Verfügung gestellt. Hierfür wurden von der GRS die folgenden Kernkraftwerkstypen ausgewählt:

- Siedewasserreaktor (SWR) der Baulinie 69
- Siedewasserreaktor (SWR) der Baulinie 72
- Druckwasserreaktor (DWR) der 2. Generation
- Druckwasserreaktor (DWR) der 3. Generation (Vor-Konvoi-Anlage)
- Druckwasserreaktor (DWR) der 4. Generation (Konvoi-Anlage)

Die Daten bzw. Informationen zu Komponenten liegen in den verschiedenen Anlagen unterschiedlich aufgearbeitet vor. Aus diesem Grund sind die der GRS zur Verfügung gestellten Daten u. a. unterschiedlich aufgebaut und haben unterschiedliche Detaillierungsgrade. Zu Beginn ihrer Arbeiten hat die GRS daher die Daten für ihre Auswertung aufgearbeitet. Dabei wurde insbesondere versucht die Darstellung der Daten anzugleichen, ohne den Inhalt zu verändern. Da dies nicht in allen Fällen möglich war, ist es aus Sicht der GRS nicht sinnvoll die Daten der verschiedenen Anlagen gemeinsam auszuwerten, sondern es erscheint eher sinnvoll die Daten anlagenspezifisch zu betrachten und zu analysieren. Im Folgenden wird diese anlagenspezifische Auswertung dargestellt, wobei die verschiedenen Anlagen anonymisiert sind (SWR A/B und DWR A/B/C).

Darüber hinaus sind auch bei den spezifischen Herstellerauswertungen die unterschiedlichen Hersteller anonymisiert dargestellt. Hierbei sind die Hersteller mit den Buchstaben A bis W gekennzeichnet. Diese Kennzeichnung wird im gesamten Bericht beibehalten. Da nicht in allen Anlagen Komponenten von jedem Hersteller eingesetzt werden, sind einige „Hersteller-Buchstaben“ nicht in jeder Auswertung vorhanden.

3.1 Daten

Die von den verschiedenen Anlagen gelieferten Daten unterteilen sich in Anlagendaten und Ereignisdaten.

Unter den Anlagendaten sind die Daten zu den eingesetzten programmierbaren oder rechnerbasierten Komponenten zu verstehen. Zu diesen Anlagendaten gehören beispielsweise Informationen über die Bezeichnung der Komponenten, die eingesetzten Typen, die Anlagenkennzeichnungen (AKZ), die Anzahl der eingesetzten Komponenten, die Hersteller und die Raumnummern, in denen diese Komponenten eingesetzt sind.

Zusätzlich zu den Anlagendaten wurden der GRS Ereignisdaten geliefert. Diese Ereignisdaten beinhalten u. a. Informationen zu Wartungs- und Instandhaltungsvorgängen bezüglich der in den Anlagendaten aufgeführten Komponenten. In diesem Zusammenhang werden unter Ereignissen beispielsweise Ausfälle oder vorbeugender Austausch verstanden. Diese Ereignisse stellen nicht zwangsläufig nach AtSMV meldepflichte Ereignisse dar.

Bei den Anlagendaten gilt die Besonderheit, dass diese den Zustand der eingebauten Komponenten in der Anlage zu dem Zeitpunkt, als der Datensatz erstellt wurde (Datensatzerstellungszeitpunkt), zeigen. Es ist daher nicht möglich, Anlagendaten zu einem beliebigen früheren oder späteren Zeitpunkt einzusehen. Alle in den Anlagendaten erwähnten Komponenten und die daraus gewonnenen Informationen beziehen sich somit auf den Stand zum Datensatzerstellungszeitpunkt. Dies bedeutet, dass Komponenten, die im Betrachtungszeitraum (Zeitraum, in dem die Ereignisse ausgewertet werden) eingebaut waren, aber vor dem Zeitpunkt der Datensatzerstellung bereits ausgebaut worden sind, nicht in den Anlagendaten zu finden sind. Sollte aber ein Ereignis bei einer solchen Komponente aufgetreten sein, findet sich dieses in den Ereignisdaten wieder. Die durch diese Situation aufgetretenen Diskrepanzen zwischen den Anlagen- und Ereignisdaten konnten jedoch in Gesprächen mit den Anlagen geklärt werden.

Insgesamt wurden Komponenten aus drei Doppelblockanlagen betrachtet. Die Ereignisdaten wurden für jeden Block (Anlage) separat ausgewertet, wobei jedoch zwei Blöcke bei dieser Auswertung zusammengefasst wurden (d. h. es folgen fünf getrennte Auswertungen der Ereignisdaten). Die Anlagendaten wurden nicht blockweise, sondern für einen Standort gemeinsam geliefert und wurden daher auch für jeden Standort gemeinsam ausgewertet.

3.2 Zusammenführung der gelieferten Daten

Aufgrund der Vielzahl an unterschiedlichen Datenlieferungen war es bei allen Anlagen notwendig, die erforderlichen Informationen in einer Tabelle pro Standort zusammenzuführen. Die Informationen über die Komponenten (Anlagendaten) wurden dabei mit den jeweiligen Ereignisdaten verknüpft. Hierdurch wurde für jeden Standort eine Auswertungstabelle generiert, wodurch eine umfangreiche Auswertung ermöglicht wurde.

Im Folgenden wird der Aufbau einer auf diese Weise generierten Auswertungstabelle am Beispiel der Anlage SWR A erläutert. Die Auswertungstabellen der anderen Anlagen sind ähnlich aufgebaut, aber aufgrund der unterschiedlich gelieferten Daten in einigen Angaben und in der Informationstiefe verschieden. Die Auswertungstabelle der Anlage SWR A ist in Anhang A dargestellt.

Die Spaltenbezeichnungen der Auswertungstabelle werden als Attribute bezeichnet. Die Einträge in den Spalten bestehen zum größten Teil aus fest definierten Kategorien, die vom Bearbeiter vor Ort in den Anlagen ausgewählt wurden. In den anderen Spalten wurden vom Bearbeiter vor Ort Freitexte eingetragen. In Tabelle 3.1 werden die Attributskürzel und deren Beschreibungen aufgeführt. Einige der Attribute sind fest miteinander verknüpft, wie z. B. AUSF_ART und AUSF_ARTK. Hierbei beinhaltet das erste Attribut ein Kürzel für die jeweilige Kategorie und das Zweite die entsprechende Information als Klartext. Bei der Eintragung durch den Bearbeiter werden beide Attribute zusammen ausgewählt, d. h. in Abhängigkeit des Kürzels ergibt sich der Klartext.

Da sich einige Attribute bzw. Kategorien inhaltlich überschneiden, ist es in der Praxis möglich, dass unterschiedliche Bearbeiter dasselbe Ereignis unterschiedlich kategorisieren. Dies kann dazu führen, dass z. B. Driftereignisse von Messumformern in dem Attribut „Ursache“ zum Teil der Kategorie „Drift“ und zum Teil der Kategorie „Alterung“ zugeordnet werden. Die genauen Gründe für die im Einzelnen gewählten Kategorien können im Nachhinein nicht mehr nachvollzogen werden, so dass durch diese Überschneidungen eine separate Auswertung der einzelnen Kategorien nicht immer möglich ist. Aus diesem Grund hat die GRS Kategorien mit großen Überschneidungsbereichen gemeinsam ausgewertet.

Tab. 3.1 Erläuterungen zu den Attributen der Auswertungstabelle der Anlage SWR A (siehe Anhang A)

Attributskürzel	**Beschreibung des Attributs**
AEL_NR	Nummer des Ereignisses; wird bei Ausfällen, Austausch etc. laufend vergeben
AKZ	AKZ der betroffenen Komponente (Freitext)
EBP	Einbauplatz der betroffenen Komponente (Freitext)
EIN_DAT	Datum der Erfassung des Ereignisses (Freitext)
AUSF_ART	Kürzel der Ausfallart (feste Kategorien)
AUSF_ARTK	Ausfallart in Klartext (feste Kategorien)
VANLZUST	Kürzel des Anlagenzustandes bei Ereigniseintritt (feste Kategorien)
VANLZUSTK	Anlagenzustand bei Ereigniseintritt in Klartext (feste Kategorien)
VAUSF_ERK	Kürzel für Erkennung des Ereignisses bei ... (feste Kategorien)
VAUSF_ERKK	Erkennung des Ereignisses bei ... in Klartext (feste Kategorien)

Attributskürzel	Beschreibung des Attributs
VAUSF_ERK_SONST	gehört zu Erkennung des Ereignisses bei ..., wird ausgefüllt, falls unter VAUSF_ERKK „Sonstiges“ angegeben ist (Freitext)
VAUSF_ERK_TEXT	gehört zu Erkennung des Ereignisses bei ..., enthält die WKP-Nummer, falls unter VAUSF_ERKK „WKP“ angegeben ist
VFEHLBES	Kürzel der Fehlerbeschreibung (feste Kategorien)
VFEHLBESK	Fehlerbeschreibung in Klartext (feste Kategorien)
REPA_ART	Kürzel der Reparaturart/Ausfallbehebung (feste Kategorien)
REPA_ARTK	Reparaturart/Ausfallbehebung in Klartext (feste Kategorien)
REPAA_DAT	Datum des Beginns der Ausfallbehebung
REPAA_UHR	Uhrzeit des Beginns der Ausfallbehebung
REPAE_DAT	Datum des Endes der Ausfallbehebung
REPAE_UHR	Uhrzeit des Endes der Ausfallbehebung
VAUSF_DAT	Datum der erstmaligen Erkennung des Ausfalls
VAUS_UHR	Uhrzeit der erstmaligen Erkennung des Ausfalls
AEL_KURZ	Erläuterung zu Reparatur/Austausch (Freitext)
AEL_ERROR	Erläuterung zum Fehler (Freitext)
AEL_FEHLER	Fehlerbeschreibung und Bemerkungen (Freitext)
AEL_ARBEIT	Beschreibung der ausgeführten Arbeiten/Ursache (Freitext)
VFEHLART	Kürzel der Informationen zur Fehlerart (feste Kategorien)
VFEHLARTK	Informationen zur Fehlerart in Klartext (feste Kategorien)
ABLAUF_W	Kürzel zum weiteren Verlauf (V: zur Verschrottung, R: zur Reparatur, A: zur Abschlussbearbeitung)
BFS	BFS der Komponente
AKZ	AKZ der Komponente
RAUM	Raum-Kennzeichen der Komponente
HERSTELLER	Hersteller der Komponente
HTA	Hersteller-Typ-Bezeichnung der Komponente (sollte über alle Anlagen gleich sein)
BAUART	Bauart der Komponente
IND_NR	Individuum-Nummer der Komponente
OBJEKT_NR	Objekt-Nummer der Komponente
BAUJAHR	Baujahr der Komponente
PLANERTYP	weitere, zusätzliche Typangabe des Komponente

4 Auswertung anlagenspezifischer Betriebserfahrung unterhalb der Meldeschwelle

Ziel dieses Kapitels ist es, die Ereignis- und Anlagendaten auszuwerten, um einen Überblick über Ausfälle von programmierbaren oder rechnerbasierten leittechnischen Komponenten zu erhalten. Dafür werden in den folgenden Abschnitten Auswertungen hinsichtlich unterschiedlicher Aspekte durchgeführt. Zudem wird ein Vergleich mit den im Bericht „Analyse zum Einsatz und Betrieb elektrotechnischer Einrichtungen“ /GRS 15/ erfassten Daten vorgenommen.

4.1 SWR A

Bei den erfassten Anlagendaten der Anlage SWR A handelt es sich um 2944 Datensätze zu programmierbaren oder rechnerbasierten Komponenten. Davon entfallen 1887 Datensätze auf Komponenten aus dem Bereich Leittechnik, 210 Datensätze auf den Bereich der Elektrotechnik und 847 Datensätze auf den Bereich der Messumformer.

Für den Betrachtungszeitraum von 2000 bis 2012 wurden der GRS 512 Ereignisse zur Verfügung gestellt. Hiervon entfallen 134 Ereignisse auf den Bereich Leittechnik, 19 Ereignisse auf den Bereich Elektrotechnik und 359 Ereignisse auf den Bereich der Messumformer.

4.1.1 Betriebsmittelart

In diesem Abschnitt erfolgt eine Auswertung der Anlagen- und Ereignisdaten nach Betriebsmittelart. Die jeweiligen Anteile der eingesetzten Leittechnik-Komponenten an den am Standort gesamt eingesetzten Leittechnik-Komponenten aufgeschlüsselt nach ihrer Betriebsmittelart sind in Abbildung 4.1 aufgeführt. Aus dieser Abbildung ergibt sich, dass etwa die Hälfte der eingebauten Leittechnik-Komponenten an diesem Standort zur Betriebsmittelart „Baugruppe binäre Elemente“ gehört, ca. 25 % zur Betriebsmittelart „Baugruppe Regler/Steuergerät“ und knapp 10 % zu den freiprogrammierbaren Baugruppen.

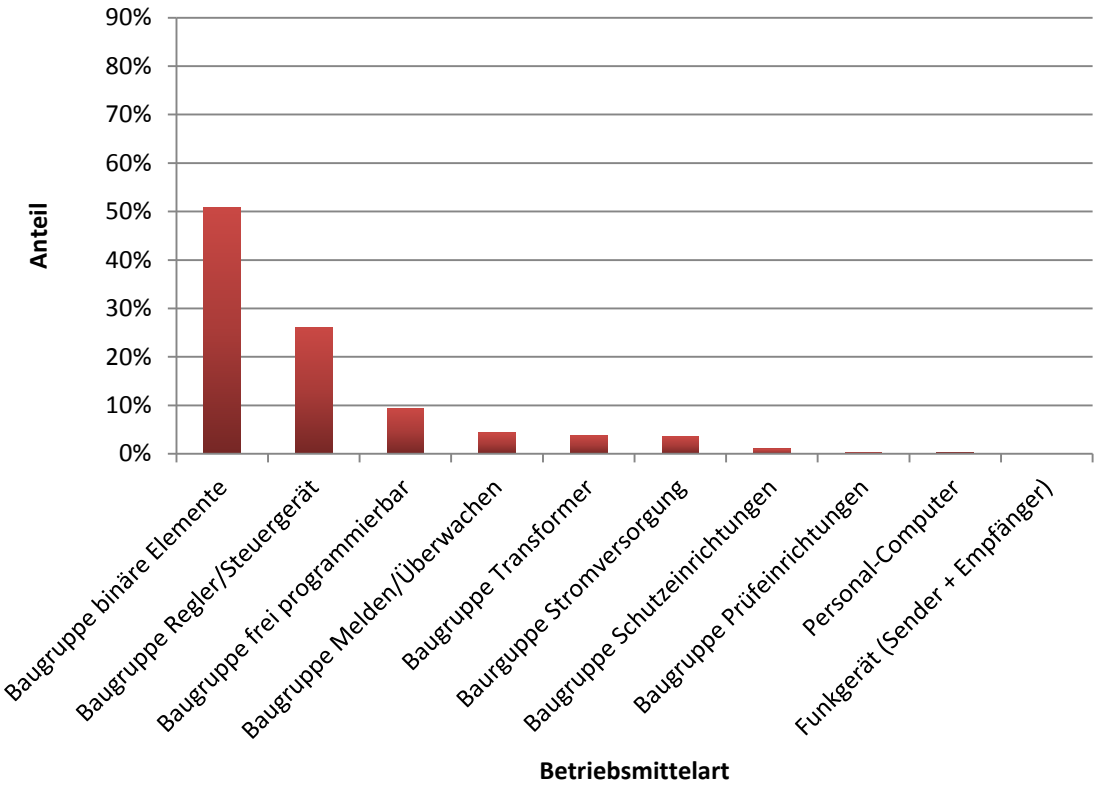

Abb. 4.1 Anteile der Leittechnik-Komponenten an den am Standort der Anlage SWR A gesamt eingesetzten Leittechnik-Komponenten aufgeschlüsselt nach ihrer Betriebsmittelart

Abbildung 4.2 zeigt das Verhältnis der Anzahl der Ereignisse einer Betriebsmittelart zur Anzahl der insgesamt eingesetzten Komponenten dieser Betriebsmittelart für Leittechnik-Komponenten am Standort. In dieser Abbildung ist erkennbar, dass beispielsweise etwa ein Zehntel der Betriebsmittelart „Baugruppe frei programmierbar“ im Laufe des Betrachtungszeitraums von 13 Jahren in Ereignisse involviert war. Der scheinbar größte Anteil kann der Betriebsmittelart „Personal Computer“ zugeordnet werden. Hierbei handelt es sich jedoch nur um einzelne Individuen, so dass die statistische Aussagekraft dieses Balkens für diese Betriebsmittelart extrem gering ist. Des Weiteren ist die hohe Anzahl der Ereignisse der Betriebsmittelart „Baugruppe Melden/Überwachen“ auf einen vorbeugenden Austausch von Kondensatoren auf Melde- und Speicherkarten zurückzuführen.

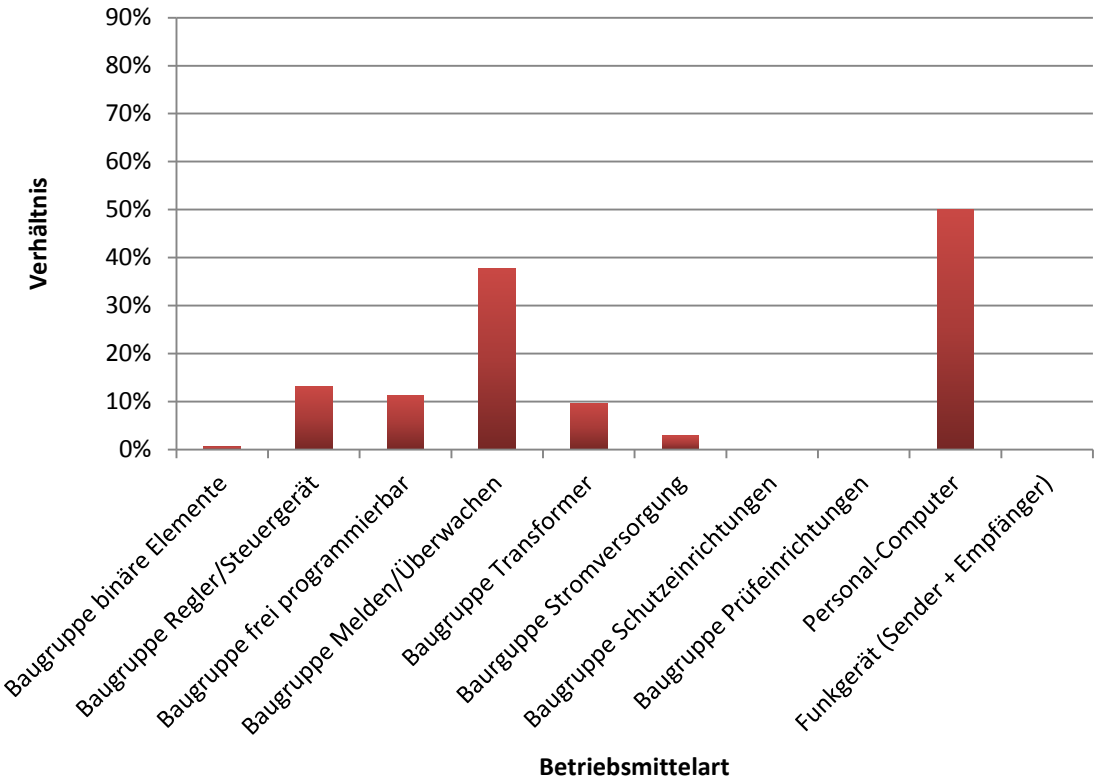

Abb. 4.2 Verhältnis der Anzahl der Ereignisse einer Betriebsmittelart zur Anzahl der insgesamt eingesetzten Komponenten dieser Betriebsmittelart für Leittechnik-Komponenten am Standort der Anlage SWR A

Bei den Auswertungen der anderen Anlagen fallen viele Ereignisse mit Schreibern ins Auge. Die Ereignisse für Schreiber waren in den ersten Datenlieferungen der Anlage SWR A nicht enthalten. Diese wurden nachgeliefert. Ausfallgründe für Schreiber sind auch bei der Anlage SWR A wie in den anderen betrachteten Anlagen (siehe Abschnitte 4.2.1, 4.3.1, 4.4.1 und 4.5.1) hauptsächlich mechanische Fehler.

4.1.2 Zeitlicher Verlauf der Ereignisse

In diesem Abschnitt soll der zeitliche Verlauf der Ereignisse analysiert werden. Dafür ist in Abbildung 4.3 der prozentuale Anteil der Leittechnik-Ereignisse über die jeweiligen Jahre, in denen sie aufgetreten sind, in Bezug auf die Gesamtanzahl der Leittechnik-Ereignisse aufgetragen. Es ist erkennbar, dass zwischen den Jahren 2003 und 2012 die Anzahl der Ereignisse pro Jahr in etwa gleich ist. Die etwas niedrigere Anzahl der Ereignisse in den Jahren 2000 – 2002 liegt vermutlich daran, dass die Aufzeichnung der Informationen am Standort noch nicht so detailliert wie heutzutage implementiert

war. Im Vergleich zwischen den einzelnen Jahren sticht lediglich die erhöhte Anzahl an Ereignissen im Jahr 2004 hervor, in dem es mehr als doppelt so viele Ereignisse gegeben hat. Die Erklärung dafür ist ein Generatorschaden in der Anlage, der im Jahr 2004 aufgetreten ist und bei dem es zu einer Vielzahl von Komponentenausfällen gekommen ist. Auf diese Thematik wird detaillierter in Abschnitt 5.10 eingegangen.

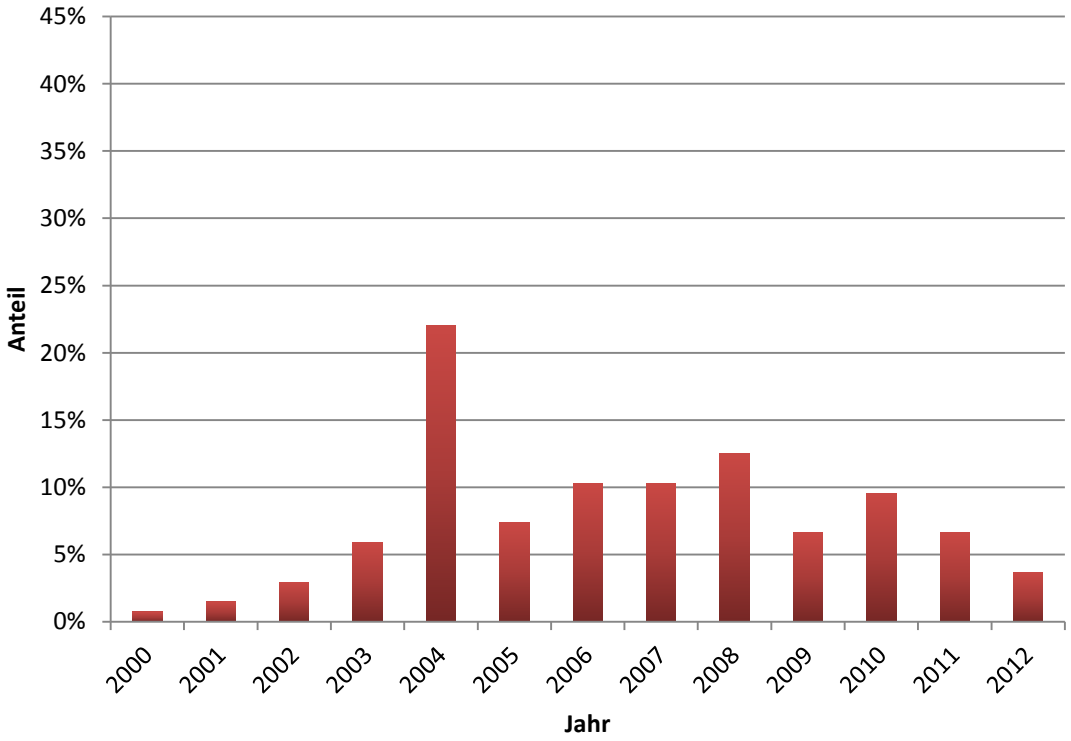

Abb. 4.3 Prozentualer Anteil der Ereignisse pro Jahr in Bezug auf die Gesamtanzahl der Ereignisse für die Leittechnik-Komponenten der Anlage SWR A

4.1.3 Hersteller

Dieser Abschnitt widmet sich der Auswertung der eingesetzten Hersteller. Aus Abbildung 4.4 kann dafür entnommen werden, dass von den 1887 erfassten programmierbaren oder rechnerbasierten Leittechnik-Komponenten ca. 73 % von Hersteller A waren. Den Herstellern H und D konnten ca. 23 % bzw. 4 % der Komponenten zugeordnet werden, wohingegen die Hersteller R und S nur einen geringen Anteil (kleiner als 0,5 %) an den Komponenten hatten.

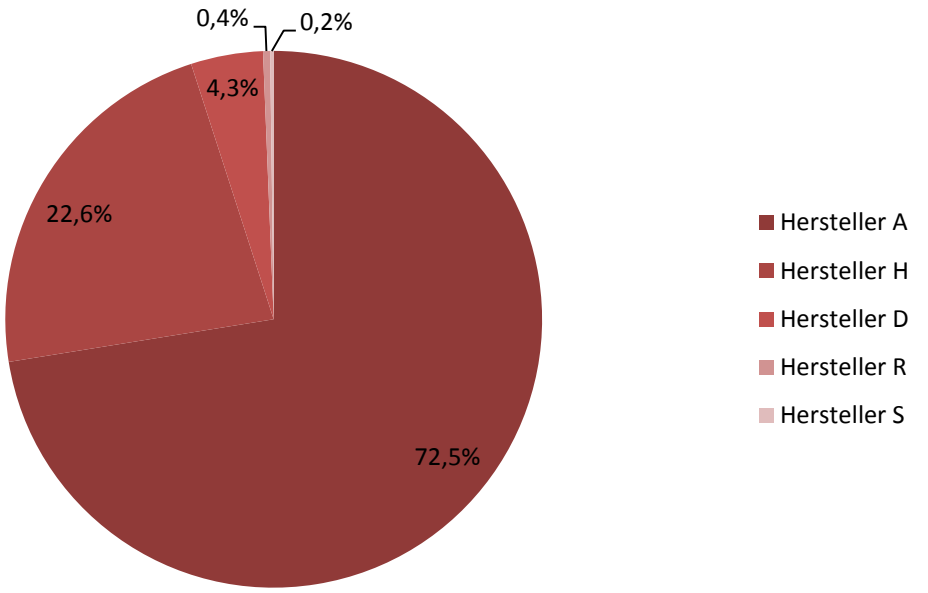

Abb. 4.4 Anteile der Hersteller an den für die Anlage SWR A erfassten programmierbaren oder rechnerbasierten Leittechnik-Komponenten

In Abbildung 4.5 ist das Verhältnis von Ereignisanzahl an Komponenten eines bestimmten Herstellers zur Anzahl der eingesetzten Komponenten für diesen Hersteller für die erfassten Leittechnik-Komponenten dargestellt. Hierbei zeigt sich, dass von den Komponenten des Herstellers A, welcher mit ca. 73 % den größten Anteil an den eingebauten Leittechnik-Komponenten ausgemacht hat, ca. 4 % von Ereignissen betroffen waren. Von den Komponenten des Herstellers H, welche einen Anteil von ca. 23 % an der Gesamtanzahl der Leittechnik-Komponenten hatten, sind ca. 11 % von Ereignissen betroffen gewesen. Etwa 38 % der Komponenten des Herstellers D waren von Ereignissen betroffen, während die Komponenten der Hersteller R und S gar nicht von Ereignissen betroffen waren.

Die hohe Anzahl von Ereignissen der Komponenten des Herstellers D wurde genauer untersucht. Hierbei fiel auf, dass es sich in allen Fällen um Melde- und Speicherkarten handelte. In ca. 87 % dieser Fälle handelt es sich um einen vorbeugenden Austausch von Elektrolytkondensatoren und damit nicht um einen Ausfall der Komponente. Aus Weiterleitungsnachrichten (WLN 08/88 und WLN 06/92) ist bekannt, dass Elektrolytkondensatoren nach einer gewissen Betriebsdauer erhöhte Ausfallraten aufweisen und daher in regelmäßigen Abständen ausgetauscht werden sollten.

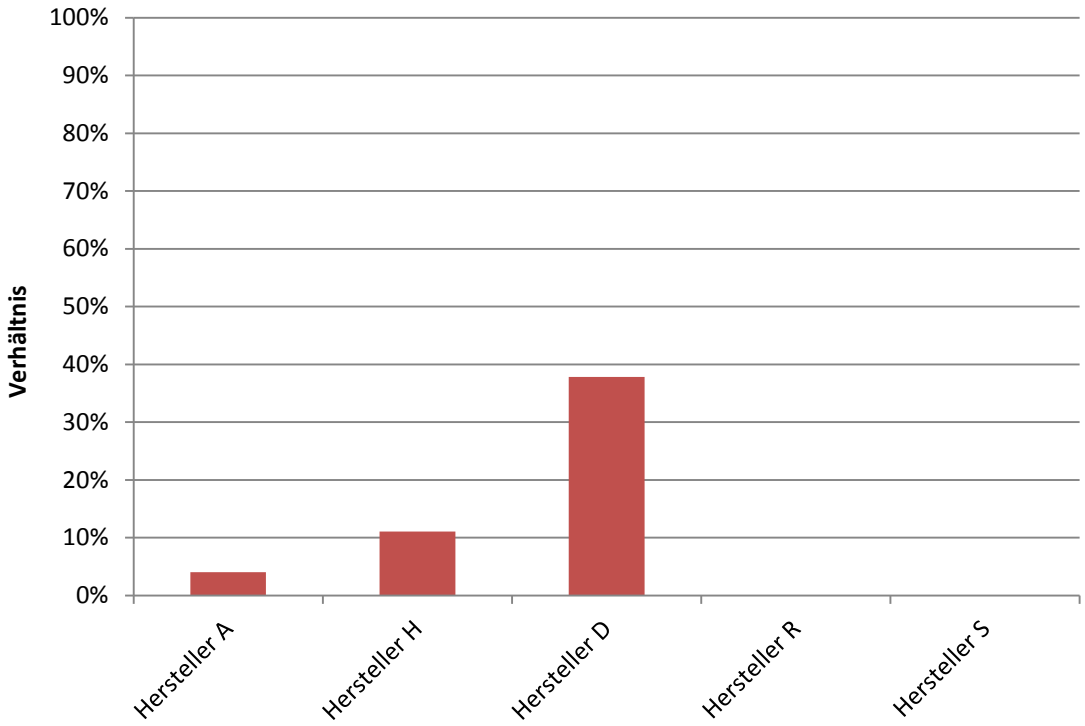

Abb. 4.5 Verhältnis von Ereignisanzahl an Komponenten eines bestimmten Herstellers zur Anzahl der eingesetzten Komponenten für diesen Hersteller für die erfassten Leittechnik-Komponenten der Anlage SWR A

Durch die in der Auswertungstabelle für die Anlage SWR A vorhandenen Informationen zur alten und neuen Komponente konnte untersucht werden, ob es bei einem Austausch der Komponente zu einem Wechsel des Herstellers gekommen war. Es zeigte sich, dass ein Herstellerwechsel die Ausnahme darstellt und daher eine weitere statistische Auswertung in diese Richtung aufgrund der zu geringen Datenmenge nicht sinnvoll ist.

4.1.4 Vergleich zwischen Leittechnik-Komponenten, Elektrotechnik-Komponenten und Messumformern

Wie bereits zu Beginn dieses Berichtes erwähnt, ist das Ziel des Projektes, die in Kernkraftwerken eingesetzten programmierbaren oder rechnerbasierten Leittechnik-Komponenten (L) näher zu untersuchen. Im Gegensatz dazu, werden im Bericht „Analyse zum Einsatz und Betrieb elektrotechnischer Einrichtungen“ /GRS 15/ ähnliche Auswertungen für programmierbare oder rechnerbasierte Elektrotechnik-Komponenten (E) und Messumformer (M) vorgenommen. Da ein Vergleich der verschiedenen pro-

grammierbaren oder rechnerbasierten Komponenten weitere Erkenntnisse bringen könnte, wird im Folgenden untersucht, ob die unterschiedlichen Komponentenarten (L, E, M) verschiedene Ausfallzahlen oder Charakteristika aufweisen. Dazu werden die Ereignisse von L, E und M hinsichtlich verschiedener Attribute relativ zueinander verglichen.

Die Farbgebung in den folgenden Abbildungen ist im gesamten Bericht konsistent. Auswertungen von Leittechnik-Komponenten (L) werden in Rot dargestellt, Auswertungen von Elektrotechnik-Komponenten (E) in Grün und Auswertungen von Messumformern (M) in Blau.

4.1.4.1 System

Zunächst werden die Systeme, in denen die programmierbaren oder rechnerbasierten Komponenten eingesetzt sind, für alle Komponentenarten (L, E, M) aufgetragen. Die Problematik dabei besteht für die Anlage SWR A darin, dass in den vorliegenden Daten die Informationen über das System nur im AKZ enthalten sind. Dies bedeutet, dass ohne das AKZ eine Zuordnung zu einem bestimmten System nicht möglich ist. In den Daten ist aber nur für einige Komponenten das AKZ angegeben. Ein Grund dafür ist, dass eine Baugruppe mehrere Kanäle haben kann und somit mit einer Vielzahl von Systemen verbunden sein kann. Beispielsweise können bei Ausfall einer Ausgabebaugruppe mit 32 Kanälen alle 32 Kanäle und somit 32 AKZ betroffen sein.

Insgesamt hat sich gezeigt, dass bei 660 von 2944 Komponenten (L, E, M) Angaben zum AKZ vorliegen. Hauptsächlich ist das AKZ bei Messumformern angegeben (562). Bei Leittechnik-Komponenten sind es 65 mit AKZ und bei Elektrotechnik-Komponenten 33.

Dies bedeutet, dass für die Leittechnik-Komponenten eine Systemzuordnung bei nur ca. 3 % der Komponenten möglich war. Diese Systemzuordnung ist in Abbildung 4.6 aufgetragen. Aus dieser Grafik kann entnommen werden, dass von diesen Leittechnik-Komponenten ca. 37 % auf das System „Turbine, Kondensator und Generator“, ca. 20 % auf das System „Gleichstromerzeugung/-verteilung“ sowie ca. 12 % auf das System „Nebenanlagen“ entfallen sind. Des Weiteren sind ca. 9 % auf das System „Brennelementhandhabung“ und ca. 8 % auf die Schränke für Steuerung/Schutz entfallen. Mit ca. 5 % folgt das System „SHB mit Einbauten“ und mit ca. 3 % das System

„Hochspannungs-Eigenbedarfsanlagen“. Zur besseren Übersicht wurden die Systeme, die einen Anteil von kleiner als 3 % haben, nicht mit aufgetragen.

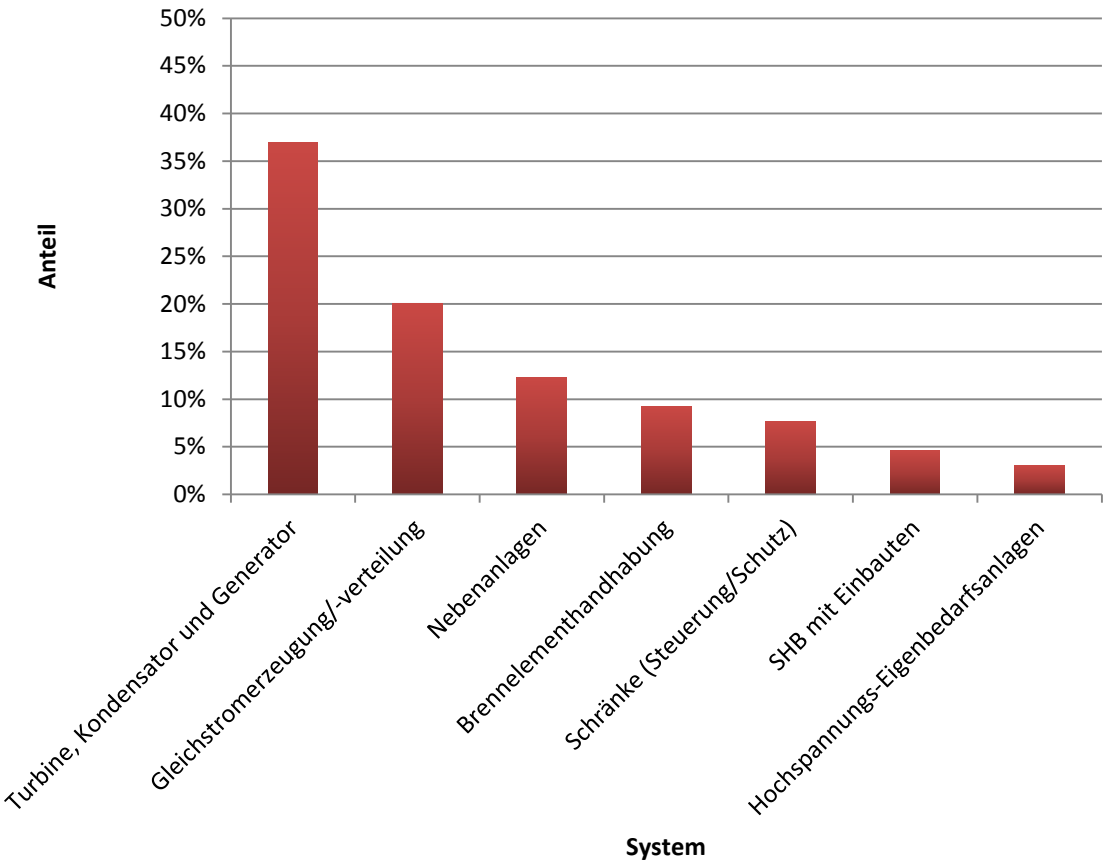

Abb. 4.6 Anteile der in der Anlage SWR A eingebauten Leittechnik-Komponenten an den Systemen

Bei den Elektrotechnik-Komponenten war eine Systemzuordnung bei ca. 16 % der Komponenten möglich, was in Abbildung 4.7 aufgetragen ist. Den größten Anteil hat dabei mit ca. 48 % das System „Wasser-Dampfkreislauf“ ausgemacht, gefolgt von den Systemen „Nebenanlagen“ mit ca. 21 % und „Hochspannungsanlagen (Energieverteilung)“ mit ca. 8 %. Jeweils ca. 6 % sind auf die Systeme „Reaktorhilfsanlagen“ und „Hochspannungs-Eigenbedarfsanlagen“ entfallen. Darüber hinaus hatten die Systeme „Turbine, Kondensator und Generator“ und „gesicherte Schienen/Notstromerzeugung“ einen Anteil von ca. 3 %.

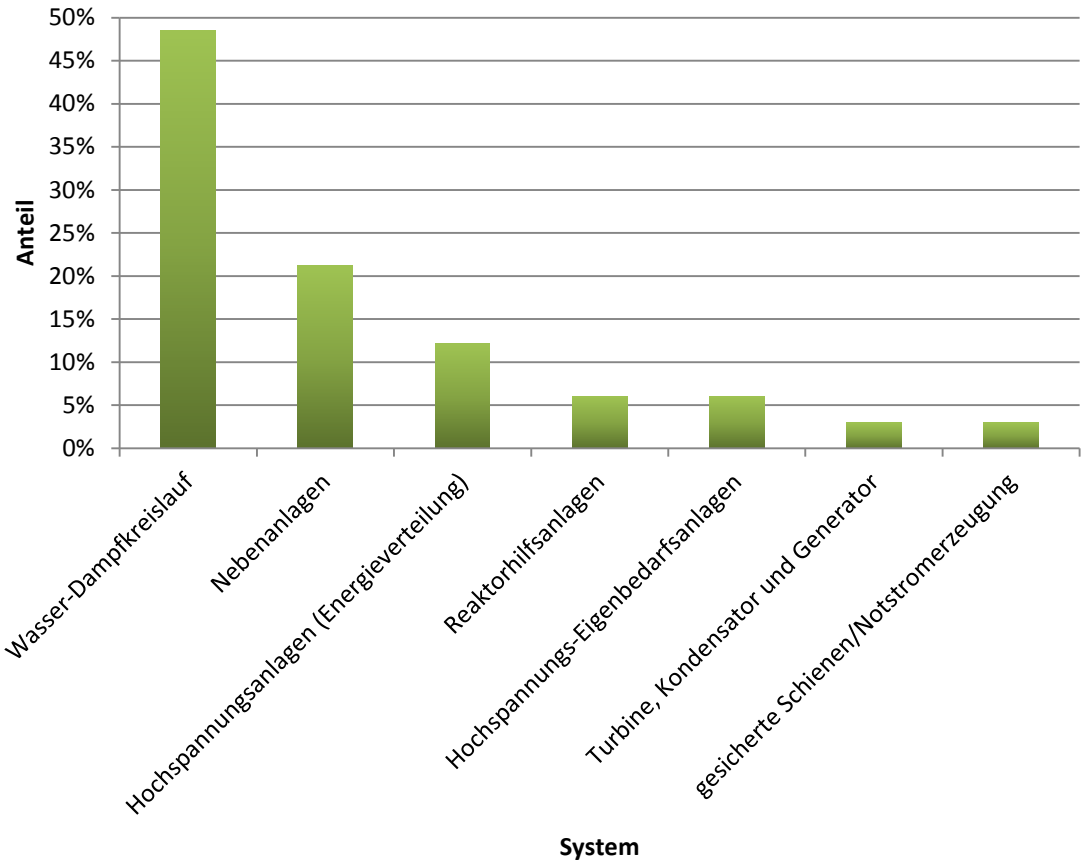

Abb. 4.7 Anteile der in der Anlage SWR A eingebauten Elektrotechnik-Komponenten an den Systemen

Für ca. 66 % der Messumformer konnte ein System zugeordnet werden, was in Abbildung 4.8 dargestellt ist. Davon waren ca. 27 % im System „Reaktorhilfsanlagen“ eingesetzt, ca. 19 % im System „Nebenanlagen“ und ca. 17 % im System „Wasser-Dampfkreislauf“. Danach folgten mit ca. 9 % das System „Turbine, Kondensator und Generator“, das System „Kühlwasseranlagen“ mit ca. 8 %, das System „SHB mit Einbauten“ mit ca. 7 %, das System „gesichertere Schienen/Notstromerzeugung“ mit ebenfalls ca. 7 % und das System „nukleare Dampferzeugung“ mit ca. 6 %.

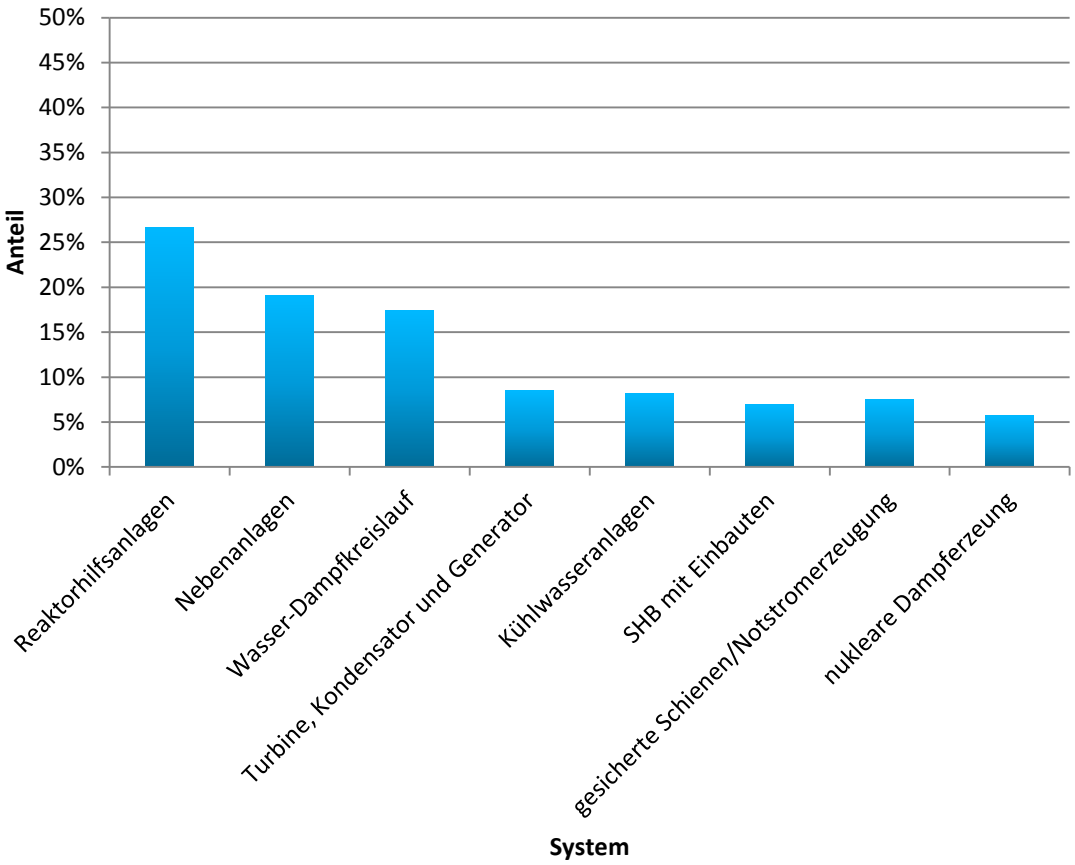

Abb. 4.8 Anteile der in der Anlage SWR A eingebauten Messumformer an den Systemen

Im Gegensatz zu diesen Abbildungen ist in den nächsten Abbildungen aufgetragen, welche Systeme bei den Ereignissen betroffen waren. In Abbildung 4.9 ist dies für die Leittechnik-Komponenten dargestellt, in Abbildung 4.10 für die Elektrotechnik-Komponenten und in Abbildung 4.11 für die Messumformer. Zur besseren Übersicht sind in diesen 3 Abbildungen nur die Systeme dargestellt, die einen Anteil von mindestens 3 % haben.

Aus Abbildung 4.9 kann entnommen werden, dass mit ca. 35 % am meisten das System „Schränke (Steuerung/Schutz)“ von Ereignissen betroffen war, gefolgt dem System „Turbine, Kondensator und Generator“ mit ca. 31 % und das System „Brennelementhandhabung“ mit ca. 16 %. Des Weiteren kamen Ereignisse in den Systemen „Nebenanlagen“ (ca. 6 %), „Gleichstromerzeugung/-verteilung“ (ca. 6 %), „Warten und örtliche Leitstände“ (ca. 5 %) und „SHB mit Einbauten“ (ca. 4 %) vor.

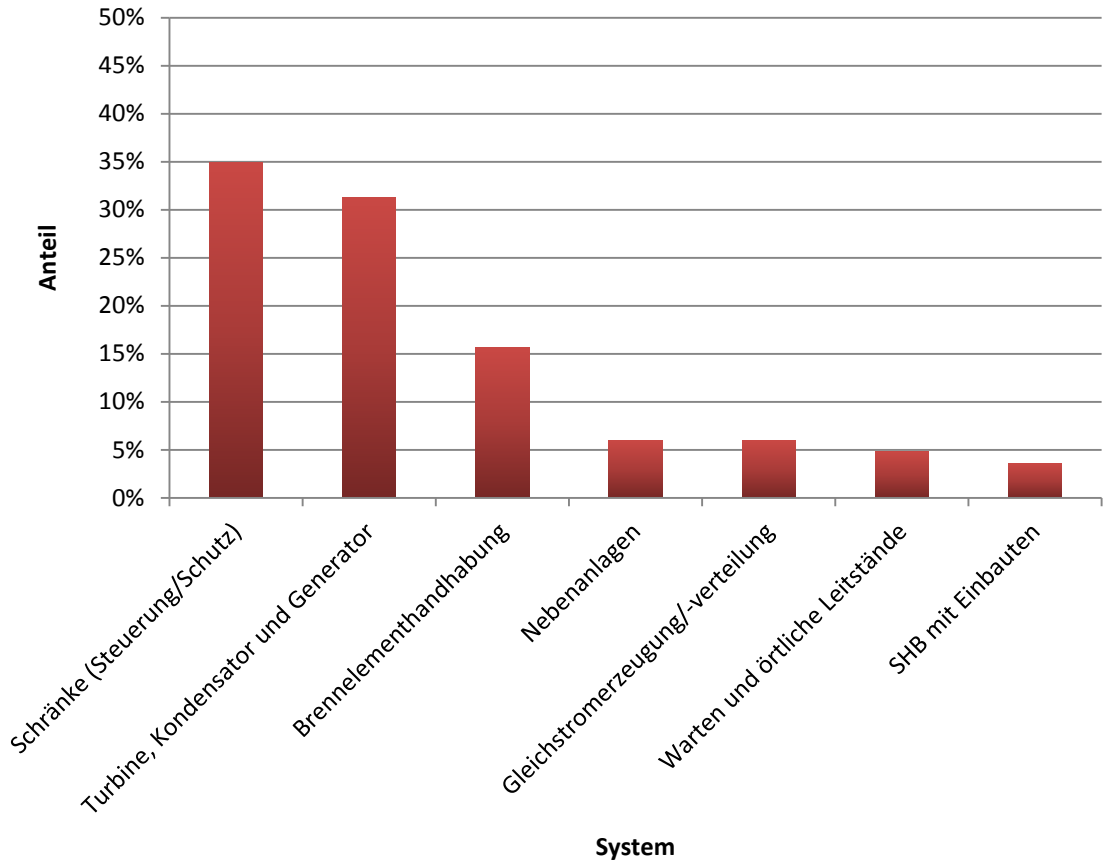

Abb. 4.9 Anteile der von Leittechnik-Ereignissen betroffenen Systeme in der Anlage SWR A

Abbildung 4.10 zeigt, dass bei den Ereignissen der Elektrotechnik-Komponenten der größte Anteil auf das System „Hochspannungsanlagen (Energieverteilung)“ mit ca. 29 % entfallen ist, gefolgt von dem System „Nebenanlagen“ und „gesicherte Schienen/Notstromerzeugung)“ mit jeweils ca. 21 %. Bei den Ereignissen des Systems „Hochspannungsanlagen (Energieverteilung)“ handelt es sich zum großen Teil um eine Rückrufaktion eines Herstellers und damit um einen vorbeugenden Austausch. Diese Thematik wird in Abschnitt 5.5 nochmal aufgegriffen. Etwa 14 % der Ereignisse betrafen das System „Hochspannungs-Eigenbedarfsanlagen)“ sowie jeweils ca. 7 % die Systeme „Turbine, Kondensator und Generator“ und „Wasser-Dampfkreislauf“.

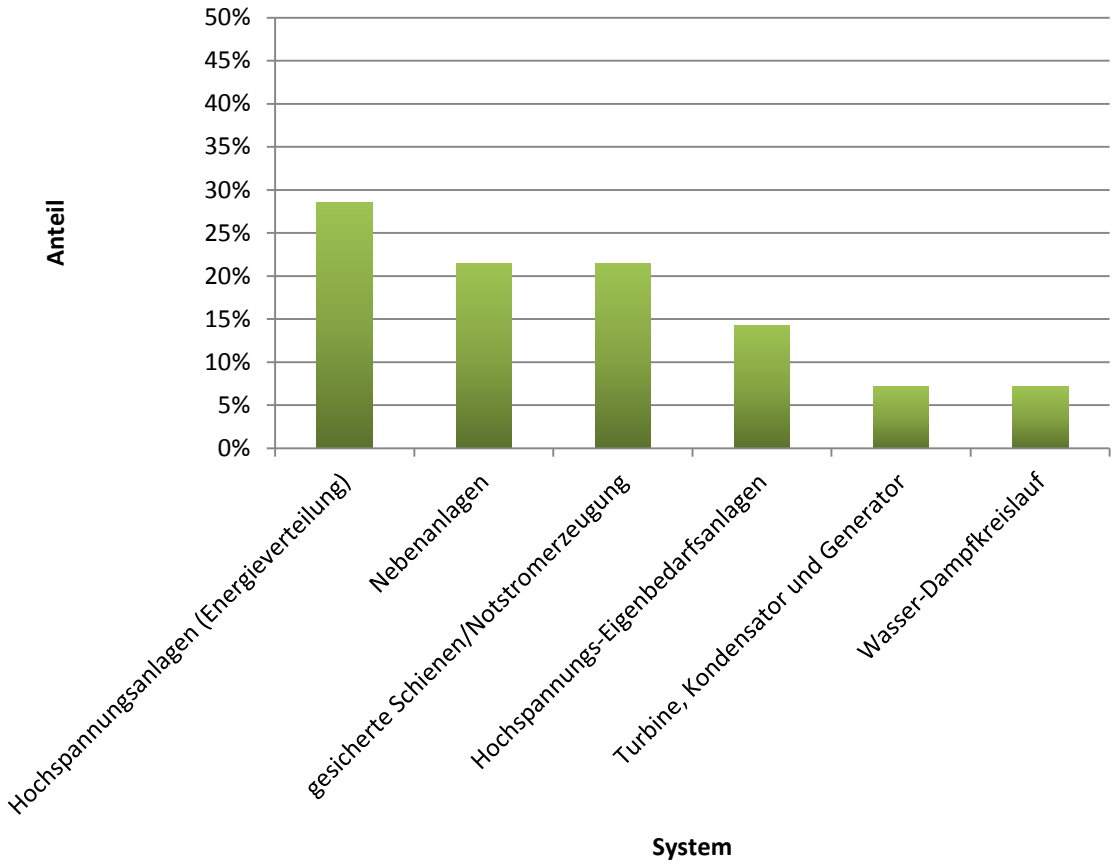

Abb. 4.10 Anteile der von Elektrotechnik-Ereignissen betroffenen Systeme in der Anlage SWR A

Im Bereich der Messumformer (Abbildung 4.11) war vor allem das System „Reaktorhilfsanlagen“ betroffen, welche an den Ereignissen einen Anteil von ca. 24 % eingenommen haben. Danach folgte das System „SHB mit Einbauten“ mit ca. 17 % sowie die Systeme „Nebenanlagen“ und „gesicherte Schienen/Notstromerzeugung“ mit jeweils ca. 15 %. Des Weiteren verteilten sich die Ereignisse auf die Systeme „Wasser-Dampfkreislauf“ (ca. 9 %), „Turbine, Kondensator und Generator“ (ca. 8 %), „Kühlwasseranlagen“ (ca. 7 %) und „nukleare Dampferzeugung“ (ca. 4 %). Die meisten der Ereignisse entfallen hier systemübergreifend auf Driftereignisse.

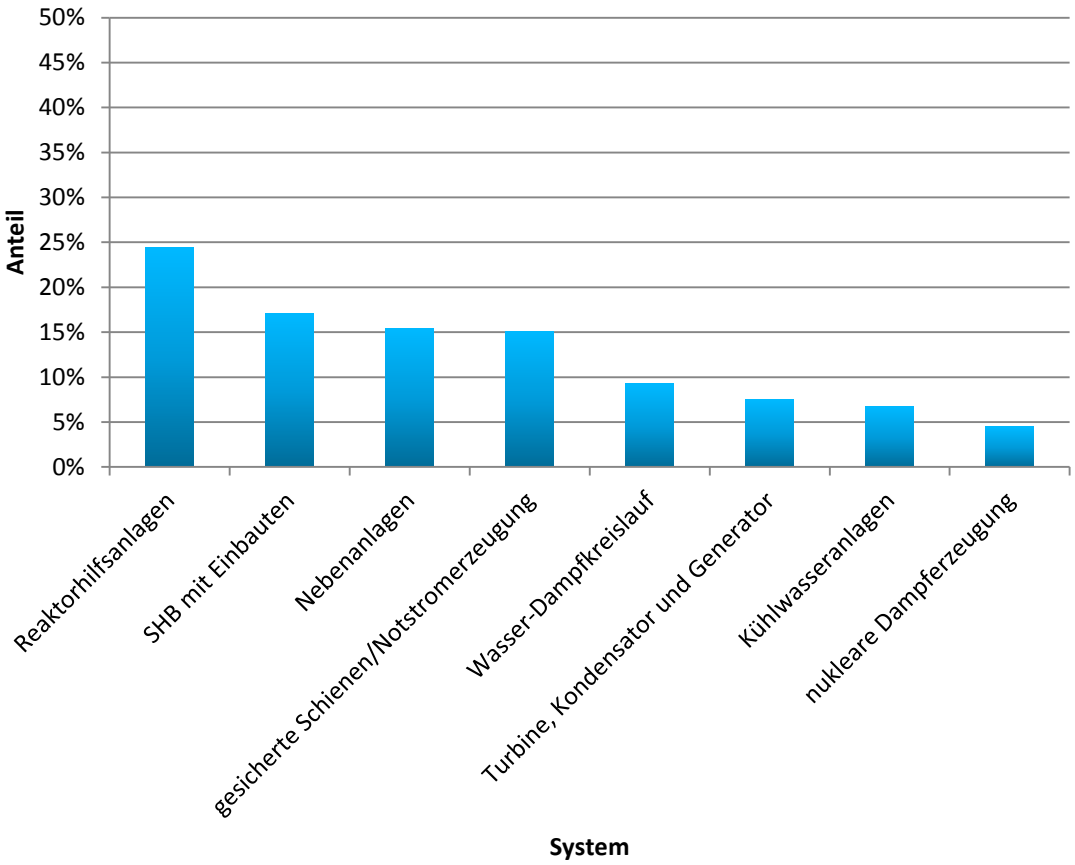

Abb. 4.11 Anteile der von Messumformer-Ereignissen betroffenen Systeme in der Anlage SWR A

4.1.4.2 Ausfallart

Im Folgenden wird die Ausfallart der Komponenten der Elektro- und Leittechnik sowie der Messumformer untersucht (siehe Abbildung 4.12). Die meisten aktiven Ausfälle weisen Komponenten aus dem Bereich der Leittechnik auf (ca. 44 %), gefolgt von den Elektrotechnik-Komponenten mit ca. 35 % und den Messumformern mit ca. 31 %. Generell ist ebenfalls erkennbar, dass der aktive Ausfall bei den Leittechnik-Komponenten am häufigsten vorkommt. Passive Ausfälle an Leittechnik-Komponenten traten mit einem Anteil von ca. 31 % auf und zu einem Austausch einer Leittechnik-Komponente durch vorbeugende Instandhaltung kam es in ca. 24 % der Fälle. Der prinzipielle Unterschied zwischen aktiven und passiven Ausfällen wird in Anhang B beschrieben.

Bei den Messumformern hingegen sind die meisten der Ausfälle passiver Natur (ca. 67 %). Vorbeugend wurden kaum Mängel behoben, der Prozentsatz liegt hier bei

ca. 2 %. Dies unterscheidet sich deutlich von den Elektrotechnik-Komponenten, die vorbeugend den höchsten Prozentsatz von ca. 41 % aufweisen sowie von den Leittechnik-Komponenten, die in ca. 24 % der Fälle vorbeugend instandgehalten werden. Diese hohe Anzahl von vorbeugender Instandhaltung bei den Elektrotechnik-Komponenten kann auf verschiedene Rückrufaktionen der Hersteller zurückgeführt werden. Die Thematik der Rückrufaktionen wird in Abschnitt 5.5 nochmal aufgegriffen.

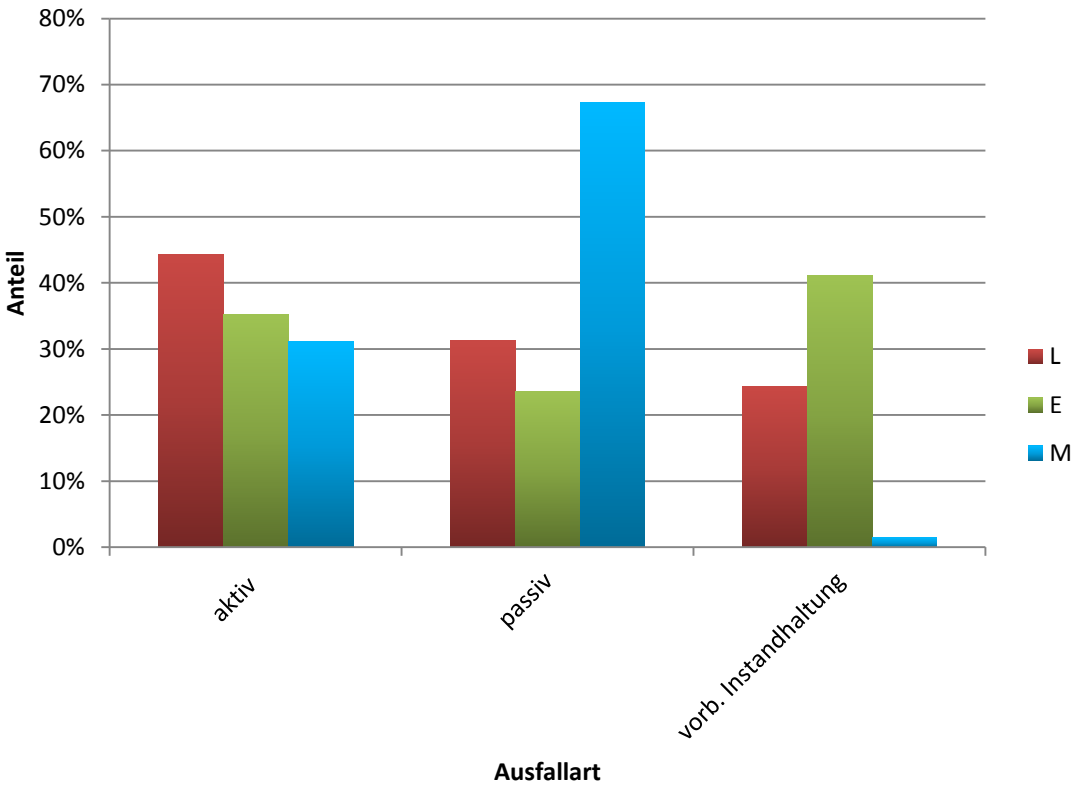

Abb. 4.12 Anteile der verschiedenen Ausfallarten in der Anlage SWR A für die Komponenten der Elektro- und Leittechnik sowie für Messumformer

4.1.4.3 Fehlererkennung

In diesem Abschnitt wird ausgewertet, wie das entsprechende Ereignis in der Anlage erkannt wurde. Abbildung 4.13 zeigt den Vergleich zwischen den einzelnen Erkennungsarten „Prüfung“, „Anforderung“, „Betrieb“, „Schichtrundgang“, „vorbeugende Instandhaltung“ und „Meldung“.

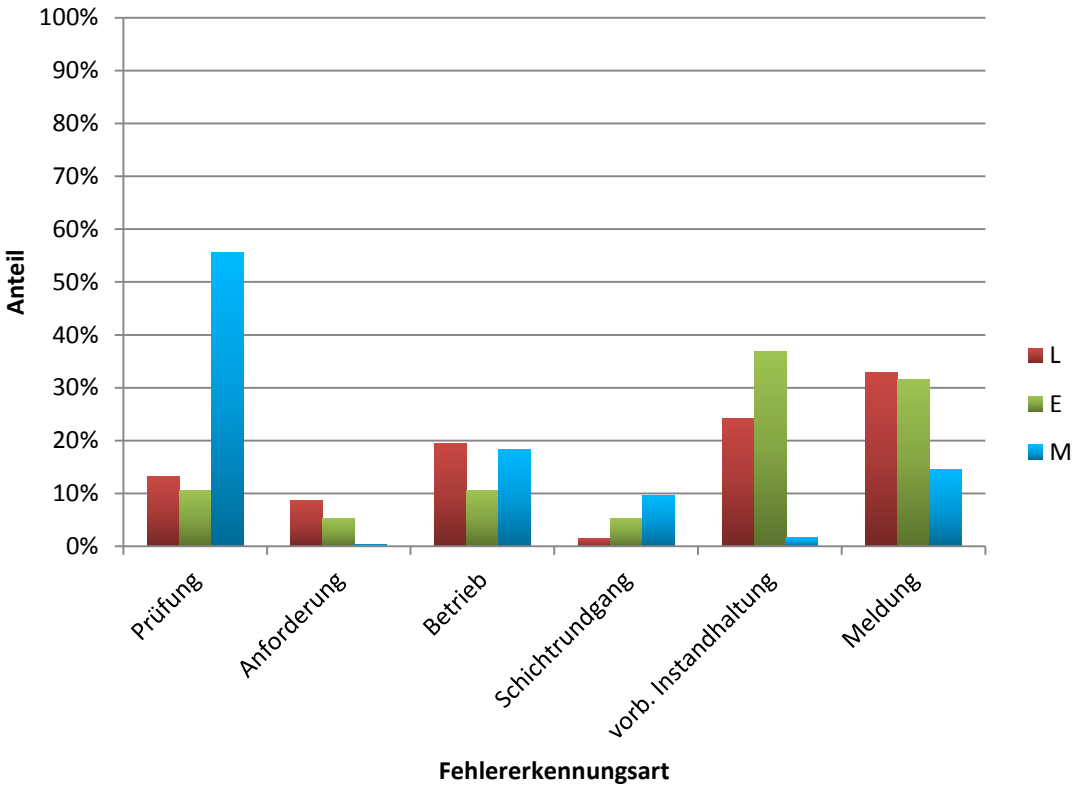

Abb. 4.13 Anteile der verschiedenen Fehlererkennungsarten in der Anlage SWR A für die Komponenten der Elektro- und Leittechnik sowie für Messumformer

Die meisten Ereignisse bei Messumformern wurden im Rahmen von Prüfungen erkannt, wobei es sich in etwa 50 % dieser Fälle um Driftereignisse handelte. Hierbei handelt es sich um Ereignisse, die vom analogen Teil des Messumformers herrühren (siehe Abschnitt 5.9).

Die hohe Fehlererkennungsrate von Elektrotechnik-Komponenten bei vorbeugender Instandhaltung (ca. 37 %) ist auf Rückrufaktionen des Herstellers A zurückzuführen. Knapp ein Viertel der Ereignisse mit Leittechnik-Komponenten ist ebenfalls auf vorbeugender Instandhaltung zurückzuführen, wobei es sich ebenfalls um Rückrufaktionen handelt. Das Thema „Rückrufaktionen“ wird in Abschnitt 5.5 nochmal aufgegriffen.

Gegenüber den anderen Fehlererkennungsarten erscheinen die Ereignisse bei Anforderung besonders problematisch, da bei diesen der Fehler erst bei Anforderung der Komponenten entdeckt wird und vorher unerkannt vorliegt. Den höchsten Anteil bilden hierbei die Leittechnik-Komponenten mit etwa 9 %, während der Ausfall bei Anforde-

rung bei Messumformern einsatzbedingt (die Messumformer sind kontinuierlich in Betrieb) zu vernachlässigen ist. Die Elektrotechnik-Komponenten liegen zwar auch im einstelligen Prozentbereich, allerdings ist aufgrund der geringen Datenmenge zu diesen keine statistische Aussage möglich. Da der Ausfall bei Anforderung von erhöhtem Interesse ist, wird darauf in Abschnitt 4.1.4.5 genauer eingegangen. Eine Untersuchung zur zeitlichen Entwicklung der Fehlererkennung ist in Abschnitt 5.8 zu finden.

4.1.4.4 Selbstmeldende und nicht selbstmeldende Ausfälle

Ein weiteres Kriterium bei der Auswertung der Ereignisse liegt in der Unterscheidung zwischen selbstmeldenden und nicht selbstmeldenden Ereignissen (für eine genauere Beschreibung siehe Anhang B). Bei selbstmeldenden Ereignissen muss es sich nicht immer um in Betrieb befindliche Komponenten handeln, sondern es kann ebenfalls Komponenten betreffen, die als Standby Komponenten (Einsatz erst bei Anforderung) überwacht werden.

Knapp zwei Drittel der Ereignisse mit Leittechnik-Komponenten sind selbstmeldend, was im Vergleich der drei betrachteten Gruppen (L, E, M) den höchsten Anteil ausmacht (siehe Abbildung 4.14). Nicht selbstmeldende Ereignisse traten am häufigsten bei Messumformern auf. Hier handelt es sich in den meisten Fällen um Driftereignisse (ca. 64 %), welche, wie in Abschnitt 4.1.4.3 dargestellt, oft bei Prüfungen erkannt werden. Die ca. 64 % sind als untere Schranke für den Anteil der Driftereignisse zu sehen. Dies liegt daran, dass der Mitarbeiter des Kraftwerks, der das Ereignis einträgt, gewisse Wahlmöglichkeiten zwischen den Kategorien der Attribute hat, bei einigen Attributen aber auch Freitext eingegeben werden kann (siehe Abschnitt 3.2). Die Einschätzung des Ereignisses kann somit je nach Bearbeiter unterschiedlich erfolgen. Es kann also zu Einzelereignissen kommen, die verschieden zugeordnet wurden, weshalb der Wert für gewisse Größen nur als untere Schranke angegeben werden kann.

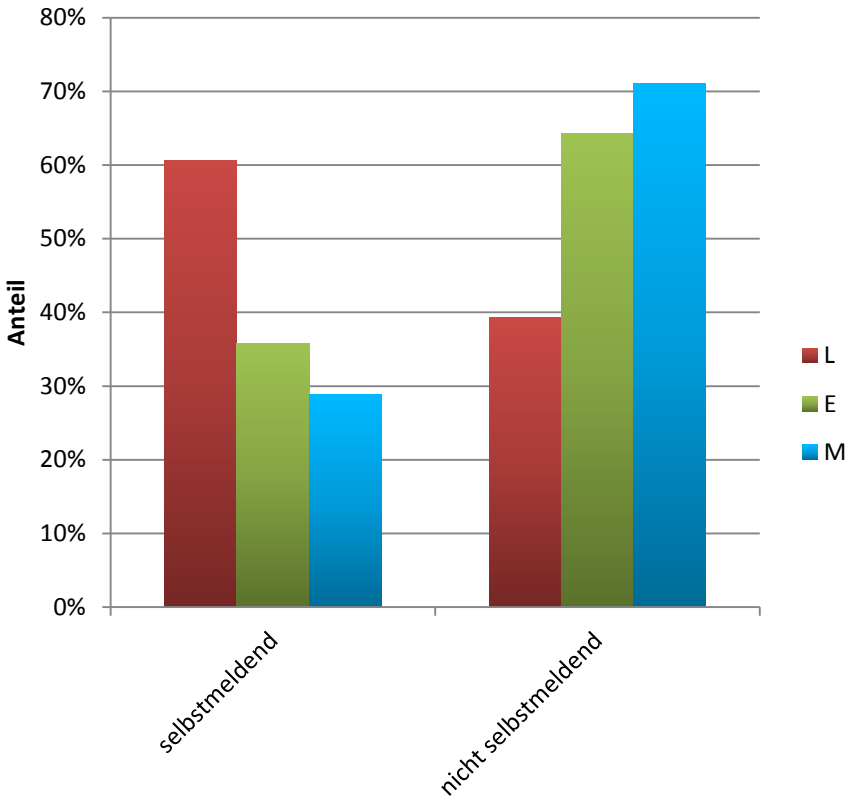

Abb. 4.14 Anteile der selbstmeldenden und nicht selbstmeldenden Ereignisse für die Komponenten der Elektro- und Leittechnik sowie für Messumformer

Im Folgenden werden die nicht selbstmeldenden Ereignisse hinsichtlich der Fehlererkennungsart untersucht. Die Auswertung wird wie in Abschnitt 4.1.4.3 durchgeführt. Allerdings werden die auszuwertenden Daten ausschließlich auf die nicht selbstmeldenden Ereignisse beschränkt. Das Ergebnis der Auswertung ist in Abbildung 4.15 dargestellt.

Auffällig ist, dass drei Viertel der nicht selbstmeldenden Ereignisse bei Messumformern durch Prüfungen erkannt wurden. Hierbei handelt es sich zumeist um die schon erwähnten Driftereignisse.

Die Hälfte der nicht selbstmeldenden Ereignisse bei Elektrotechnik-Komponenten basiert auf dem Austausch von Komponenten aufgrund vorbeugender Instandhaltung. Hier handelt es sich um Rückrufaktionen, welche im Abschnitt 5.5 näher erläutert werden.

Auffällig im Bereich der Leittechnik ist, dass bei ca. 26 % der Komponenten der Ausfall erst bei Anforderung detektiert wurde. Eine genaue Untersuchung dieser Ereignisse

hat keinen systematischen Zusammenhang aufgezeigt. In über der Hälfte dieser Fälle sind die Komponenten der Betriebsmittelart „Baugruppe Regler/Steuergerät“ zuzuordnen.

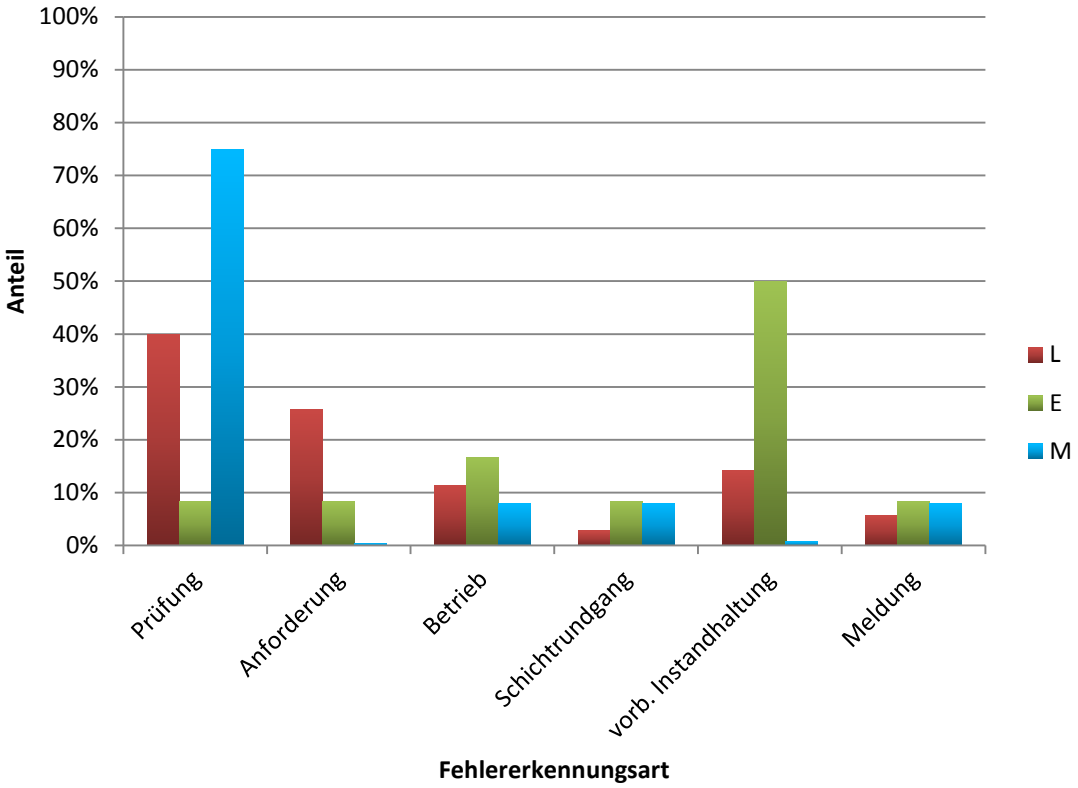

Abb. 4.15 Anteile der verschiedenen Fehlererkennungsarten für die nicht selbstmeldenden Fehler aus Abb. 4.14 für die Komponenten der Elektro- und Leittechnik sowie für Messumformer

Die detaillierten Untersuchungen der nicht selbstmeldenden Fehler ergaben keine auffälligen Defizite im Bereich der Prüfungen oder keine neuen Ausfallmechanismen, die dazu führen würden, dass bekannte (etablierte) Erkennungsmechanismen nicht funktionieren.

4.1.4.5 Fehler bei Anforderung

Wie schon in den vorangegangenen Abschnitten beschrieben, sind nicht selbstmeldende Fehler, die erst bei Anforderung entdeckt werden, von besonderem Interesse. Denn diese Ereignisse bleiben über längere Zeit unentdeckt und können mehrere

Komponenten gleichzeitig betreffen. Ein Beispiel hierfür sind Ereignisse mit ausgefallenen Pufferbatterien, welche genauer in Abschnitt 5.2 betrachtet werden.

Eine Auswertung aller Ereignisse (L, E, M) zeigt, dass es bei ca. 2 % dieser Ereignisse zu Ausfällen bei Anforderung gekommen ist. Davon fallen ca. 91 % auf Leittechnik-Komponenten zurück. Werden bei dieser Auswertung ausschließlich die Ereignisse mit Leittechnik-Komponenten betrachtet, sind ca. 9 % dieser Ereignisse, solche Ausfälle, die erst bei Anforderung auftreten.

Da diese Ausfälle der GRS als wichtig erschienen, wurden weitere Untersuchungen zu dieser Thematik durchgeführt. Dafür wurden u. a. ergänzende Informationen (z. B. Reparaturberichte) herangezogen und ausgewertet. Im Rahmen dieser Untersuchungen sind keine Auffälligkeiten bezüglich der eingesetzten Software oder einer anderen systematischen Ursache erkannt worden. Auch gab es keine Erkenntnisse über neue Ausfallmechanismen.

4.1.4.6 Ausfallbehebung

Im Weiteren wird die Ausfallbehebung für die verschiedenen Komponenten (L, E, M) miteinander verglichen. Für die Ausfallbehebung gilt, dass nach Erkennung eines Ereignisses eine Komponente repariert oder ausgetauscht werden kann. Für den Fall, dass der Fehler vorher bekannt ist (z. B. durch einen Hinweis eines Herstellers), kann die Komponente auch vorbeugend instandgehalten werden. Die jeweiligen Anteile der Ereignisse an diesen drei Ausfallbehebungsmöglichkeiten für die Leittechnik- und Elektrotechnik-Komponenten sowie für die Messumformer sind in Abbildung 4.16 dargestellt.

Die erhöhte Anzahl an Reparaturen für die Messumformer (ca. 70 %) kann wieder auf die bereits erwähnten Driftereignisse zurückgeführt werden, wobei Neueinstellungen/Justierungen vorgenommen wurden (siehe auch Abschnitt 5.9).

Die Anteile der vorbeugenden Instandhaltung für die Leittechnik- und die Elektrotechnik-Komponenten stehen in Verbindung mit den Rückrufaktionen, die im Abschnitt 5.5 nochmal aufgegriffen werden.

Die hohen Anteile der Austauschereignisse für die Leittechnik- und die Elektrotechnik-Komponenten sind plausibel, da in diesem Bereich eine Reparatur durch den meist komplexen Aufbau erschwert ist.

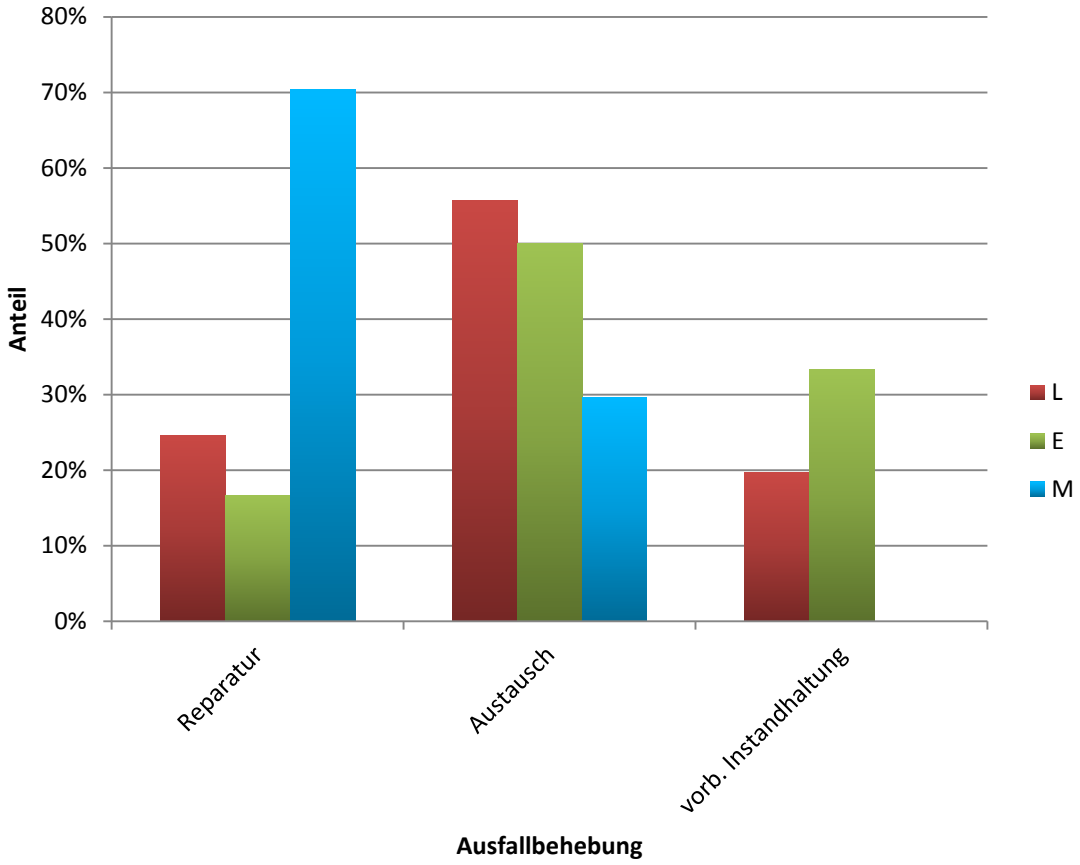

Abb. 4.16 Anteile der Ausfallbehebungsmöglichkeiten für die Komponenten der Elektro- und Leittechnik sowie für Messumformer

Laut Auskunft der Anlagen werden Komponenten, soweit wirtschaftlich vertretbar, bevorzugt repariert. Aus diesem Grund wird die Produktlebensdauer in Abschnitt 5.4 genauer betrachtet.

4.1.4.7 Anlagenzustand bei Ereigniseintritt

Als ergänzende Auswertung wird der jeweilige Anlagenzustand bei Ereigniseintritt betrachtet. Ziel ist es damit die Anzahl der Ereignisse bei den jeweiligen Anlagenzuständen in Relation zu den zeitlichen Anteilen, die die einzelnen Anlagenzustände im Jahr

einnehmen, zu setzen. Für die Anlage SWR A wird diese detailliertere Auswertung in Abschnitt 5.6 vorgenommen.

4.2 SWR B

Bei den erfassten Anlagendaten der Anlage SWR B sind nur die Komponenten aufgeführt, die in Ereignissen bereits auffällig geworden sind. Zusätzlich dazu ist die zum Datensatzerstellungszeitpunkt aktuelle Anzahl dieser am Standort eingesetzter Komponenten mit angegeben. Es handelt es sich dabei um insgesamt 938 Datensätze von programmierbaren oder rechnerbasierten Komponenten. Davon entfallen 726 Datensätze auf Komponenten aus dem Bereich Leittechnik und 212 Datensätze auf den Bereich der Messumformer. Daten zu Elektrotechnik-Komponenten liegen nicht vor.

Für den Betrachtungszeitraum von 1993 bis 2013 wurden der GRS 78 Ereignisse zur Verfügung gestellt. Hiervon entfallen 56 Ereignisse auf den Bereich der Leittechnik und 22 Ereignisse auf den Bereich der Messumformer. Da keine Elektrotechnik-Komponenten mit geliefert wurden, liegen auch keine entsprechenden Ereignisse vor. Darüber hinaus muss für die Anlage SWR B beachtet werden, dass im Vergleich zur Anlage SWR A eine deutlich reduzierte Ereignisanzahl vorliegt. Aus diesem Grund können einige der Auswertungen aus Abschnitt 4.1 nicht durchgeführt werden.

4.2.1 Betriebsmittelart

In diesem Abschnitt erfolgt ausschließlich eine Auswertung der Ereignisdaten nach Betriebsmittelart im Gegensatz zur SWR A-Auswertung (siehe Abschnitt 4.1.1), bei der die Anlagen- und Ereignisdaten ausgewertet wurden. In Abbildung 4.17 ist das Verhältnis der Anzahl der Leittechnik-Ereignisse einer Betriebsmittelart zur Gesamtanzahl der Leittechnik-Ereignisse aufgetragen.

In Abbildung 4.17 ist erkennbar, dass bei der Anlage SWR B etwa 55 % der Ereignisse auf Schreiber (6 fach-Punktschreiber, 3-fach Linienschreiber, Punktschreiber), welche mikroprozessorgesteuert sind, entfallen. Bei diesen Ereignissen handelt es sich zumeist um Fehler, welche den mechanischen Teil des Schreibers und nicht die Software betreffen.

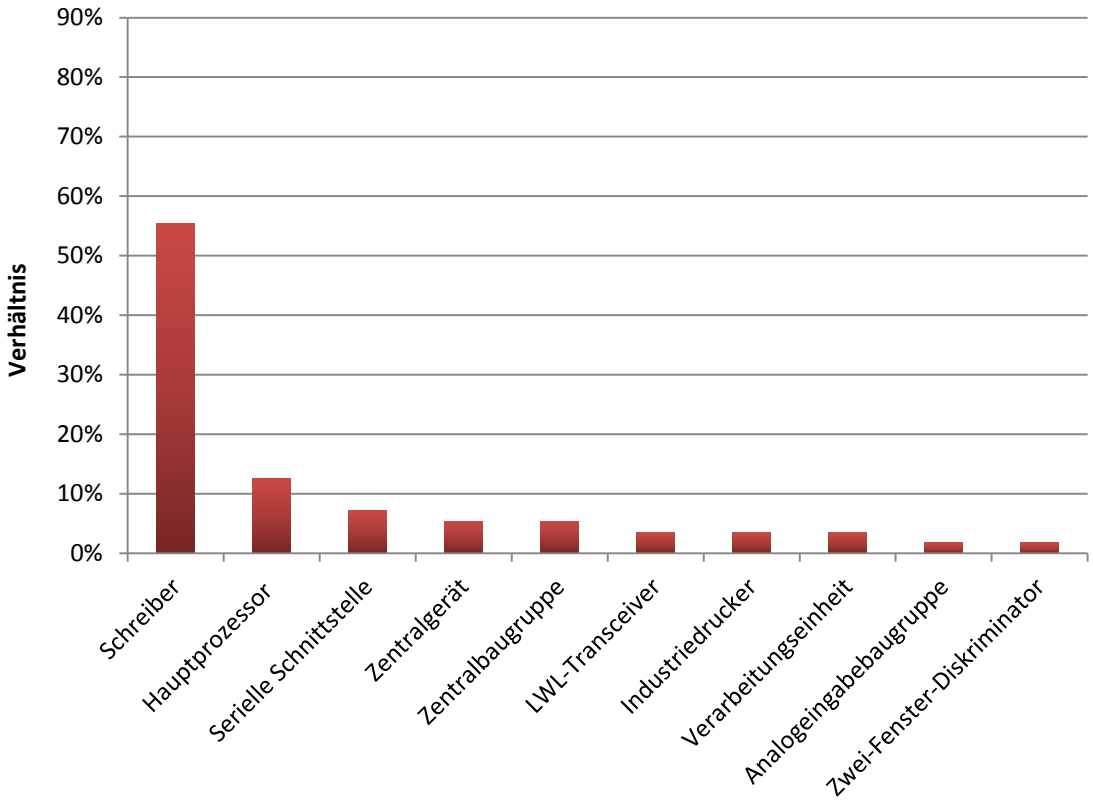

Abb. 4.17 Verhältnis der Anzahl der Leittechnik-Ereignisse einer Betriebsmittelart zur Gesamtanzahl der Leittechnik-Ereignisse für die Anlage SWR B

4.2.2 Zeitlicher Verlauf der Ereignisse

Ähnlich wie in Abschnitt 4.1.2 sind für die Anlage SWR B in Abbildung 4.18 die Anteile der vorliegenden Ereignisse über die jeweiligen Jahre, in denen sie aufgetreten sind, aufgetragen.

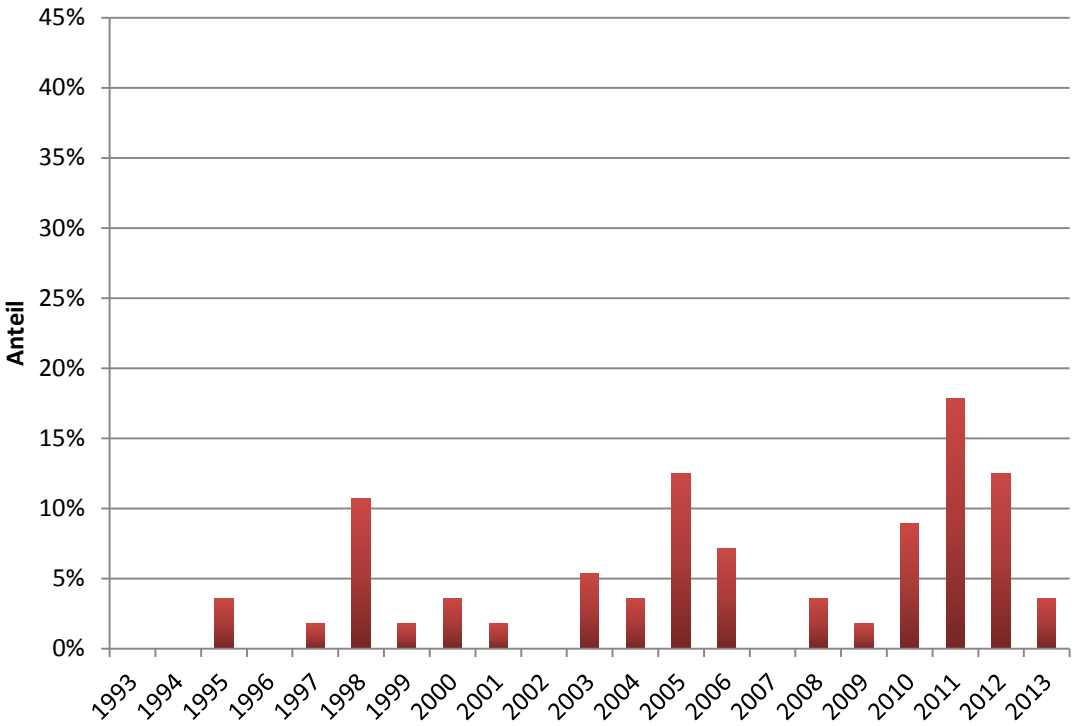

Abb. 4.18 Prozentualer Anteil der Ereignisse pro Jahr in Bezug auf die Gesamtanzahl der Ereignisse für die Leittechnik-Komponenten der Anlage SWR B

Die erhöhte Anzahl an Ereignissen im Jahr 2011 wurde einer genaueren Untersuchung unterzogen. Hierbei stellte sich heraus, dass es eine zeitliche Korrelation zwischen etwa 50 % dieser Fälle gibt. Diese Ereignisse sind auf eine nicht selbstmeldende Alterung von Schreibern zurückzuführen, welche während einer Revision bei wiederkehrenden Prüfungen (WKP) erkannt wurde. Die Ursache dafür waren mechanische Fehler, die Software selbst war nicht betroffen. Für die erhöhte Anzahl an Ereignissen in den Jahren 1998, 2005, 2006, 2010 und 2012 wurden keine signifikanten Zusammenhänge gefunden. Für die Jahre 1993, 1994, 1996 und 2002 wurden keine Ereignisse zu Leittechnik-Komponenten mit geliefert und für das Jahr 2007 wurden der GRS keine Informationen (L und M) vorgelegt.

4.2.3 Hersteller

In diesem Abschnitt werden die Leittechnik-Komponenten hinsichtlich der eingesetzten Hersteller untersucht. Die Anteile der einzelnen Hersteller an den erfassten programmierbaren oder rechnerbasierten Leittechnik-Komponenten des Standorts sind in Abbildung 4.19 dargestellt. Hieraus ergibt sich, dass der Hersteller L mit ca. 43 % und der

Hersteller A mit ca. 38 % den größten Anteil der Komponenten gestellt hat. Die Hersteller B und P waren mit ca. 16 % und ca. 3 % vertreten.

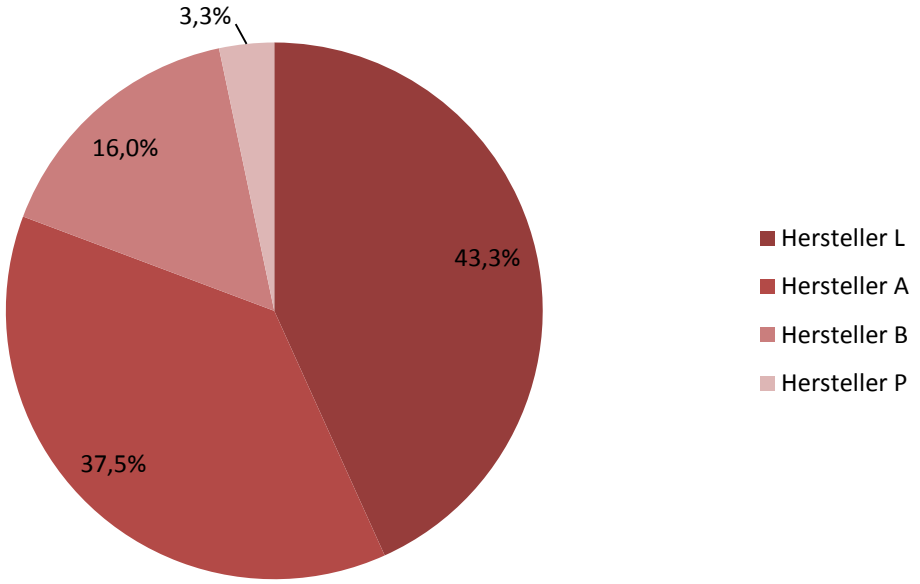

Abb. 4.19 Anteile der Hersteller an den für den Standort der Anlage SWR B erfassten programmierbaren oder rechnerbasierten Leittechnik-Komponenten

In Abbildung 4.20 ist das Verhältnis von Ereignisanzahl an Komponenten eines bestimmten Herstellers zur Anzahl der eingesetzten Komponenten für diesen Hersteller für die erfassten Leittechnik-Komponenten dargestellt. Es zeigt sich, dass von den Komponenten des Herstellers L, welcher mit ca. 43 % den größten Anteil an den eingebauten Leittechnik-Komponenten ausgemacht hat, ca. 4 % von Ereignissen betroffen waren. Von Komponenten des Herstellers B, welche einen Anteil von ca. 16 % an der Gesamtanzahl der Leittechnik-Komponenten hatten, waren ca. 7 % von Ereignissen betroffen. Die Komponenten von Hersteller A hingegen, hatten mit ca. 38 % den zweitgrößten Anteil an den eingebauten Komponenten und von diesen waren im Betrachtungszeitrum ca. 12 % von Ereignissen betroffen. Hersteller P war mit einem kleineren Anteil von ca. 3 % an den eingebauten Komponenten vertreten, wovon etwa 8 % von Ereignissen betroffen waren. Insgesamt wurden keine Auffälligkeiten bezüglich der Ausfallrate der Leittechnik-Komponenten der verschiedenen Hersteller festgestellt.

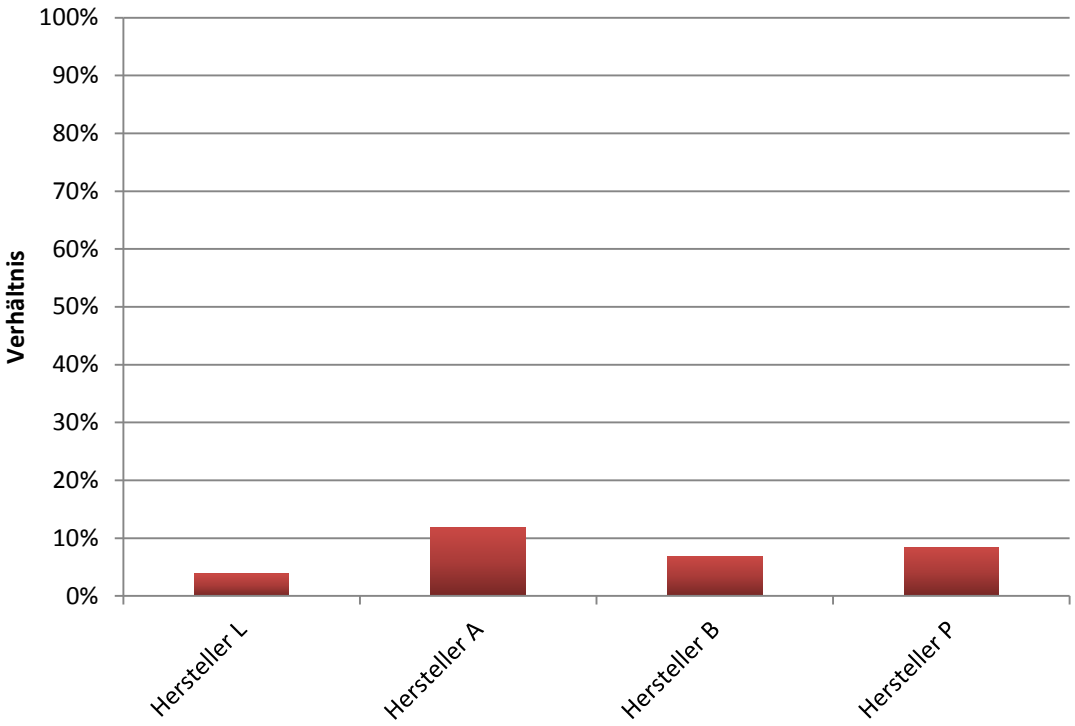

Abb. 4.20 Verhältnis von Ereignisanzahl an Komponenten eines bestimmten Herstellers zur Anzahl der eingesetzten Komponenten für diesen Hersteller für die erfassten Leittechnik-Komponenten der Anlage SWR B

4.2.4 Vergleich zwischen Leittechnik-Komponenten und Messumformern

Wie bereits erwähnt, ist das Ziel des Projektes die in Kernkraftwerken eingesetzten programmierbaren oder rechnerbasierten Leittechnik-Komponenten (L) näher zu untersuchen. Im Gegensatz dazu, werden im Bericht „Analyse zum Einsatz und Betrieb elektrotechnischer Einrichtungen“ /GRS 15/ auch Auswertungen von Elektrotechnik-Komponenten (E) und Messumformern (M) durchgeführt. Da ein Vergleich der Ergebnisse ggf. neue Informationen preisgeben könnte, werden im Folgenden insbesondere die Charakteristika der Komponentenarten L und M mit einander verglichen (Daten zu Elektrotechnik-Komponenten lagen in dieser Anlage nicht vor).

Die Farbgebung in den folgenden Abbildungen ist im gesamten Bericht konsistent. Auswertungen von Leittechnik-Komponenten (L) werden in Rot dargestellt und Auswertungen von Messumformern (M) in Blau.

4.2.4.1 Fehlerart

Zuerst werden die Fehlerarten im Bereich der Leittechnik-Komponenten und der Messumformer analysiert. Das Ergebnis ist in Abbildung 4.21 dargestellt. Es zeigt sich, dass im Bereich der Leittechnik die Hälfte der Ereignisse nicht selbstmeldend war und bei den Messumformern dieser Anteil bei ca. 36 % lag. Im Gegensatz dazu entfallen in diesem Fall auf die selbstmeldenden Fehler ca. 43 % der Ereignisse mit Messumformern und etwa 34 % auf Ereignisse mit Leittechnik-Komponenten.

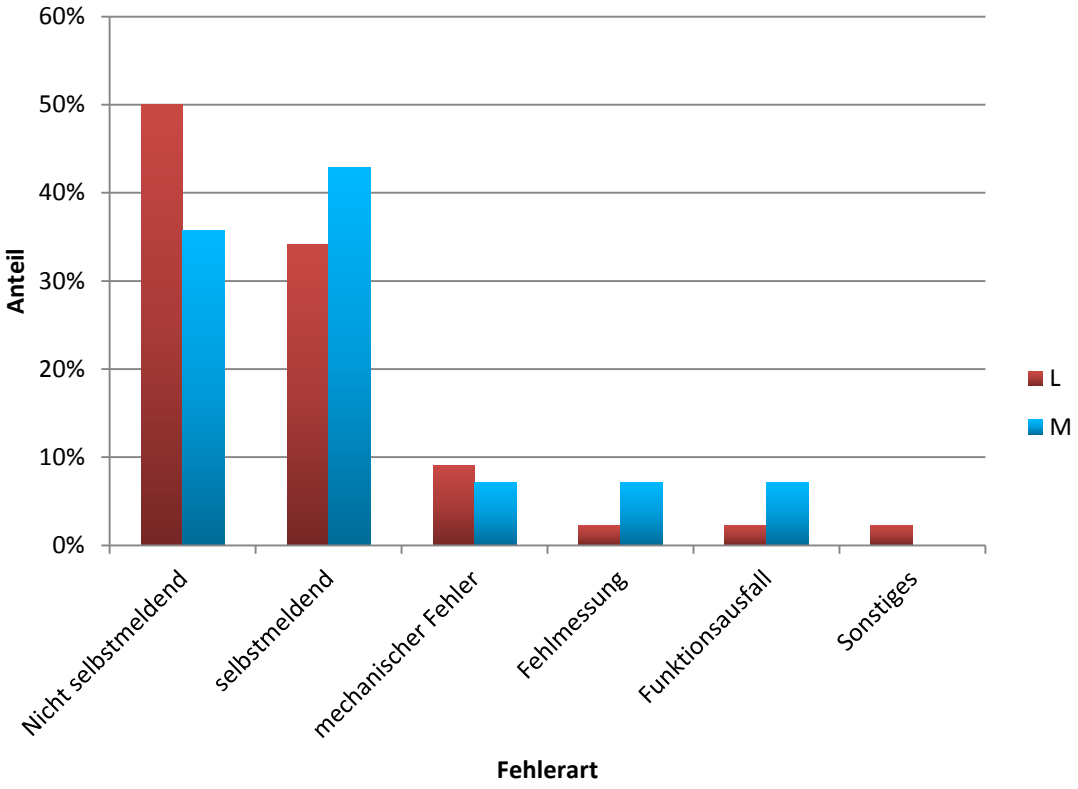

Abb. 4.21 Anteile der verschiedenen Fehlerarten in der Anlage SWR B für die Leittechnik-Komponenten sowie für Messumformer

Aus Abbildung 4.21 ergibt sich zudem, dass die mechanischen Fehler im Bereich der Leittechnik bei ca. 9 % lagen. Dieser Wert ist wieder nur als untere Schranke für mechanische Fehler anzusehen. Diese Fehler sind wie bereits oben erwähnt auf Schreiber zurückzuführen. Es kann zudem gesehen werden, dass ca. 7 % der Ereignisse mechanische Fehler im Bereich Messumformer waren. Fehlmessungen waren im Bereich der Leittechnik die Ursache für etwa 2 % und bei den Messumformern für etwa 7 % der Ereignisse verantwortlich. Sonstige Fehler und Funktionsausfälle beliefen sich

bei den Leittechnik-Komponenten auf jeweils ca. 2 %, während es bei den Messumformern 0 % und ca. 7 % waren.

Zu der Fehlerart „Sonstiges“ liegen keine näheren Informationen vor.

Da, wie gerade dargestellt, ein großer Anteil der Ereignisse sowohl bei den Komponenten der Leittechnik als auch bei den Messumformern auf nicht selbstmeldende Fehler zurückzuführen ist, und diese wie bereits in Abschnitt 4.1.4.4 von besonderem Interesse sind, wird diese Fehlerart im Folgenden genauer betrachtet.

Abbildung 4.22 zeigt den Anteil der jeweiligen Fehlererkennungsart von nicht selbstmeldenden Fehlern im Bereich der Leittechnik-Komponenten und der Messumformer. Durch Betriebsstörungen wurden etwa 40 % der Ereignisse mit Leittechnik-Komponenten und drei Viertel der Ereignisse im Bereich der Messumformer auffällig.

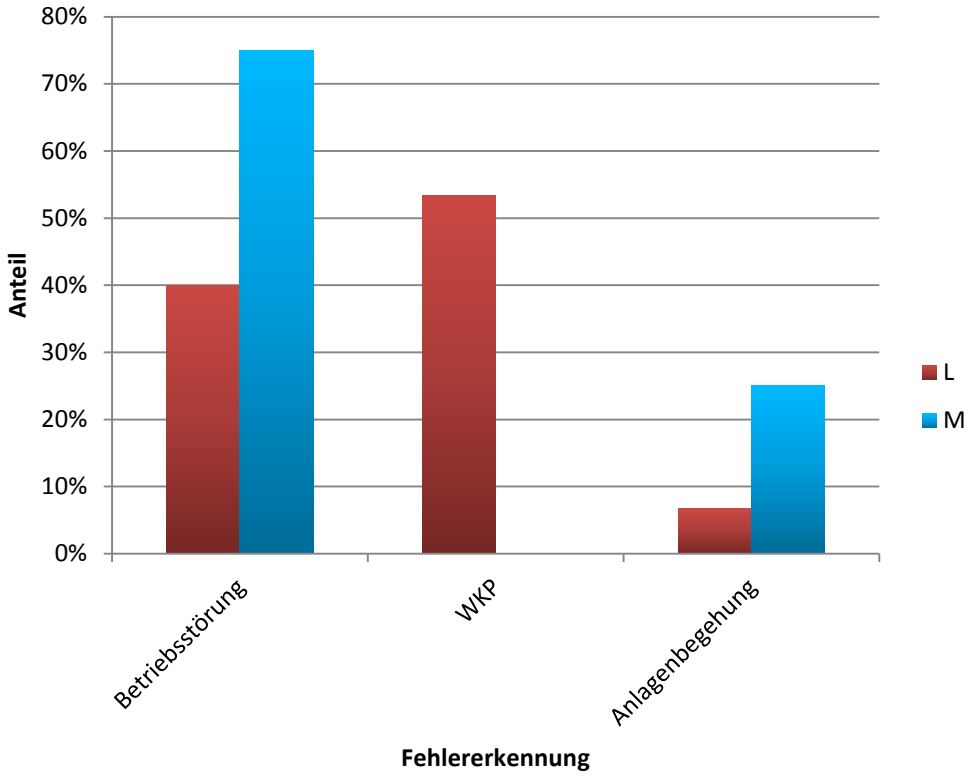

Abb. 4.22 Anteile der verschiedenen Fehlererkennungsarten für die nicht selbstmeldenden Fehler aus Abb. 4.21

Etwas über 50 % der Ereignisse mit Leittechnik-Komponenten wurden bei einer wiederkehrenden Prüfung (WKP) entdeckt, wobei es sich hier nur um Ereignisse mit

Schreibern handelt. Ereignisse der Messumformer wurden nicht bei einer WKP entdeckt. Zusätzlich wurden ca. 7 % der Ereignisse bei Leittechnik-Komponenten und ca. 25 % der Ereignisse bei Messumformern bei Anlagenbegehung erkannt.

4.2.4.2 Fehlererkennung

Basierend auf der vorangegangenen Auswertung, werden im Folgenden die möglichen Fehlererkennungsarten bezogen auf alle Ereignisse der Anlage genauer analysiert. Die entsprechenden Anteile für die Leittechnik-Komponenten und Messumformer sind in Abbildung 4.23 dargestellt.

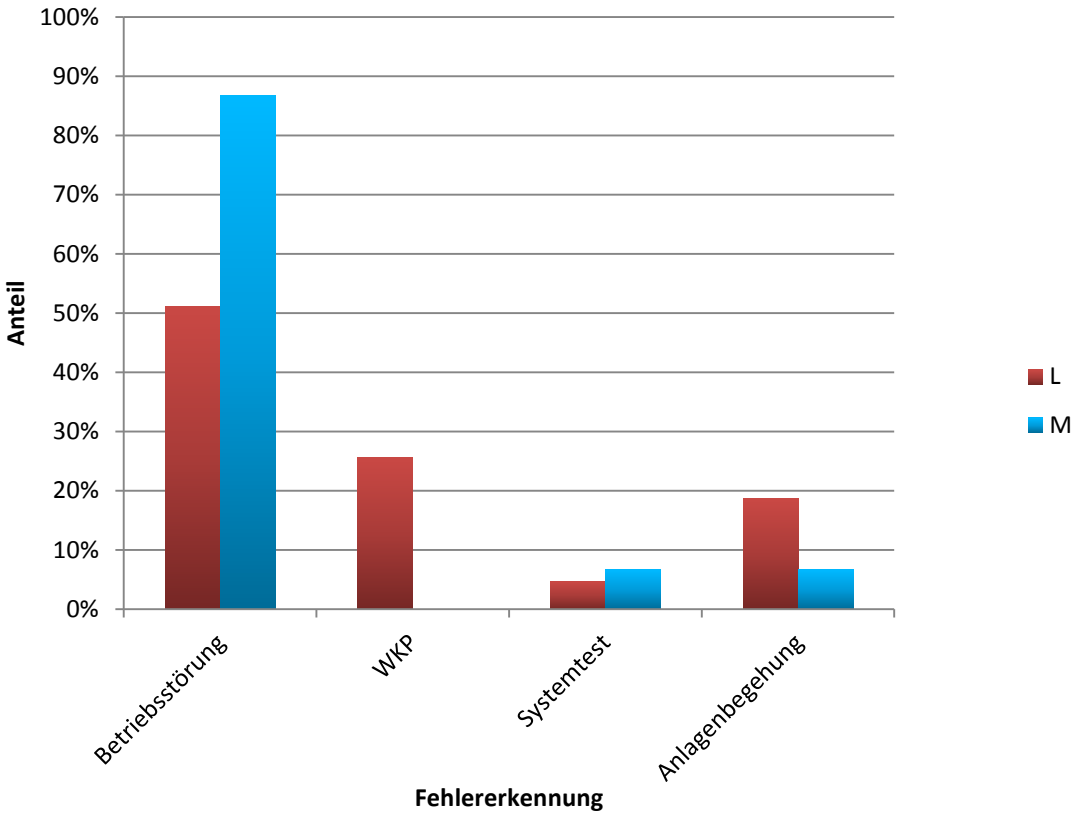

Abb. 4.23 Anteile der verschiedenen Fehlererkennungsarten in der Anlage SWR B für die Komponenten der Leittechnik sowie für Messumformer

Der weitaus größte Anteil mit ca. 87 % der Ereignisse konnte für die Messumformer aufgrund einer Betriebsstörung erkannt werden, während es bei Komponenten der Leittechnik etwas mehr als die Hälfte der Ereignisse waren. Die hohe Anzahl an Ereignissen mit Messumformern kann auf Driftereignisse zurückgeführt werden.

Bei einer wiederkehrenden Prüfung (WKP) wurden ca. 26 % der Ereignisse mit Leittechnik-Komponenten erkannt, wohingegen diese Art der Fehlererkennung bei Messumformern nicht zum Tragen kam. Bei diesen Ereignissen der Leittechnik-Komponenten waren zum größten Teil (ca. 91 %) Schreiber involviert.

Etwa 5 % der Fehler wurden bei den Ereignissen mit Leittechnik-Komponenten durch einen Systemtest erkannt und etwa 19 % durch eine Anlagenbegehung. Bei den Ereignissen mit Messumformern waren es in beiden Fällen ca. 7 %. Im Bereich der Leittechnik sind ca. 88 % der Ereignisse, welche durch eine Anlagenbegehung erkannt wurden, auf defekte Schreiber zurückzuführen.

4.2.4.3 Ursache

Aus den erfassten Daten zur Anlage SWR B konnte im Vergleich zu den Auswertungen der SWR A-Daten zusätzlich die jeweilige Ursache der Ereignisse untersucht werden. Abbildung 4.24 zeigt die Anteile der jeweiligen Ursache für die Leittechnik-Komponenten und die Messumformer.

Es ist deutlich, dass sowohl für die Leittechnik-Komponenten als auch für die Messumformer der größte Anteil der Ereignisse mit ca. 36 % bzw. etwa 58 % auf die Alterung der Komponenten entfallen ist. Ein Blick auf die zugehörigen Komponenten ergibt, dass die Ereignisse in der Leittechnik größtenteils von Schreibern verursacht wurden und die Messumformer-Ereignisse u. a. aufgrund von ausgefallenen Pufferbatterien hervorgerufen wurden (siehe hierzu Abschnitt 5.2).

Des Weiteren ergibt sich aus Abbildung 4.24, dass die Ursache für ca. 32 % der Ereignisse in der Leittechnik als „Sonstiges“ deklariert ist. Weiterhin fallen die ca. 24 % der Leittechnik-Ereignisse auf, die durch mechanische Fehler verursacht worden sind. Hierbei ist zu beachten, dass es sich ausschließlich um Schreiber-Ereignisse handelt. Darüber hinaus ist erkennbar, dass die Ereignisse mit Messumformern mit etwa 8 % gleichverteilt auf die Ursachen „Bauelementausfall“, „unzulässige Werte“, „defektes elektronisches Bauteil“, „Drift“ und „Sonstiges“ aufgeteilt sind.

Zu der Ursache „Sonstiges“ liegen keine näheren Informationen vor.

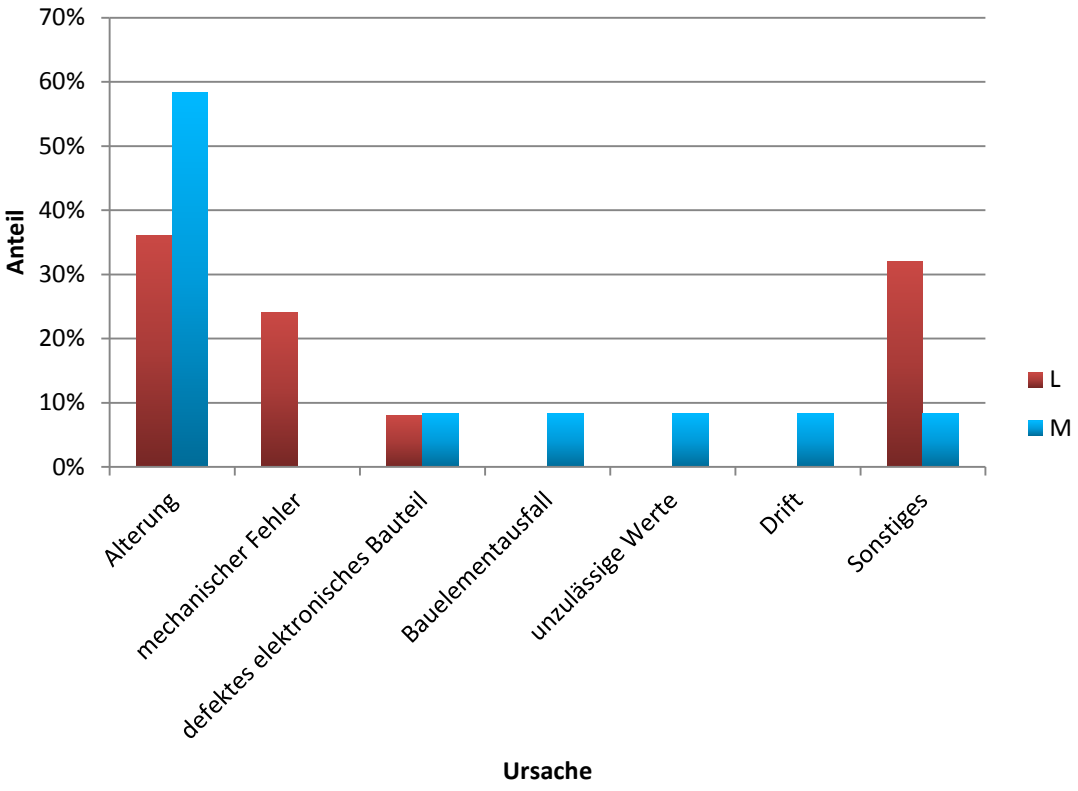

Abb. 4.24 Anteile der verschiedenen Ursachen für die Ereignisse in der Anlage SWR B für die Komponenten der Leittechnik sowie für Messumformer

4.2.4.4 Anlagenzustand bei Ereigniseintritt

In Abbildung 4.25 sind die Anteile der Anlagenzustände bei Ereigniseintritt dargestellt. Es ist ersichtlich, dass im Betrieb der Anlage ca. 47 % der Ereignisse mit Leichttechnik-Komponenten und ca. 90 % der Ereignisse mit Messumformer entdeckt wurden. Da bei den SWR B-Daten der Anlagenzustand nur in „Betrieb“ und „Revision“ unterteilt ist, zeigt Abbildung 4.25 folgerichtig, dass bei Revision ca. 53 % der Ereignisse mit Leittechnik-Komponenten und ca. 10 % der Ereignisse mit Messumformern entdeckt wurden. Im Bereich der Leittechnik liegt der Anteil defekter Schreiber an den bei Revision entdeckten Ereignissen bei ca. 62 %.

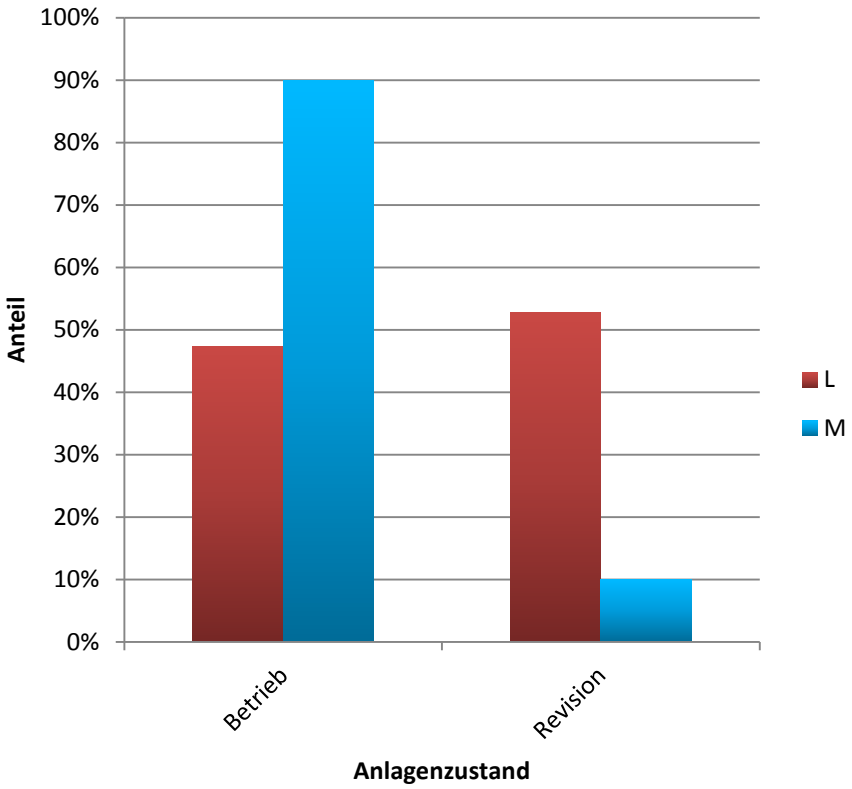

Abb. 4.25 Anteile der Anlagenzustände bei Ereigniseintritt in der Anlage SWR B für die Komponenten der Leittechnik sowie für Messumformer

In Abschnitt 5.6 wird für die Anlage SWR A die Anzahl der Ereignisse bei den jeweiligen Anlagenzuständen in Relation zu den zeitlichen Anteilen, die die einzelnen Anlagenzustände im Jahr einnehmen, gesetzt. Aufgrund der geringen Datendichte für die Anlage SWR B wird dieses hier nicht gemacht.

4.3 DWR A

Im Gegensatz zur Anlage SWR A sind in den erfassten Anlagendaten der Anlage DWR A nur die Komponenten aufgeführt, die in Ereignissen bereits auffällig geworden sind. Zusätzlich dazu ist die zum Datensatzerstellungszeitpunkt aktuelle Anzahl dieser am Standort eingesetzter Komponenten mit angegeben. Es handelt sich insgesamt um 2734 Datensätze zu programmierbaren oder rechnerbasierten Komponenten. Hierbei entfallen 1292 Komponenten auf den Bereich Leittechnik, 387 Komponenten auf den Bereich Elektrotechnik und 1055 Komponenten auf den Bereich Messumformer.

Für den Betrachtungszeitraum von 2006 bis 2013 wurden der GRS insgesamt 157 Ereignisse übermittelt. Hiervon entfallen 74 Ereignisse auf den Bereich Leittechnik, 6 Ereignisse auf den Bereich Elektrotechnik und 77 Ereignisse auf den Bereich Messumformer. Darüber hinaus muss für die Anlage DWR A beachtet werden, dass im Vergleich zur Anlage SWR A eine deutlich reduzierte Ereignisanzahl vorliegt. Aus diesem Grund können einige der Auswertungen aus Abschnitt 4.1 nicht durchgeführt werden.

4.3.1 Betriebsmittelart

Wie bereits bei den Anlagen SWR A und SWR B erfolgt in diesem Abschnitt eine Auswertung der Daten hinsichtlich der eingesetzten Betriebsmittelarten. Hierfür ist das Verhältnis der Anzahl der Leittechnik-Ereignisse einer Betriebsmittelart zur Gesamtanzahl der Leittechnik-Ereignisse in Abbildung 4.26 aufgetragen.

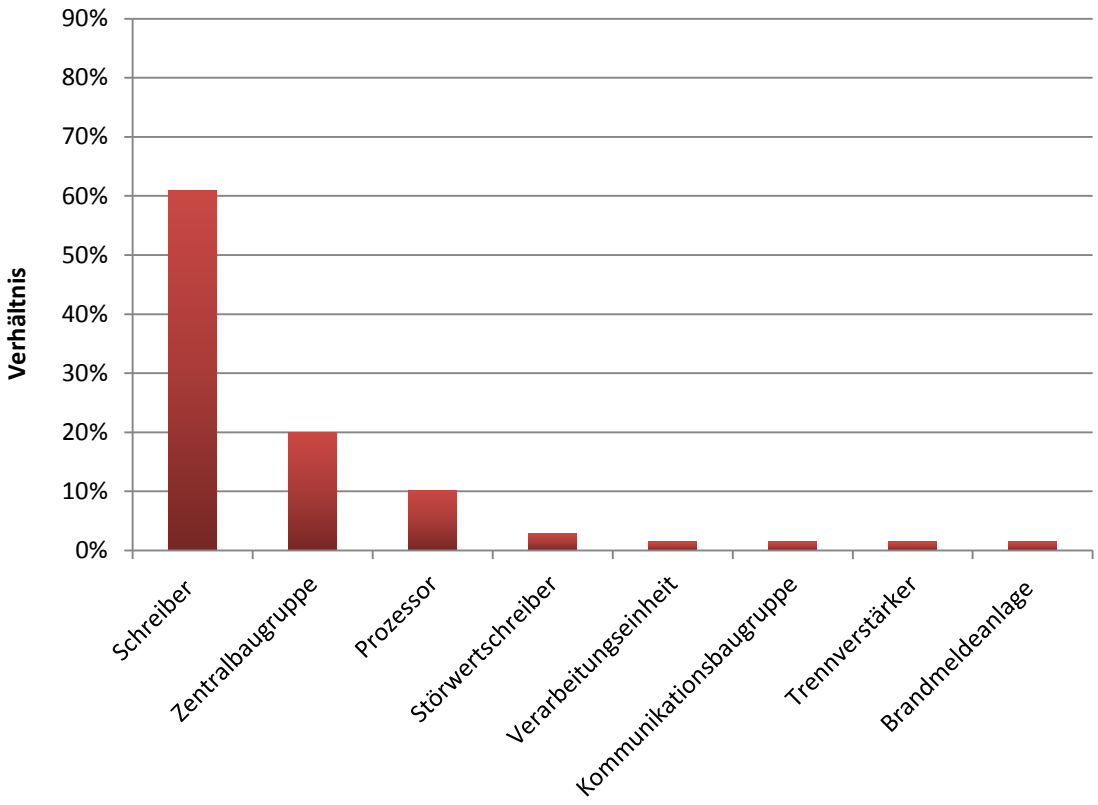

Abb. 4.26 Verhältnis der Anzahl der Leittechnik-Ereignisse einer Betriebsmittelart zur Gesamtanzahl der Leittechnik-Ereignisse für die Anlage DWR A

Es ist deutlich erkennbar, dass ca. 61 % der Ereignisse mit Leittechnik-Komponenten auf mikroprozessorgesteuerte Schreiber (insbesondere Punktschreiber) zurückzufüh-

ren sind. Wie die folgenden Auswertungen noch zeigen werden, beziehen sich die meisten dieser Ereignisse auf den mechanischen Teil der Schreiber. Aus dung 4.26 kann zudem entnommen werden, dass ca. 20 % der Ereignisse von Leittechnik-Komponenten auf Zentralbaugruppen entfallen und ca. 10 % auf Prozessoren.

4.3.2 Zeitlicher Verlauf der Ereignisse

Wie bei der Auswertung für die Anlagen SWR A und SWR B erfolgt in Abbildung 4.27 eine Auftragung der Anteile der vorliegenden Leittechnik-Ereignisse über die jeweiligen Jahre, in denen sie aufgetreten sind (siehe Abschnitt 4.1.2 und 4.2.2).

Im Gegensatz zu den beiden erwähnten Auswertungen ist hier keine Besonderheit bei den verschiedenen Anteilen erkennbar. Auch die genauere Analyse der Ereigniseintrittszeiten blieb ohne Befund.

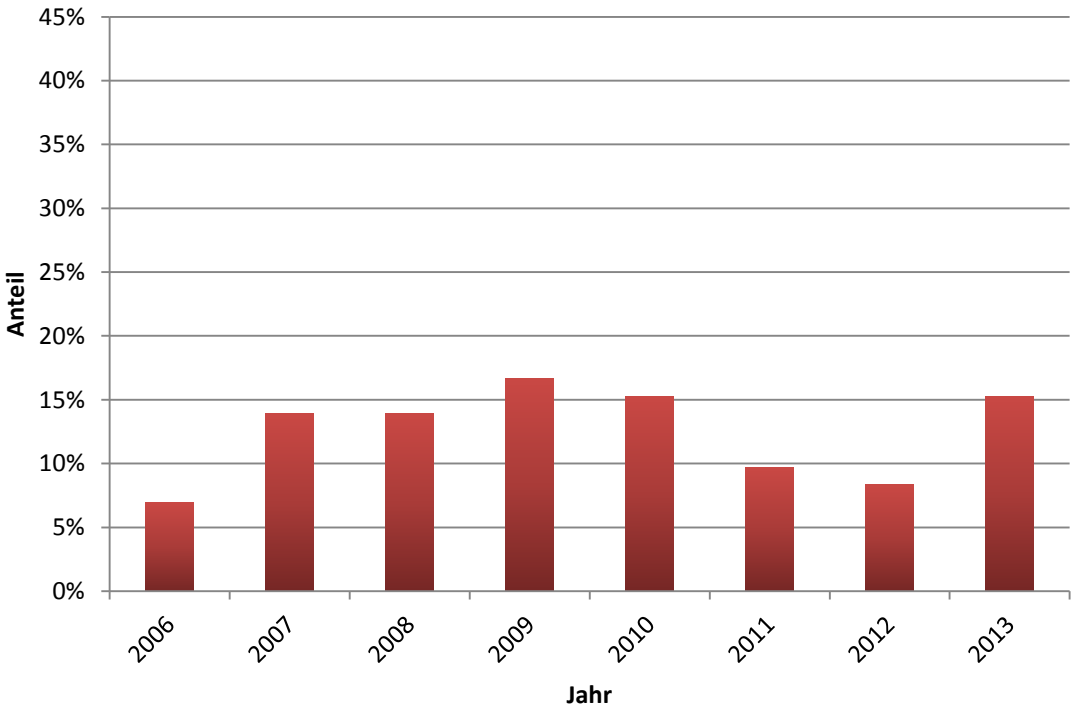

Abb. 4.27 Prozentualer Anteil der Ereignisse pro Jahr in Bezug auf die Gesamtanzahl der Ereignisse für die Leittechnik-Komponenten der Anlage DWR A

4.3.3 Hersteller

Im Folgenden wird analysiert, welche Hersteller hinsichtlich der erfassten Leittechnik-Komponenten in der Anlage DWR A eingesetzt waren und welchen Anteil der jeweilige Hersteller bei den zugehörigen Ereignissen hatte.

In Abbildung 4.28 ist dargestellt, welche Hersteller am Standort eingesetzt waren und welchen Anteil diese an den Leittechnik-Komponenten hatten. Von den insgesamt betrachteten 1292 eingesetzten Leittechnik-Komponenten war der überwiegende Anteil von ca. 88 % von Hersteller A. Ein weitaus geringerer Anteil fiel auf den Hersteller I (ca. 10 %). Der Hersteller G war mit ca. 2 % am geringsten bei den Leittechnik-Komponenten vertreten.

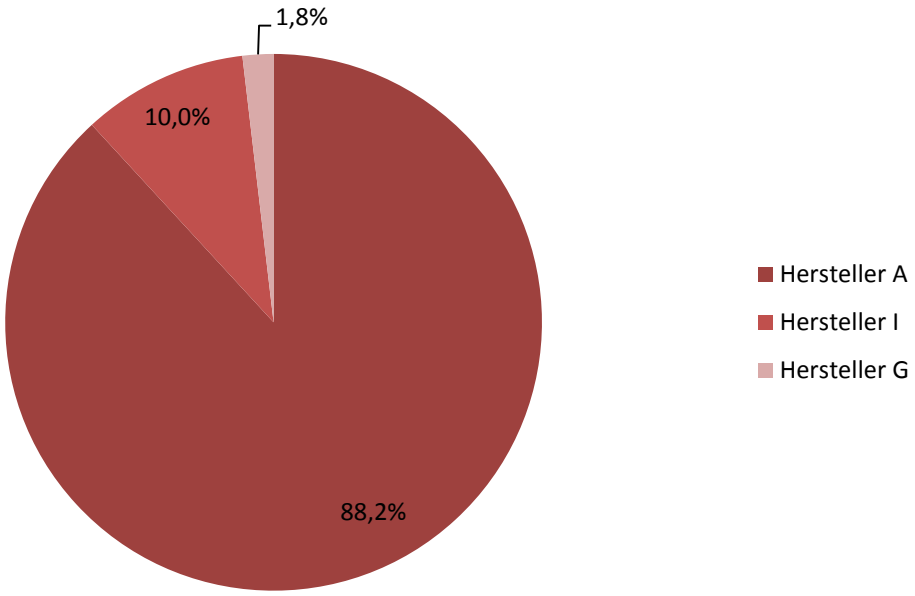

Abb. 4.28 Anteile der Hersteller an den für den Standort der Anlage DWR A erfassten programmierbaren oder rechnerbasierten Leittechnik-Komponenten

Aufbauend darauf ist in Abbildung 4.29 das Verhältnis von Ereignisanzahl an Komponenten eines bestimmten Herstellers zur Anzahl der eingesetzten Komponenten für diesen Hersteller für die erfassten Leittechnik-Komponenten dargestellt. Hierbei hat sich gezeigt, dass von den Komponenten des Herstellers A, welcher mit ca. 88 % den größten Anteil an den eingebauten Leittechnik-Komponenten ausgemacht hat, ca. 6 % von Ereignissen betroffen waren. Auf die Komponenten des Herstellers I, welche einen Anteil von ca. 10 % an der Gesamtanzahl der erfassten Leittechnik-Komponenten hat-

te, entfielen ca. 2 % der Ereignisse. Die Komponenten von Hersteller G hatten einen Anteil von ca. 4 %. Da in dieser Auswertung keine Auffälligkeiten erkennbar waren, wurde hier auf eine weitere detailliertere Analyse verzichtet.

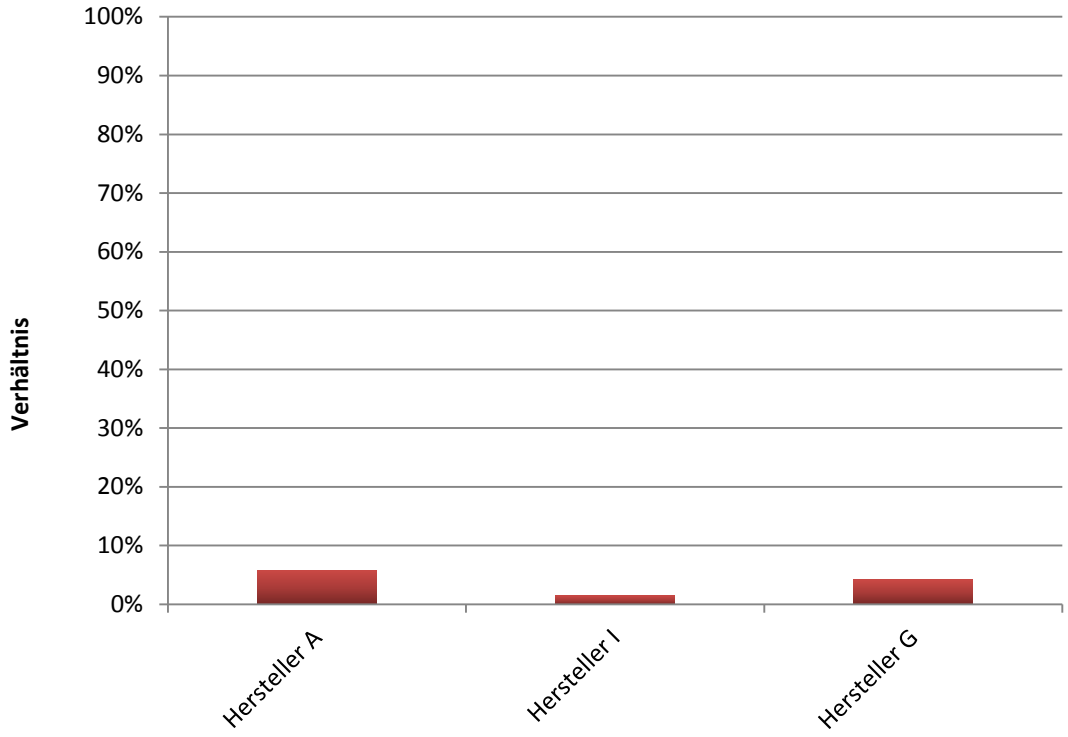

Abb. 4.29 Verhältnis von Ereignisanzahl an Komponenten eines bestimmten Herstellers zur Anzahl der eingesetzten Komponenten für diesen Hersteller für die erfassten Leittechnik-Komponenten der Anlage DWR A

4.3.4 Vergleich zwischen Leittechnik-Komponenten und Messumformern

Wie bereits erwähnt, ist das Ziel des Projektes die in Kernkraftwerken eingesetzten programmierbaren oder rechnerbasierten Leittechnik-Komponenten (L) näher zu untersuchen. Im Gegensatz dazu, werden im Bericht „Analyse zum Einsatz und Betrieb elektrotechnischer Einrichtungen“ /GRS 15/ auch Auswertungen von Elektrotechnik-Komponenten (E) und Messumformern (M) durchgeführt. Bei der Auswertung zur Anlage DWR A stellte sich hier jedoch heraus, dass nur wenige Ereignisse mit Elektrotechnik-Komponenten vorhanden waren und somit eine aussagekräftige Auswertung nicht möglich war. In dem folgenden Vergleich wird daher auf die Einbeziehung der Elektrotechnik-Komponenten verzichtet.

Die Farbgebung in den folgenden Abbildungen ist im gesamten Bericht konsistent. Auswertungen von Leittechnik-Komponenten (L) werden in Rot dargestellt und Auswertungen von Messumformern (M) in Blau.

4.3.4.1 System

Aufgeführt sind in Abbildung 4.30 die von Ereignissen betroffenen Systeme für die Leittechnik-Komponenten und in Abbildung 4.31 für die Messumformer. Für eine bessere Übersicht sind in beiden Abbildungen nur die Systeme dargestellt, die einen Anteil von größer als 3 % haben.

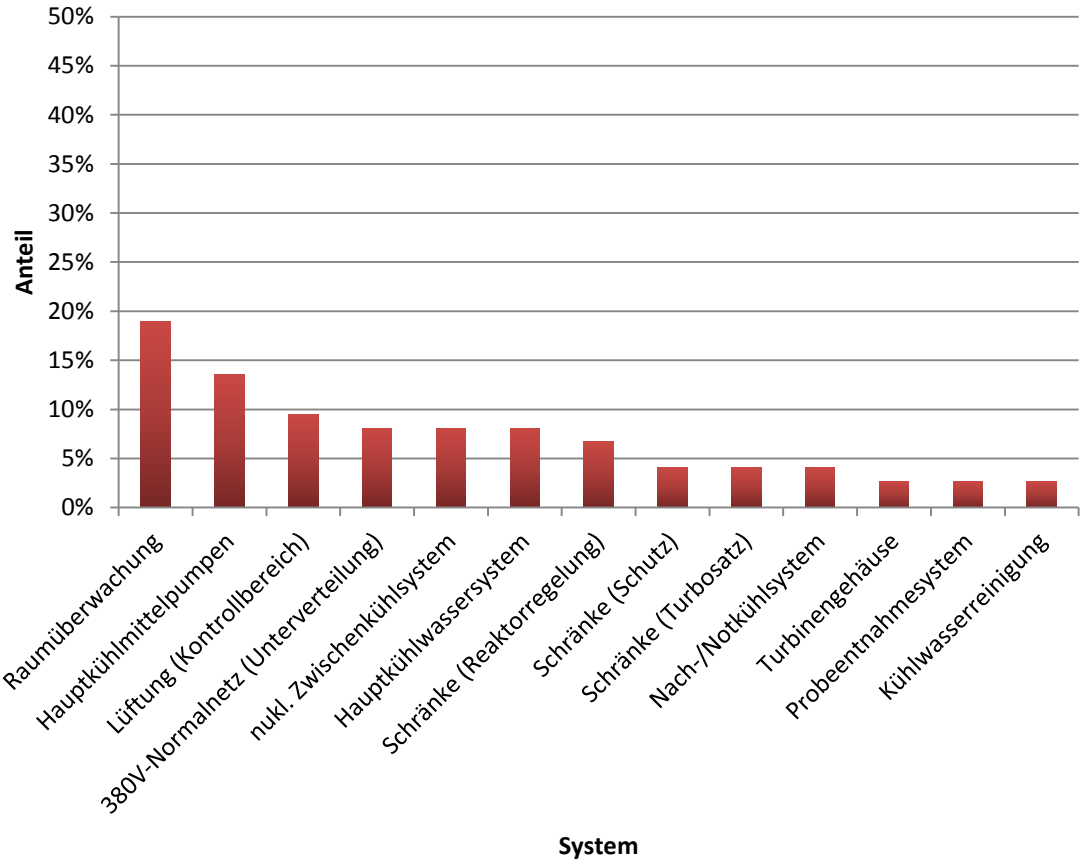

Abb. 4.30 Anteile der von Leittechnik-Ereignissen betroffenen Systeme in der Anlage DWR A

Aus Abbildung 4.29 kann entnommen werden, dass knapp 19 % der Leittechnik-Ereignisse dem Bereich der Raumüberwachung zugeschrieben werden konnten. Hierbei handelt es sich zum größten Teil um Ausfälle von Punktschreibern. Am zweithäu-

figsten ist das System der Hauptkühlmittelpumpen von Fehlern betroffen gewesen (ca. 14 %), wobei es sich auch hier meistens um Punktschreiber handelt. Im Bereich von 8 % liegen in diesem Fall die Systeme der Lüftung für den Kontrollbereich, des 380kV-Normalnetzes der Unterverteilung, des nuklearen Zwischenkühlsystems, des Hauptkühlwassersystems und der Reaktorregelungsschränke. Alle anderen Systeme hatten einen Anteil von kleiner als 5 %.

Für die Messumformer-Ereignisse ist in Abbildung 4.31 erkennbar, dass in ca. 14 % der Fälle das Ereignis im Hauptkühlwassersystem aufgetreten ist. Bei jeweils ca. 6 % der Messumformer-Ereignisse waren die Systeme der Wasserstoffversorgung für den Generator, der Lüftung für den Kontrollbereich und der Notstromdieselaggregate betroffen. Noch weiter zu erwähnen sind die Systeme der Speisewasserförderung und der Reinigungsanlage für Kühlwassersysteme die beide jeweils einen Anteil von ca. 5 % hatten. Alle anderen Systeme liegen bei einem Anteil von kleiner als 5 %.

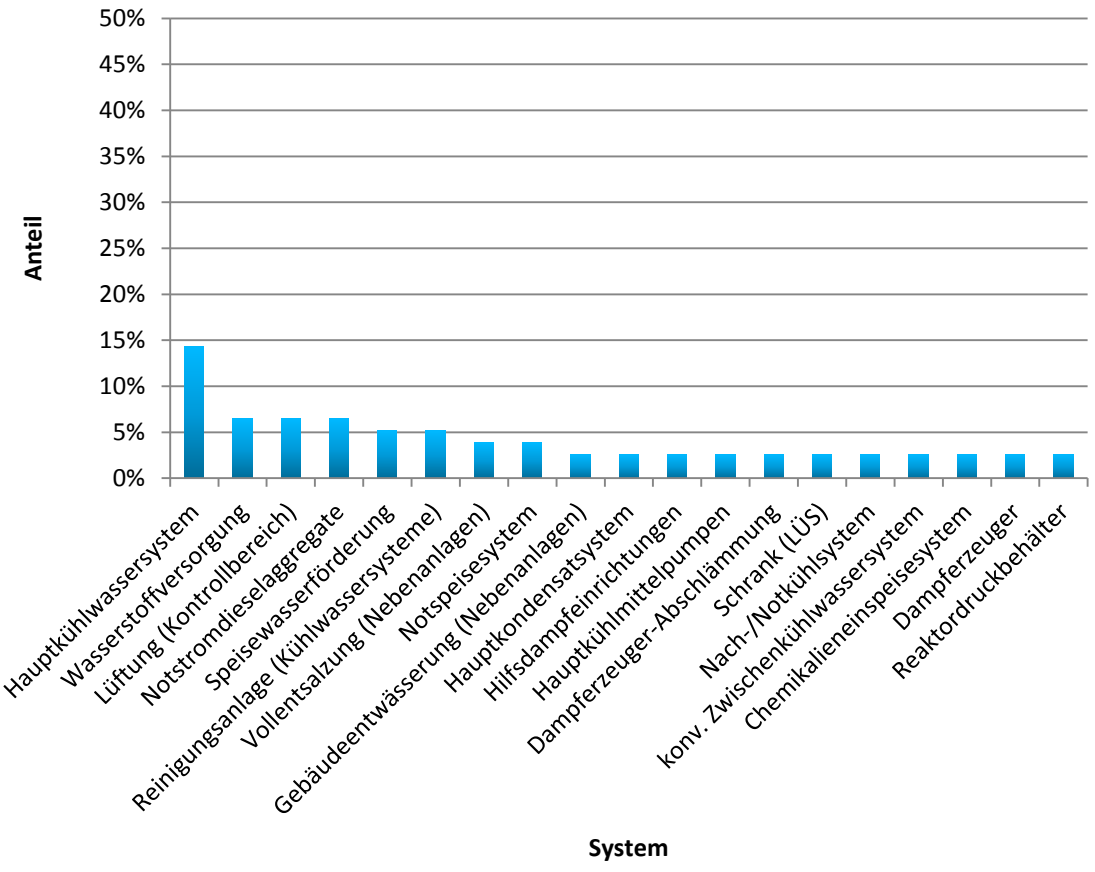

Abb. 4.31 Anteile der von Messumformer-Ereignissen betroffenen Systeme in der Anlage DWR A

4.3.4.2 Auswirkungen

Im Gegensatz zu der Auswertung für die Anlagen SWR A und SWR B konnten die Daten der Anlage DWR A hinsichtlich der Auswirkungen, welche durch die Ereignisse verursacht wurden, untersucht werden. In Abbildung 4.32 sind dafür die jeweiligen Anteile der verschiedenen Auswirkungen dargestellt. Zur besseren Übersicht wurden die Auswirkungen, die für die Leittechnik und die Messumformer einen Anteil von kleiner als 3 % haben, nicht mit in das Diagramm aufgenommen.

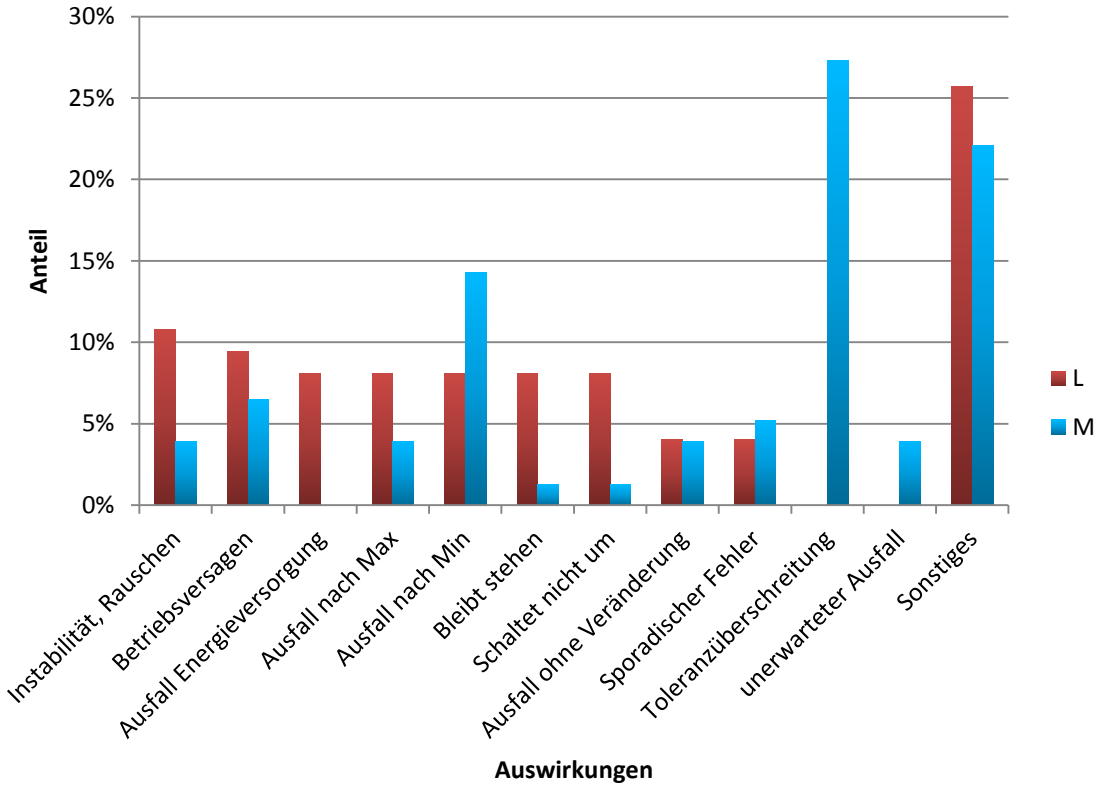

Abb. 4.32 Anteile der Auswirkungen der Ereignisse in der Anlage DWR A für die Komponenten der Leittechnik sowie für Messumformer

In etwa einem Zehntel der Fälle resultierte das Ereignis bei den Leittechnik-Komponenten entweder in „Instabilität, Rauschen“ oder „Betriebsversagen“. Messumformer waren am häufigsten von Toleranzüberschreitungen und Ausfällen nach Min bzw. Max betroffen, was den oben bereits mehrfach diskutierten Driftereignissen entspricht (siehe Abschnitt 5.9). Die Toleranzüberschreitungen bei den Messumformern liegen bei etwa 27 %, während diese Ereignisse bei der Leittechnik nicht vorhanden sind. Zur Kategorie „Sonstiges“ liegen keine weiteren Informationen vor.

4.3.4.3 Fehlererkennung

In diesem Abschnitt wird ausgewertet, wie die jeweiligen Ereignisse in der Anlage erkannt wurden. Hierfür sind in Abbildung 4.33 die jeweiligen Anteile der einzelnen Erkennungsarten „Prüfung“, „Anforderung“, „Betrieb“, „Begehung/Überwachung vor Ort“ und „Wartenüberwachung/Meldung“ aufgetragen.

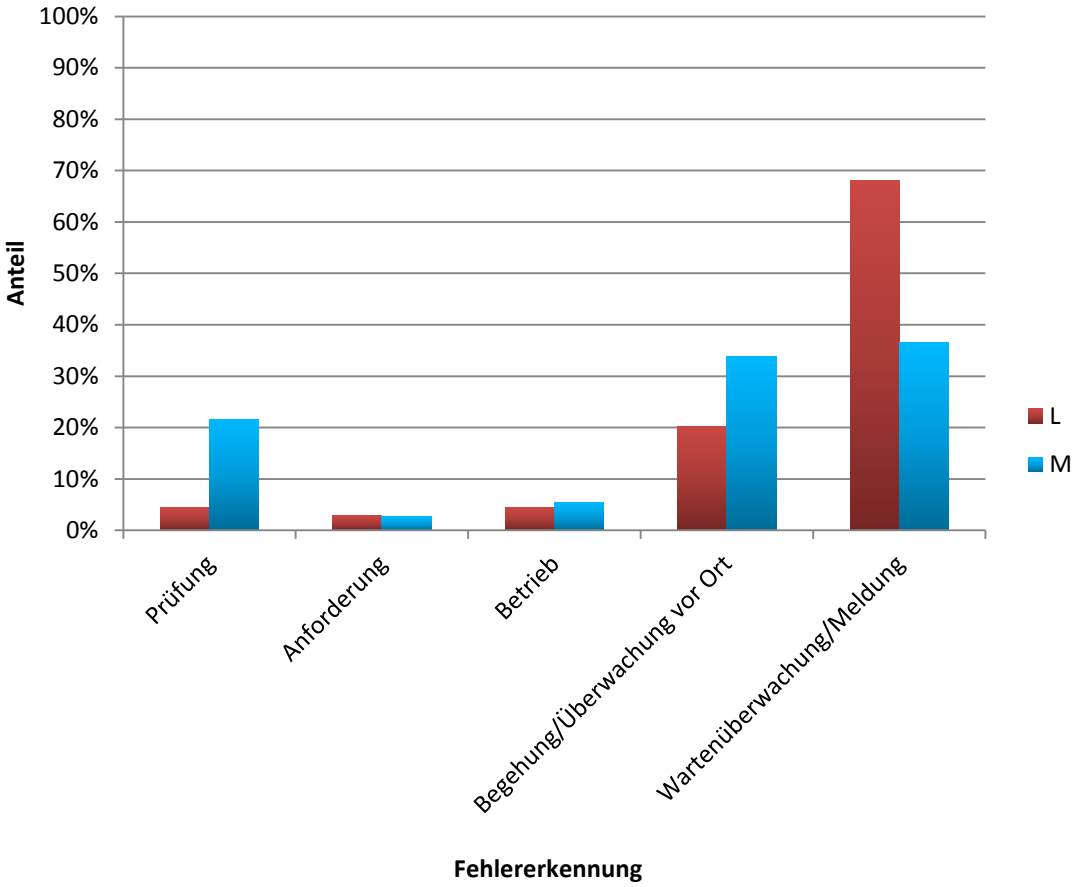

Abb. 4.33 Anteile der verschiedenen Fehlererkennungsarten in der Anlage DWR A für die Komponenten der Leittechnik sowie für Messumformer

Abbildung 4.33 zeigt, dass die Fehlererkennung „Prüfung“ für die Leittechnik-Komponenten einen sehr geringen Anteil hatte (ca. 4 %), wohingegen sie mit ca. 22 % für die Messumformer vermehrt zum Erfolg geführt hat. Aus den weiteren Unterlagen ergibt sich hieraus aber keine Tendenz zu bestimmten Fehlermechanismen.

In Abschnitt 4.1.4.3 wurde betont, dass die Fehlererkennung bei Anforderung von besonderem Interesse ist. Bei dieser Anlage liegen der Fehlererkennung durch Anforderung nur sehr wenige Ereignisse zugrunde, weshalb diese Thematik im vorliegenden

Bericht nicht weiter verfolgt wird. Die Ereignisse, die während des Betriebes erkannt wurden, stellen ebenfalls eine sehr geringe Anzahl dar und werden auch nicht weiter verfolgt.

In Bereich der Leittechnik wurden etwa 20 % der Ereignisse, bei Messumformern ca. 34 % bei einer Begehung/Überwachung vor Ort festgestellt. Bei näherer Betrachtung der Leittechnik-Ereignisse zeigt sich, dass es sich hierbei in fast einem Drittel der Fälle um einen Softwareausfall oder Programmierungsfehler handelt. Im Vergleich dazu lag bei den Messumformern der Anteil der Softwareausfälle oder Programmierungsfehler nur bei ca. 5 % und damit deutlich niedriger. Ein Fünftel dieser Softwareausfälle waren Displayfehler, welche aber keinen direkten Einfluss auf die Funktion des Messumformers selbst haben (siehe Abschnitt 5.1).

Etwas über zwei Drittel der Ereignisse mit Leittechnik-Komponenten und etwa ein Drittel der Messumformer-Ereignisse wurden durch „Wartenüberwachung/Meldung“ erkannt. Bei beiden Komponentenarten liegt in diesem Fall der Anteil der Softwareausfälle oder Programmierungsfehler bei ca. 17 %.

4.3.4.4 Ursache

Die Anteile der jeweiligen Ursache für die verschiedenen Ereignisse ist in dung 4.34 für die Leittechnik-Komponenten und die Messumformer dargestellt. Zur besseren Übersicht wurden die Ursachen, die für die Ereignisse der Leittechnik und der Messumformer einen Anteil von kleiner als 3 % aufweisen, nicht mit in das Diagramm aufgenommen.

Bei der Ursache „Verschleiß, Korrosion, Werkstofffehler“ waren bei den Leittechnik-Komponenten und bei den Messumformern zum größten Teil nur mechanische Komponenten betroffen. Das gleiche gilt für die Leittechnik-Komponenten mit der Ursache „Bauelementausfall (ohne äußeren erkennbaren Einfluss)“.

Im Gegensatz zu den Messumformern (ca. 1 %) liegt der Anteil der Softwareausfälle bei den Leittechnik-Komponenten deutlich höher (ca. 14 %). In Abschnitt 5.1 wird die Thematik der „Softwarefehler“ nochmal aufgegriffen.

Der höchste Anteil an diesen Messumformer-Ereignissen kann der Ursache „Drift“ zugeordnet werden. Diese Driftereignisse haben hierbei einen Anteil von ca. 27 % aus gemacht, während sie bei den Leittechnik-Ereignissen nicht vorkamen.

Zu der Ursache „Sonstiges“ liegen keine näheren Informationen vor.

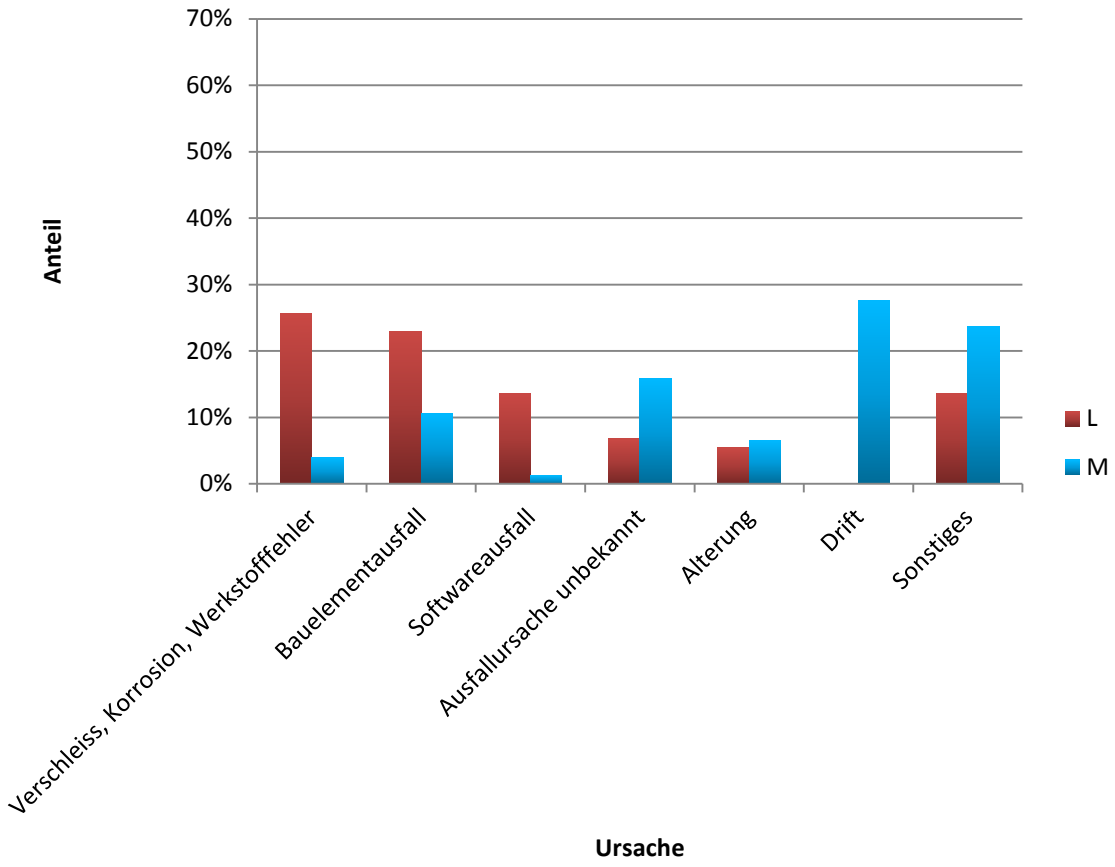

Abb. 4.34 Anteile der verschiedenen Ursachen für die Ereignisse in der Anlage DWR A für die Komponenten der Leittechnik sowie für Messumformer

4.3.4.5 Anlagenzustand bei Ereigniseintritt

In diesem Teil der Auswertung wird analysiert, in welchem Zustand sich die Anlage zum Zeitpunkt des Entdeckens des Ereignisses befand.

Aus Abbildung 4.35 kann entnommen werden, dass sowohl bei den Leittechnik-Komponenten als auch bei den Messumformern in etwa 50 % der Ereignisse im Leistungsbetrieb (10 – 100 %) erkannt wurden. Deutliche Unterschiede zwischen den beiden Komponentenarten zeigen sich bei der Erkennung eines Ereignisses in der Revisi-

on. In etwa 29 % der Ereignisse mit Messumformern und nur ca. 8 % der Ereignisse mit Leittechnik-Komponenten wurden bei diesem Anlagenzustand erkannt. Bei Stillständen außerhalb der Revision wurden ca. 34 % der Ereignisse mit Leittechnik-Komponenten und ca. 13 % der Ereignisse mit Messumformern erkannt. Nur sehr geringe Anteile der Ereignisse entfallen auf das Aufheizen bzw. Abkühlen der Anlage.

Bei den Ereignissen mit Leittechnik-Komponenten, die während des Leistungsbetriebes (10 – 100 %) erkannt wurden, handelt es sich in etwa 51 % der Fälle um Defekte an Schreibern. Diese Defekte sind zum überwiegenden Teil auf mechanische Defekte zurückzuführen. Beispielsweise mussten leere und ausgetrocknete Druckköpfe erneuert werden, Schreiber gereinigt oder verschmutzte Motoren ausgetauscht werden.

Etwa 34 % der Ereignisse mit Leittechnik-Komponenten im Leistungsbetrieb (10 - 100 %) konnten Softwarefehlern zugeordnet werden. Bei Revisionen waren ca. 50 % der Ereignisse auf Softwarefehler zurückzuführen, wohingegen es bei Stillständen außerhalb der Revision nur ca. 4 % der Ereignisse waren. Im Gegensatz dazu konnten nur etwa 2 % der Ereignisse mit Messumformern, welche im Leistungsbetrieb (10 - 100 %) erkannt wurden, auf Softwarefehler zurückgeführt werden. In der Revision lag dieser Anteil bei etwa 18 %. Insgesamt sind aber nur sehr wenig Softwarefehler aufgetreten, so dass hier eine statistische Aussage kaum möglich ist. In Abschnitt 5.1 wird die Thematik der Softwarefehler jedoch nochmal genauer betrachtet.

In Abschnitt 5.6 wird für die Anlage SWR A die Anzahl der Ereignisse bei den jeweiligen Anlagenzuständen in Relation zu den zeitlichen Anteilen, die die einzelnen Anlagenzustände im Jahr einnehmen, gesetzt. Aufgrund der geringen Datendichte für die Anlage DWR A wird dieses hier nicht gemacht.

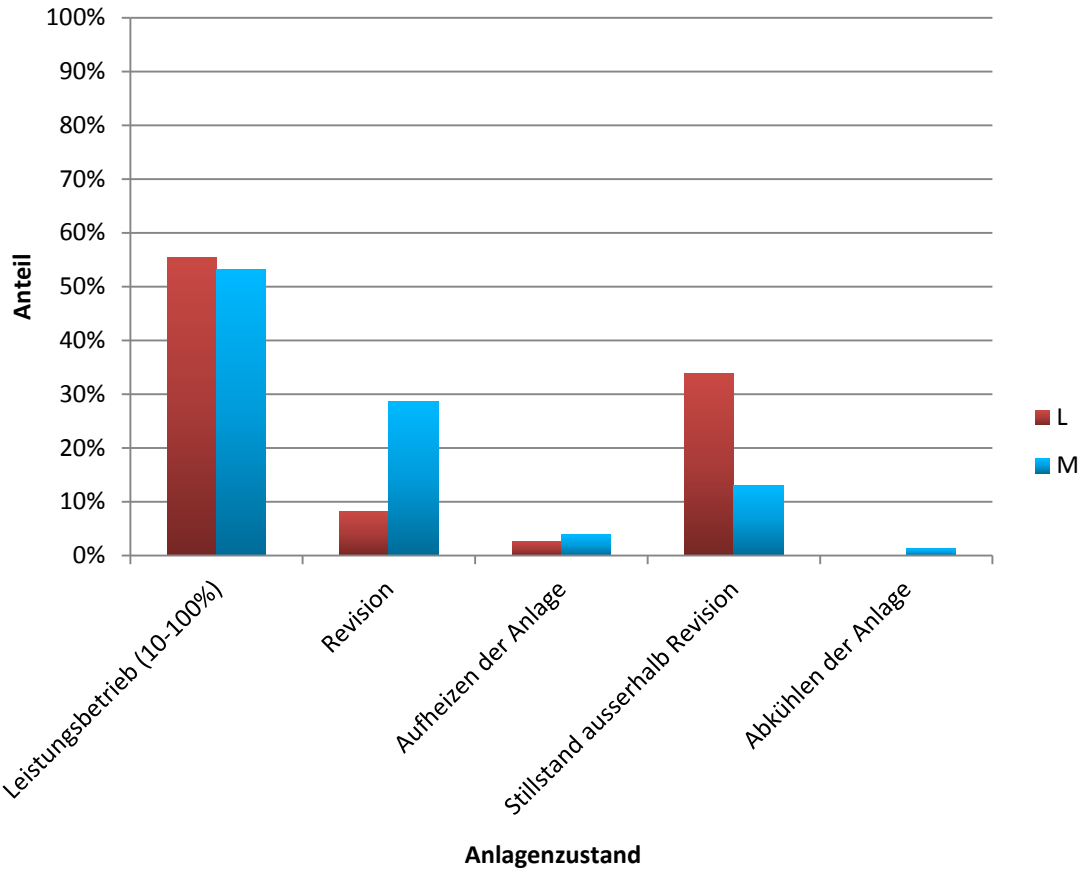

Abb. 4.35 Anteile der Anlagenzustände bei Ereigniseintritt in der Anlage DWR A für die Komponenten der Leittechnik sowie für Messumformer

4.4 DWR B

Wie bereits bei der Anlage SWR B sind in den erfassten Anlagendaten der Anlage DWR B nur die Komponenten aufgeführt, die in Ereignissen bereits auffällig geworden sind. Zusätzlich dazu ist die zum Datensatzerstellungszeitpunkt aktuelle Anzahl dieser am Standort eingesetzter Komponenten mit angegeben. Es handelt sich insgesamt um 938 Datensätze zu programmierbaren oder rechnerbasierten Komponenten. Hierbei entfallen 726 Komponenten auf den Bereich Leittechnik und 212 auf den Bereich Messumformer. Daten zu Elektrotechnik-Komponenten liegen nicht vor.

Für den Betrachtungszeitraum von 1995 bis 2013 wurden der GRS 78 Ereignisse zur Verfügung gestellt. Hiervon entfallen 33 Ereignisse auf den Bereich der Leittechnik und 45 Ereignisse auf den Bereich der Messumformer. Da keine Elektrotechnik-Komponenten mit geliefert wurden, liegen auch keine entsprechenden Ereignisse vor. Wie bereits

für die Anlage SWR B muss auch für die Anlage DWR B beachtet werden, dass im Vergleich zur Anlage SWR A eine deutlich reduzierte Ereignisanzahl vorliegt, weswegen nicht alle Auswertungen aus Abschnitt 4.1 durchgeführt werden können.

4.4.1 Betriebsmittel

Wie für die Anlage SWR B (Abschnitt 4.2.1) erfolgt auch hier nur eine Auswertung der Ereignisdaten nach der jeweiligen Betriebsmittelart. Abbildung 4.36 zeigt das Verhältnis der Anzahl der Leittechnik-Ereignisse einer Betriebsmittelart zur Gesamtanzahl der Leittechnik-Ereignisse.

Auf die Verarbeitungseinheit entfallen ca. 30 % der Ereignisse. Zudem ist erkennbar, dass etwa 27 % der Ereignisse auf mikroprozessorgesteuerte Schreiber entfallen. Bei diesen Ereignissen handelt es sich zumeist um Fehler, welche den mechanischen Teil des Schreibers und nicht die Software betreffen. Ein-/Ausgabeprozessoren sind ebenfalls in ca. 27 % der Fälle betroffen.

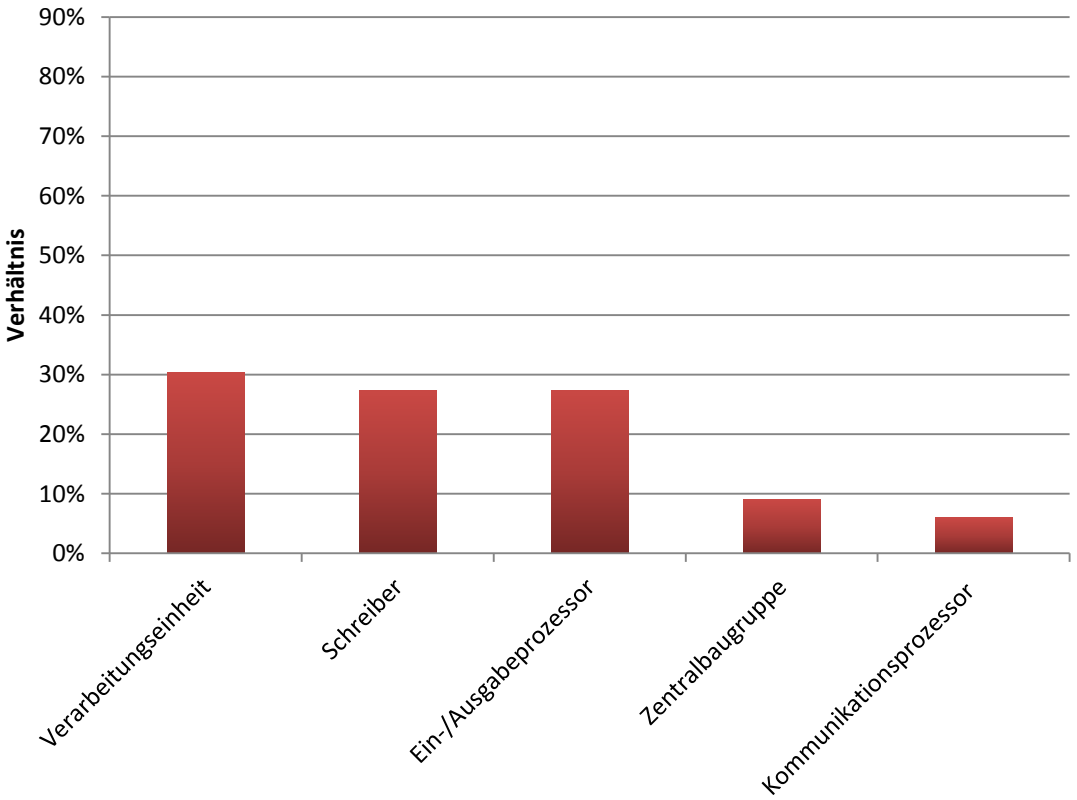

Abb. 4.36 Verhältnis der Anzahl der Leittechnik-Ereignisse einer Betriebsmittelart zur Gesamtanzahl der Leittechnik-Ereignisse für die Anlage DWR B

4.4.2 Zeitlicher Verlauf der Ereignisse

In Abbildung 4.37 sind die Ereignisse der Leittechnik-Komponenten über die jeweiligen Jahre, in denen sie aufgetreten sind, dargestellt.

Es sind leicht erhöhte Anteile in den Jahren 2009 und 2011 zu erkennen. Eine genauere Untersuchung hat keine erkennbaren Auffälligkeiten geliefert. Für die Jahre 2002, 2003 und 2005 wurden keine Ereignisse zu Leittechnik-Komponenten mitgeliefert und für die Jahre 1998 und 2001 wurden der GRS keine Informationen (L und M) vorgelegt.

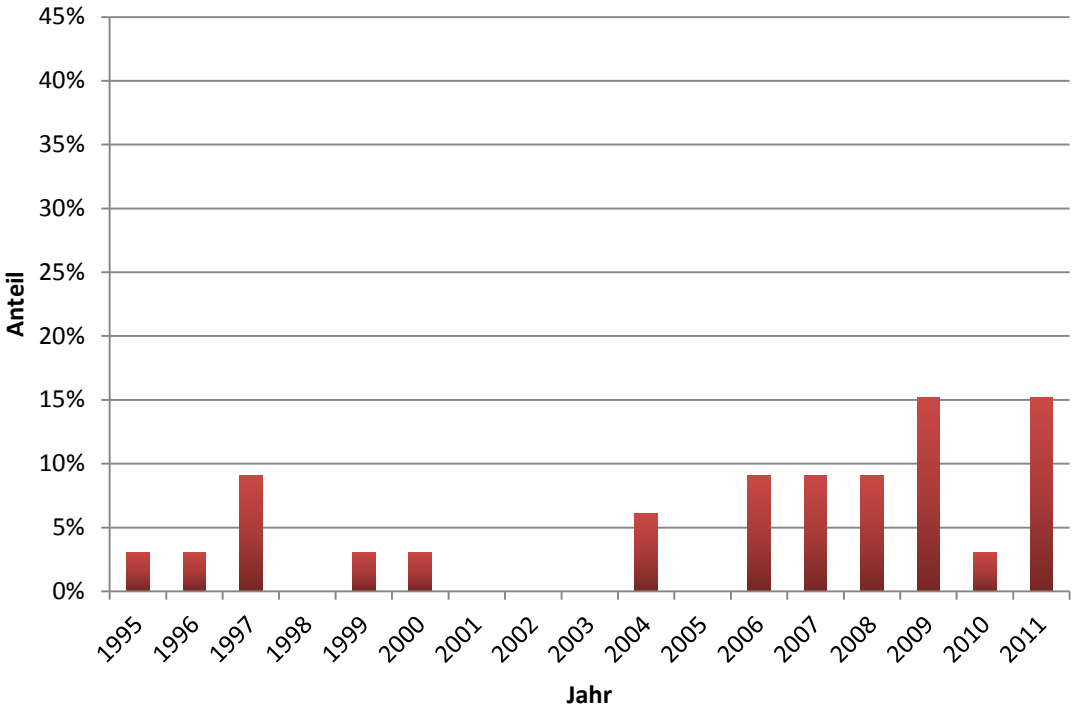

Abb. 4.37 Prozentualer Anteil der Ereignisse pro Jahr in Bezug auf die Gesamtanzahl der Ereignisse für die Leittechnik-Komponenten der Anlage DWR B

4.4.3 Hersteller

In diesem Abschnitt werden erneut die Leittechnik-Komponenten hinsichtlich der eingesetzten Hersteller genauer untersucht. Die Anteile der einzelnen Hersteller an den erfassten programmierbaren oder rechnerbasierten Leittechnik-Komponenten des Standorts sind in Abbildung 4.38 dargestellt. Hieraus ergibt sich, dass der Hersteller L mit ca. 43 % und der Hersteller A mit ca. 38 % den größten Anteil der Komponenten gestellt hat. Die Hersteller B und P waren mit ca. 16 % und ca. 3 % vertreten.

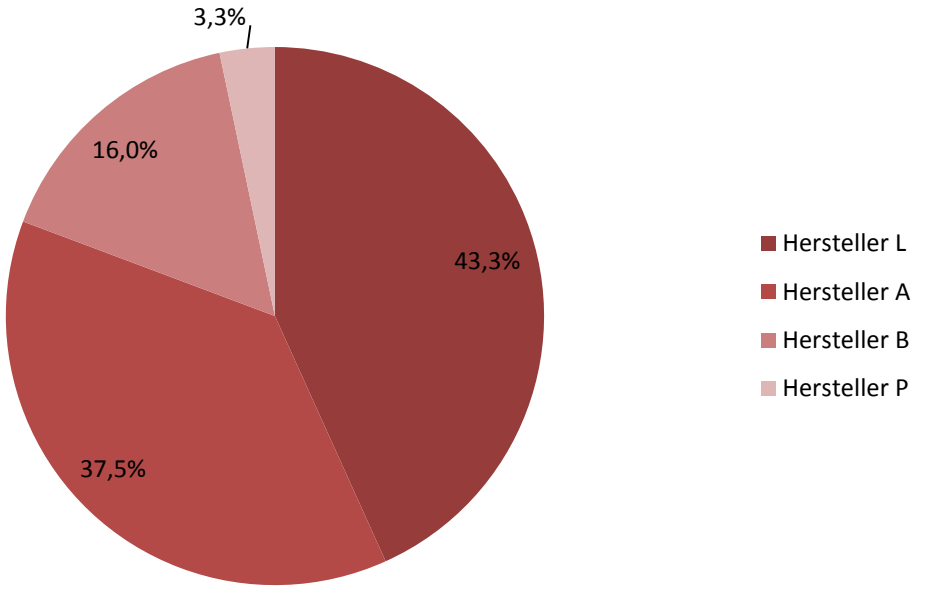

Abb. 4.38 Anteile der Hersteller an den für den Standort der Anlage DWR B erfassten programmierbaren oder rechnerbasierten Leittechnik-Komponenten

Neben der Zuordnung der Hersteller zu den Leittechnik-Komponenten ist es wie bereits erwähnt zudem interessant auszuwerten, inwiefern die verschiedenen Hersteller in den Ereignissen involviert waren. In Abbildung 4.39 ist das Verhältnis von Ereignisanzahl an Komponenten eines bestimmten Herstellers zur Anzahl der eingesetzten Komponenten für diesen Hersteller für die erfassten Leittechnik-Komponenten dargestellt. Es zeigt sich, dass von den Komponenten des Herstellers L, welcher mit ca. 43 % den größten Anteil an den eingebauten Leittechnik-Komponenten ausgemacht hat, ca. 3 % von Ereignissen betroffen waren. Von Komponenten des Herstellers B, welche einen Anteil von ca. 16 % an der Gesamtanzahl der Leittechnik-Komponenten hatten, waren ca. 8 % von Ereignissen betroffen. Die Komponenten von Hersteller A hingegen, hatten mit ca. 38 % den zweitgrößten Anteil an den eingebauten Komponenten und von diesen waren im Betrachtungszeitrum ca. 3 % von Ereignissen betroffen. Hersteller P war mit einem kleinen Anteil von ca. 3 % an den eingebauten Komponenten vertreten, wovon etwa 25 % von Ereignissen betroffen waren. Insgesamt wurden keine Auffälligkeiten festgestellt.

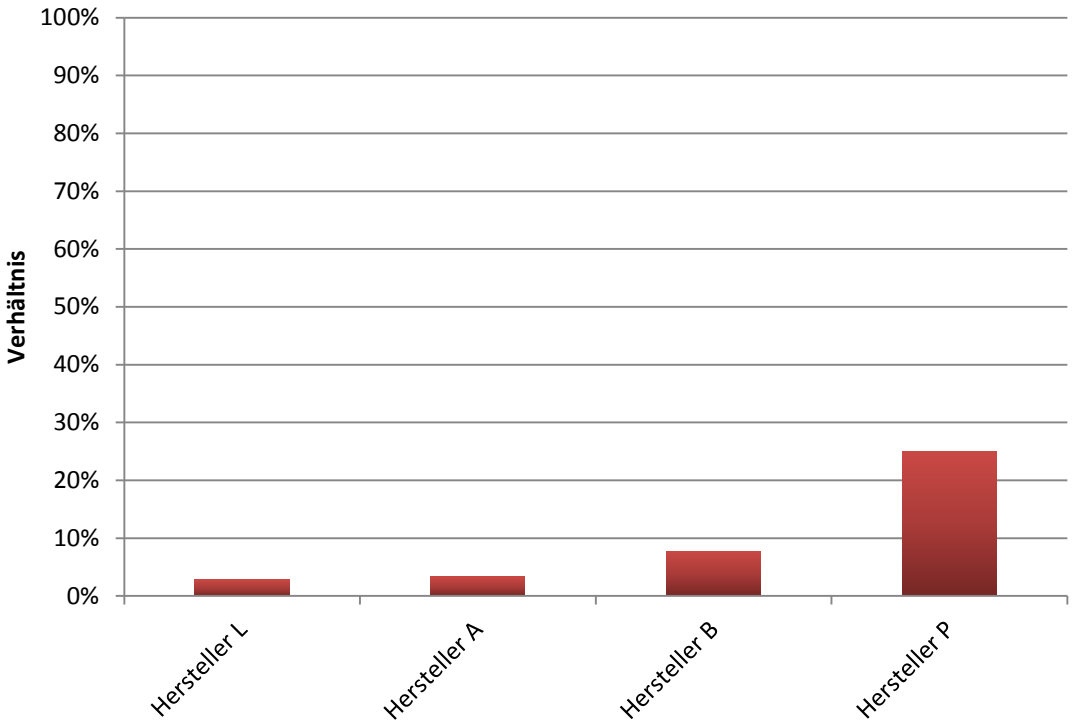

Abb. 4.39 Verhältnis von Ereignisanzahl an Komponenten eines bestimmten Herstellers zur Anzahl der eingesetzten Komponenten für diesen Hersteller für die erfassten Leittechnik-Komponenten der Anlage DWR B

4.4.4 Vergleich zwischen Leittechnik-Komponenten und Messumformern

Wie bereits erwähnt, ist das Ziel des Projektes die in Kernkraftwerken eingesetzten programmierbaren oder rechnerbasierten Leittechnik-Komponenten (L) näher zu untersuchen. Im Gegensatz dazu, werden im Bericht „Analyse zum Einsatz und Betrieb elektrotechnischer Einrichtungen“ /GRS 15/ auch Auswertungen von Elektrotechnik-Komponenten (E) und Messumformern (M) durchgeführt. Da ein Vergleich der Ergebnisse ggf. neue Informationen preisgeben könnte, werden im Folgenden insbesondere die Charakteristika der Komponentenarten L und M verglichen (Daten zu Elektrotechnik-Komponenten lagen in dieser Anlage nicht vor).

Die Farbgebung in den folgenden Abbildungen ist im gesamten Bericht konsistent. Auswertungen von Leittechnik-Komponenten (L) werden in Rot dargestellt und Auswertungen von Messumformern (M) in Blau.

4.4.4.1 Fehlerart

Zu Beginn dieses Vergleichsabschnittes werden die Anteile der unterschiedlichen Fehlerarten für die Leittechnik-Komponenten und die Messumformer im Vergleich zu einander aufgetragen. Dargestellt ist dies in Abbildung 4.40. Dieser Auftragung kann entnommen werden, dass im Bereich der Leittechnik ca. 40 % auf nicht selbstmeldende und ca. 56 % auf selbstmeldende Fehler entfallen sind. Im Gegensatz dazu, traten diese beiden Fehlerarten bei den Messumformern mit ca. 24 % bzw. ca. 17 % bei einem deutlich niedrigeren Anteil der Ereignisse auf. Bei den Messumformern hat die Fehlerart „Fehlmessung“ mit ca. 55 % den höchsten Wert aufgewiesen. Bei diesen Fehlmessungen handelt es sich u. a. lediglich um nicht plausible Anzeigewerte oder abweichende Messungen, weswegen diese hier nicht weiter thematisiert werden.

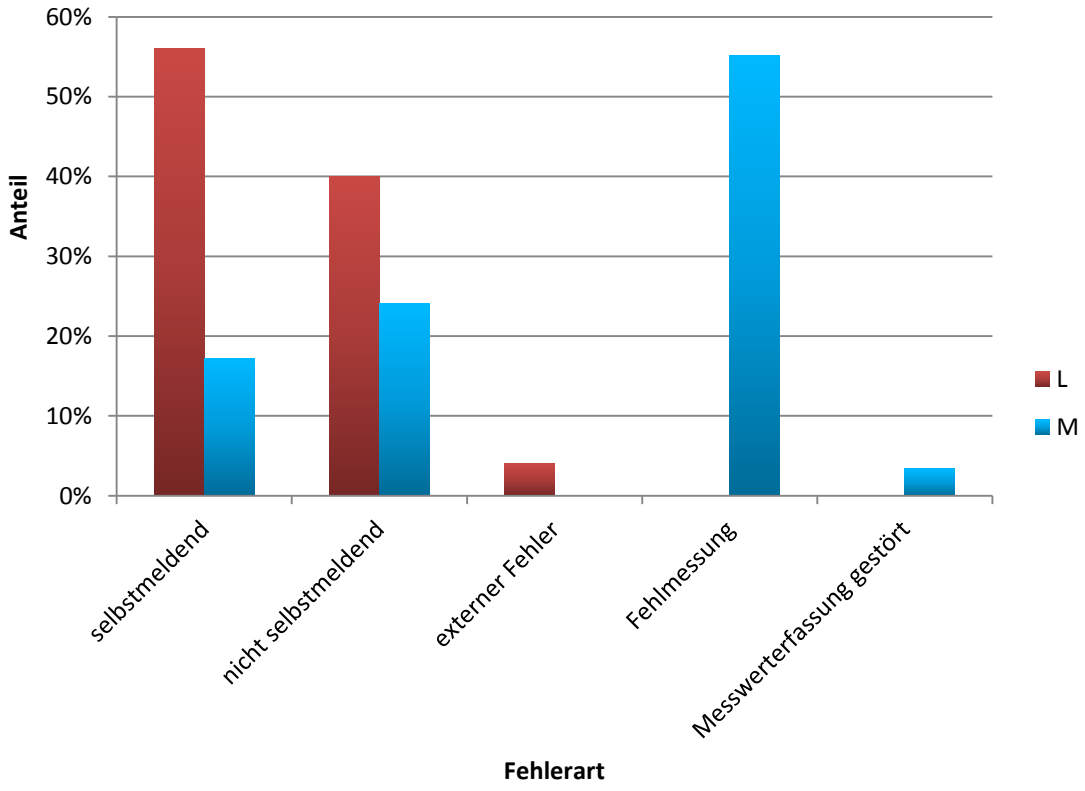

Abb. 4.40 Anteile der verschiedenen Fehlerarten in der Anlage DWR B für die Leittechnik-Komponenten sowie für Messumformer

4.4.4.2 Fehlererkennung

Ähnlich wie bei den vorangegangenen Auswertungen für die anderen Anlagen werden im Folgenden die möglichen Fehlererkennungsarten analysiert. In Abbildung 4.41 ist dafür dargestellt, wie die Ereignisse für Leittechnik-Komponenten und Messumformer in der Anlage erkannt wurden.

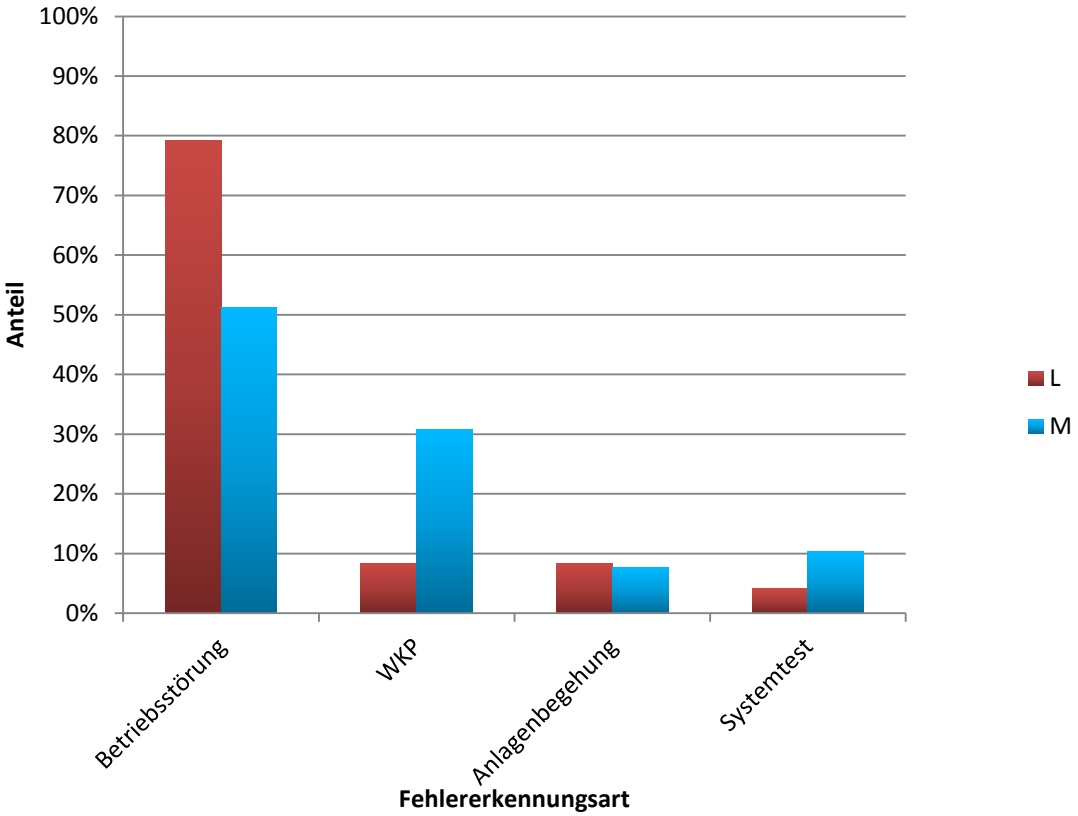

Abb. 4.41 Anteile der verschiedenen Fehlererkennungsarten in der Anlage DWR B für die Komponenten der Leittechnik sowie für Messumformer

Der größte Anteil der Ereignisse konnte für die Leittechnik-Komponenten aufgrund einer Betriebsstörung erkannt werden (ca. 79 %). Einen systematischen Zusammenhang zwischen diesen Ereignissen konnte nicht gefunden werden. Die anderen Fehlererkennungsarten (WKP, Anlagenbegehung, Systemtest) kamen für die Leittechnik-Komponenten nur sehr selten (< 8 %) vor.

Die Ereignisse der Messumformer konnten ebenfalls zum größten Teil (> 50 %) durch eine Betriebsstörung erkannt werden. Diese sind zur Hälfte auf Display- und Tastaturdefekte zurückzuführen. Etwa 30 % der Ereignisse wurden bei einer WKP aufgedeckt

wurden. Die beiden Fehlererkennungsarten „Systemtest“ und „Anlagenbegehung“ lagen jeweils bei unter 10 %.

4.4.4.3 Ursache

Bei der Auswertung zum Thema „Ursache der Ereignisse“ hat sich gezeigt, dass für die Anlage DWR B zwischen den Leittechnik-Komponenten und den Messumformern deutliche Unterschiede vorhanden sind. Die Anteile der jeweiligen Ursache sind in Abbildung 4.42 dargestellt.

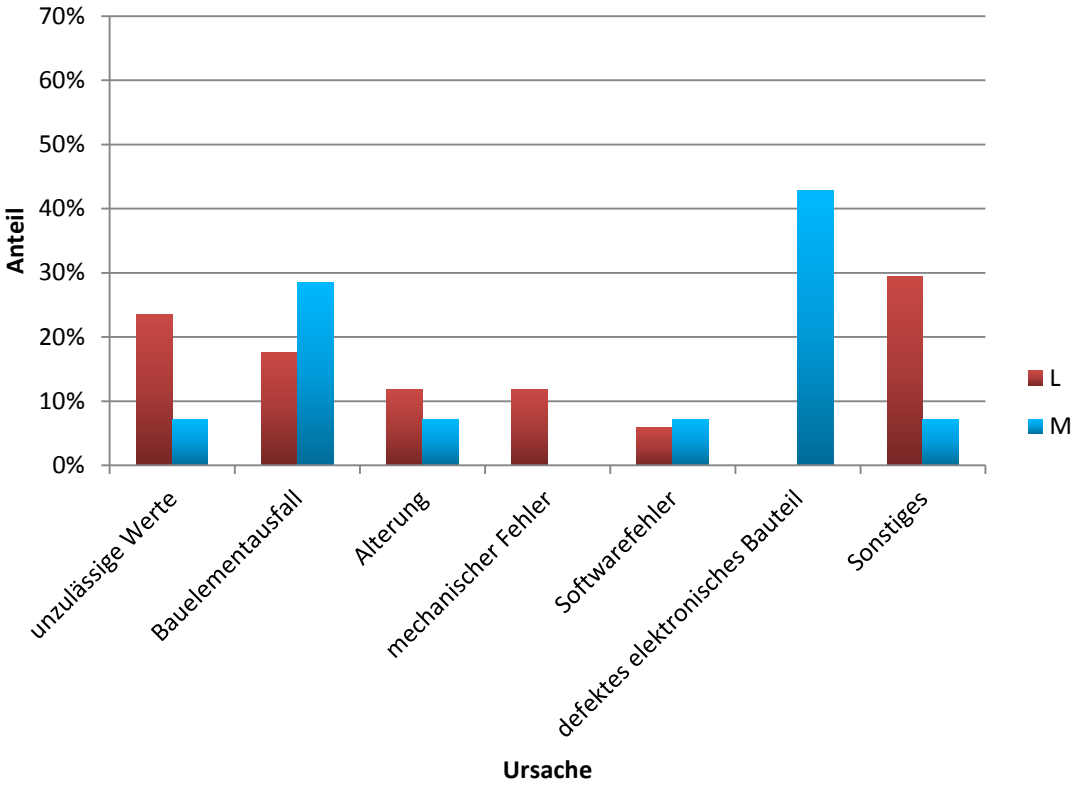

Abb. 4.42 Anteile der verschiedenen Ursachen für die Ereignisse in der Anlage DWR B für die Komponenten der Leittechnik sowie für Messumformer

Aus Abbildung 4.42 kann entnommen werden, dass die Ursache für den größten Teil der Ereignisse in der Leittechnik als „Sonstiges“ deklariert wurde (ca. 30 %). Aus den vorliegenden Unterlagen geht jedoch nicht hervor, was unter „Sonstiges“ zu verstehen ist. Die zweithäufigste Ursache der Leittechnik-Ereignisse waren unzulässige Werte (ca. 24 %). Bei ca. 18 % der Ereignisse von Leittechnik-Komponenten war die Ursache ein Bauelementausfall und bei ca. 12 % handelte es sich um Alterung. Ebenfalls mit

ca. 12 % sind die Leittechnik-Komponenten aufgrund eines mechanischen Fehlers ausgefallen. Diese Fehler können mit den Schreibern in Verbindung gebracht werden.

Im Gegensatz zu den Leittechnik-Komponenten sind die Messumformer zum allergrößten Teil aufgrund eines defekten elektronischen Bauteils ausgefallen (ca. 43 %). Diese Ursache wird gefolgt von einem Bauelementausfall, welcher einen Anteil von ca. 29 % hatte. Die weiteren Ursachen liegen unterhalb von 8 %.

4.4.4.4 Anlagenzustand bei Ereigniseintritt

Die Ereignisse traten, wie in Abbildung 4.43 zu sehen ist, bei den Leittechnik-Komponenten zu etwa 84 % im Betrieb auf, während es bei den Messumformern in ca. 60 % der Fälle zu einem Ausfall im Betrieb kam. Da bei den DWR B-Daten der Anlagenzustand nur in „Betrieb“ und „Revision“ unterteilt ist, ergibt sich daraus, dass etwa 16 % der Ereignisse mit Leittechnik-Komponenten und ca. 40 % der Ereignisse mit Messumformern in Revision auftraten. Hierbei hat sich zudem gezeigt, dass ca. 55 % der bei Revision entdeckten Ereignisse mit Messumformern bei einer wiederkehrenden Prüfung (WKP) entdeckt wurden.

In Abschnitt 5.6 werden die Ereigniszahlen bei den jeweiligen Anlagenzuständen in Relation zu den zeitlichen Anteilen, die die Anlagenzustände einnehmen, gesetzt. Diese Auswertung erfolgt für die Anlage SWR A. Aufgrund der geringen Datendichte für die Anlage DWR B wird dieses hier nicht gemacht.

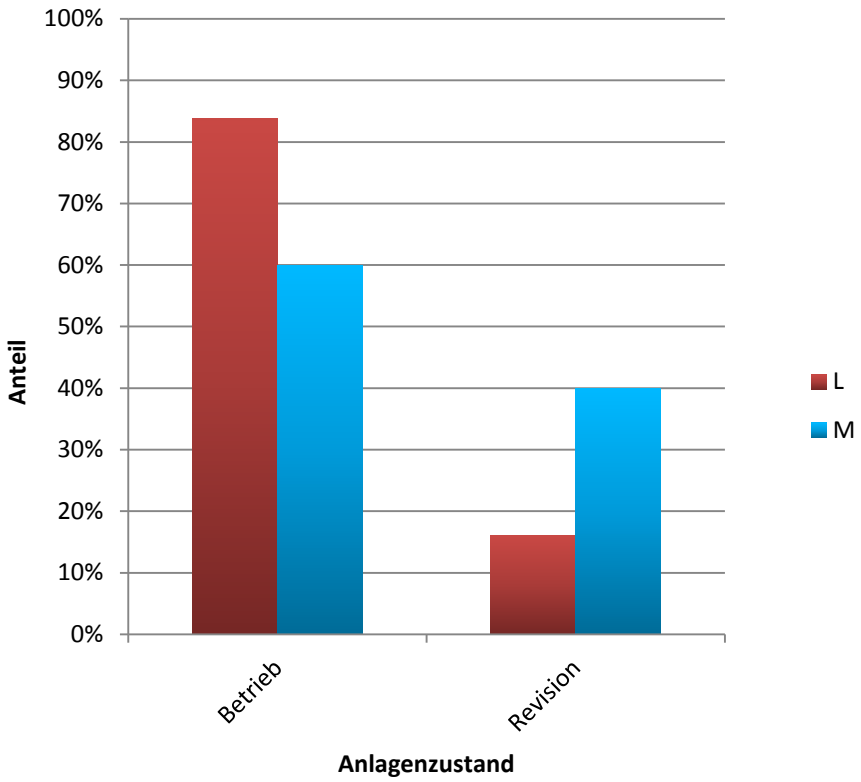

Abb. 4.43 Anteile der Anlagenzustände bei Ereigniseintritt in der Anlage DWR B für die Komponenten der Leittechnik sowie für Messumformer

4.5 DWR C

Wie bereits bei der Anlage DWR A sind in den erfassten Anlagendaten der Anlage DWR C nur die Komponenten aufgeführt, die in Ereignissen bereits auffällig geworden sind. Zusätzlich dazu ist die zum Datensatzerstellungszeitpunkt aktuelle Anzahl dieser am Standort eingesetzten Komponenten mit angegeben. Es handelt sich insgesamt um 2734 Datensätze zu programmierbaren oder rechnerbasierten Komponenten. Hierbei entfallen 1292 Komponenten auf den Bereich Leittechnik, 387 Komponenten auf den Bereich Elektrotechnik und 1055 Komponenten auf den Bereich Messumformer.

Für den Betrachtungszeitraum von 2006 bis 2013 wurden der GRS insgesamt 181 Ereignisse übermittelt. Hiervon entfallen 89 Ereignisse auf den Bereich Leittechnik, 22 Ereignisse auf den Bereich Elektrotechnik und 70 Ereignisse auf den Bereich Messumformer.

4.5.1 Betriebsmittelarten

In Übereinstimmung mit den vorherigen Auswertungen erfolgt auch hier zuerst eine Analyse der Daten in Bezug auf die eingesetzten Betriebsmittelarten. Dafür sind in Abbildung 4.44 das Verhältnis der Anzahl der Leittechnik-Ereignisse einer Betriebsmittelart zur Gesamtanzahl der Leittechnik-Ereignisse aufgetragen.

Es ist deutlich erkennbar, dass die größten Anteile bei den Ereignissen von Leittechnik-Komponenten die Betriebsmittelarten „Zentralbaugruppe“ (ca. 38 %) und „Schreiber“ (ca. 29 %) aufweisen. Bei den letzt-genannten handelt es sich insbesondere um mikroprozessorgesteuerte Punktschreiber, bei denen überwiegend nur der mechanische Teil ausgefallen ist. Des Weiteren ist noch die Betriebsmittelart „Prozessor“ zu erwähnen, welche einen Anteil von ca. 21 % bei den Ereignissen hat.

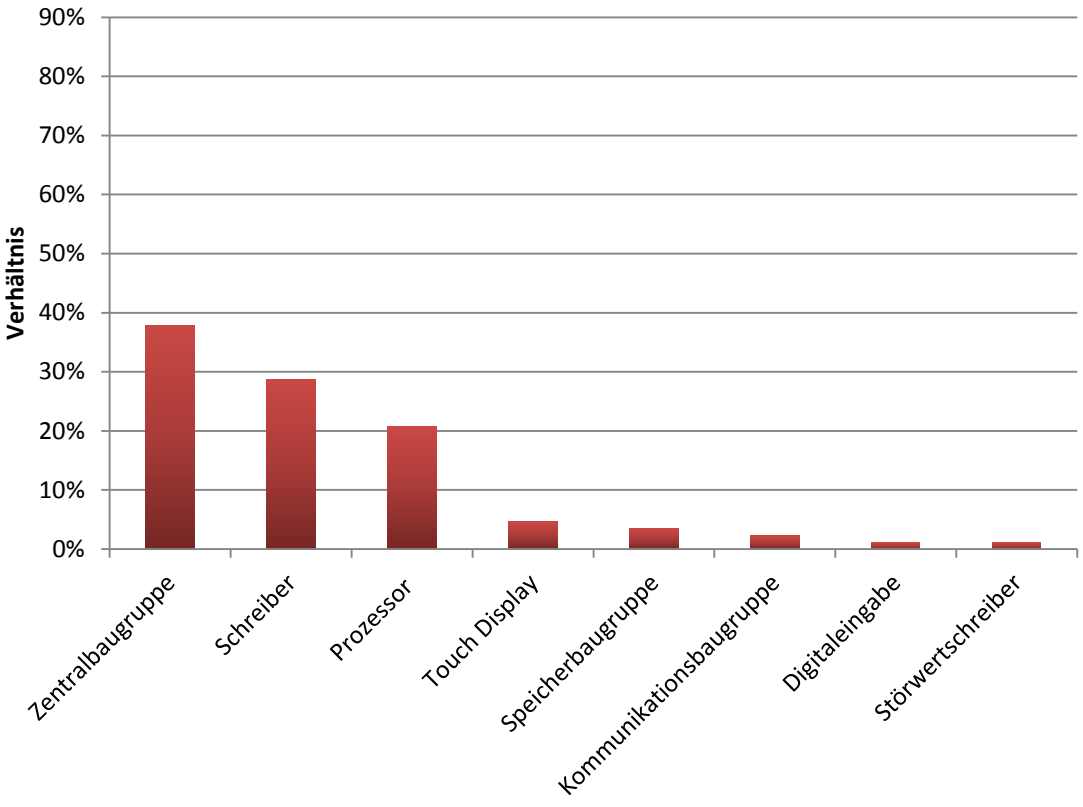

Abb. 4.44 Verhältnis der Anzahl der Leittechnik-Ereignisse einer Betriebsmittelart zur Gesamtanzahl der Leittechnik-Ereignisse für die Anlage DWR C

4.5.2 Zeitlicher Verlauf der Ereignisse

Für die Auswertung des zeitlichen Verlaufs der Leittechnik-Ereignisse wurden die jeweiligen Anteile der Ereignisse aus den Jahren 2006 bis 2013 in Abbildung 4.45 aufgetragen.

Aus der Verteilung der jeweiligen Anteile sind keine Besonderheiten hinsichtlich einer Häufung von Ereignissen erkennbar. Jedoch hat sich gezeigt, dass im Jahr 2009 6 RAM-Speicherbaugruppen im selben Schrank ausgefallen sind. Da jedoch keine weiteren Informationen zur Verfügung standen, konnte keine vertiefte Untersuchung dazu vorgenommen werden.

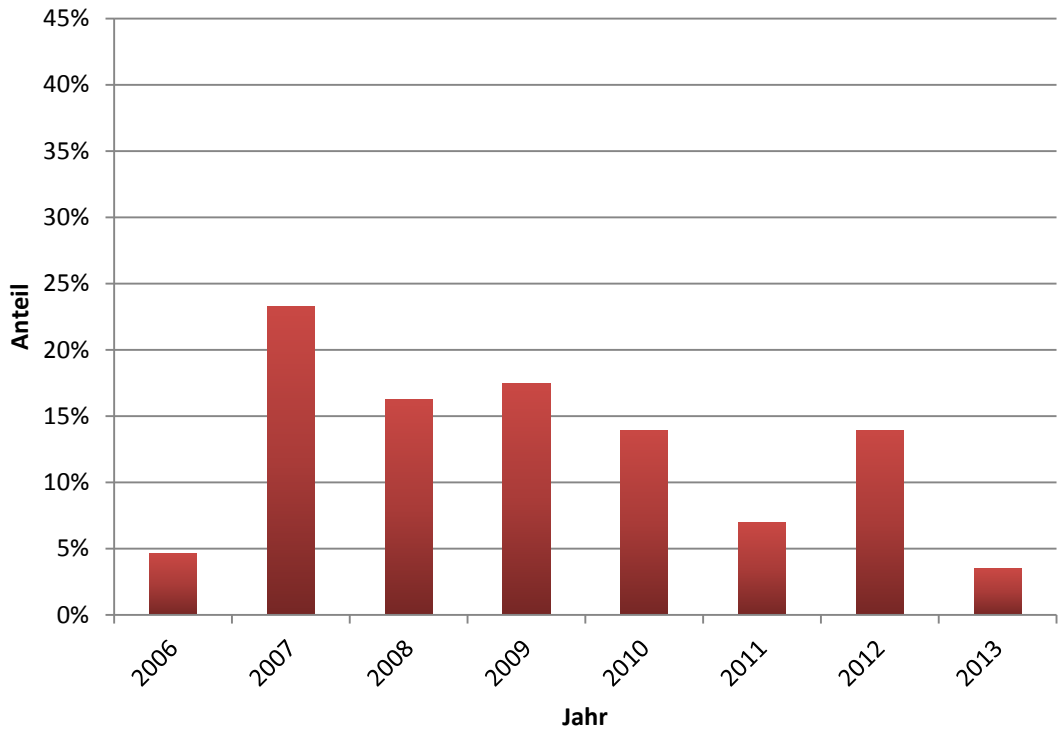

Abb. 4.45 Prozentualer Anteil der Ereignisse pro Jahr in Bezug auf die Gesamtanzahl der Ereignisse für die Leittechnik-Komponenten der Anlage DWR C

4.5.3 Hersteller

In diesem Abschnitt wird zu Beginn dargestellt, von welchem Hersteller die erfassten Leittechnik-Komponenten waren. Darauf aufbauend wird analysiert, welchen Anteil der jeweilige Hersteller an den zugehörigen Ereignissen hat.

Hierfür sind in Abbildung 4.46 die jeweiligen Anteile der Hersteller an den erfassten Leittechnik-Komponenten des Standortes gezeigt. Es ist erkennbar, dass der Großteil (ca. 88 %) dieser Leittechnik-Komponenten vom Hersteller A war. Ein weitaus geringerer Anteil entfiel auf den Hersteller I (ca. 10 %) und ein noch geringer Teil (ca. 2 %) auf den Hersteller G.

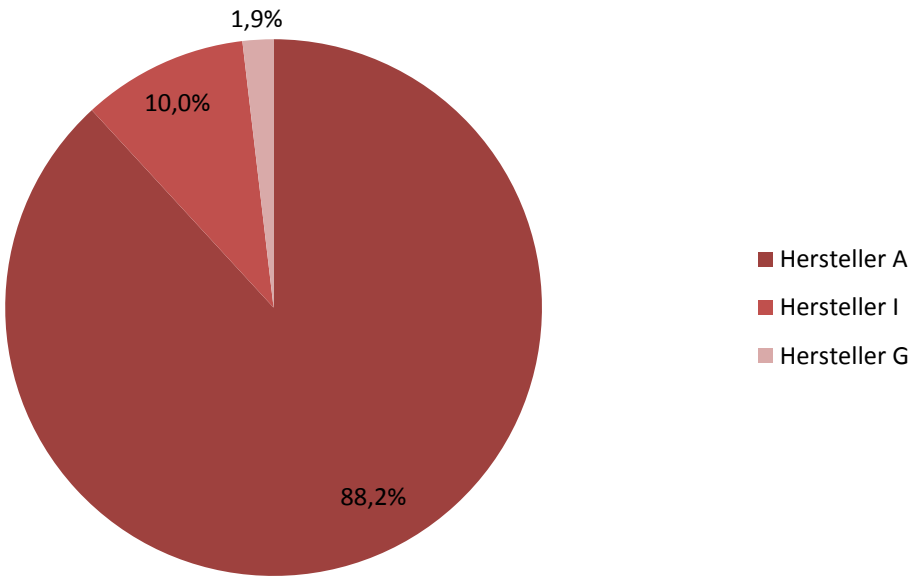

Abb. 4.46 Anteile der Hersteller an den für den Standort der Anlage DWR C erfassten programmierbaren oder rechnerbasierten Leittechnik-Komponenten

Bei den Ereignissen waren nur Komponenten des Herstellers A betroffen. Der Anteil der von Ereignissen betroffenen Komponenten des Herstellers A in Bezug auf die Gesamtanzahl der erfassten Komponenten von Hersteller A lag bei etwa 8 %.

4.5.4 Vergleich zwischen Leittechnik-Komponenten und Messumformern

Wie bereits erwähnt, ist das Ziel des Projektes die in Kernkraftwerken eingesetzten programmierbaren oder rechnerbasierten Leittechnik-Komponenten (L) näher zu untersuchen. Im Gegensatz dazu, werden im Bericht „Analyse zum Einsatz und Betrieb elektrotechnischer Einrichtungen“ /GRS 15/ auch Auswertungen von Elektrotechnik-Komponenten (E) und Messumformern (M) durchgeführt. Da ein Vergleich der verschiedenen programmierbaren oder rechnerbasierten Komponenten weitere

Erkenntnisse bringen könnte, wird im Folgenden untersucht, ob die unterschiedlichen Komponentenarten (L, E, M) verschiedene Ausfallzahlen oder Charakteristika aufweisen. Dazu werden die Ereignisse von L, E und M hinsichtlich verschiedener Attribute relativ zueinander verglichen.

Die Farbgebung in den folgenden Abbildungen ist im gesamten Bericht konsistent. Auswertungen von Leittechnik-Komponenten (L) werden in Rot dargestellt, Auswertungen von Elektrotechnik-Komponenten (E) in Grün und Auswertungen von Messumformern (M) in Blau.

4.5.4.1 System

Ein Überblick für die Anlage DWR C über die von den Leittechnik-Ereignissen betroffenen Systeme ist in Abbildung 4.47 dargestellt. Für eine bessere Übersicht sind dabei nur die Systeme dargestellt, die mindestens einen Anteil von 3 % haben.

Der größte Anteil der Leittechnik-Ereignisse betraf die Systeme der sonstigen Schränke und der Leitungssystem-Zwischenspeicher (ca. 14 %), gefolgt von den Systemen der Rückkühlanlage (ca. 10 %) und der Fällung (ca. 9 %) sowie den Systemen der Probeentnahme und der Schränke der Turbine/Generator (Scheibe 2) mit jeweils ca. 7 %. In ca. 5 % der Fälle waren Systeme der Wechseleinrichtungen am Reaktor sowie Schränke für den Kühlturm betroffen. Die anderen Systeme liegen bei einem Anteil von kleiner als 5 %.

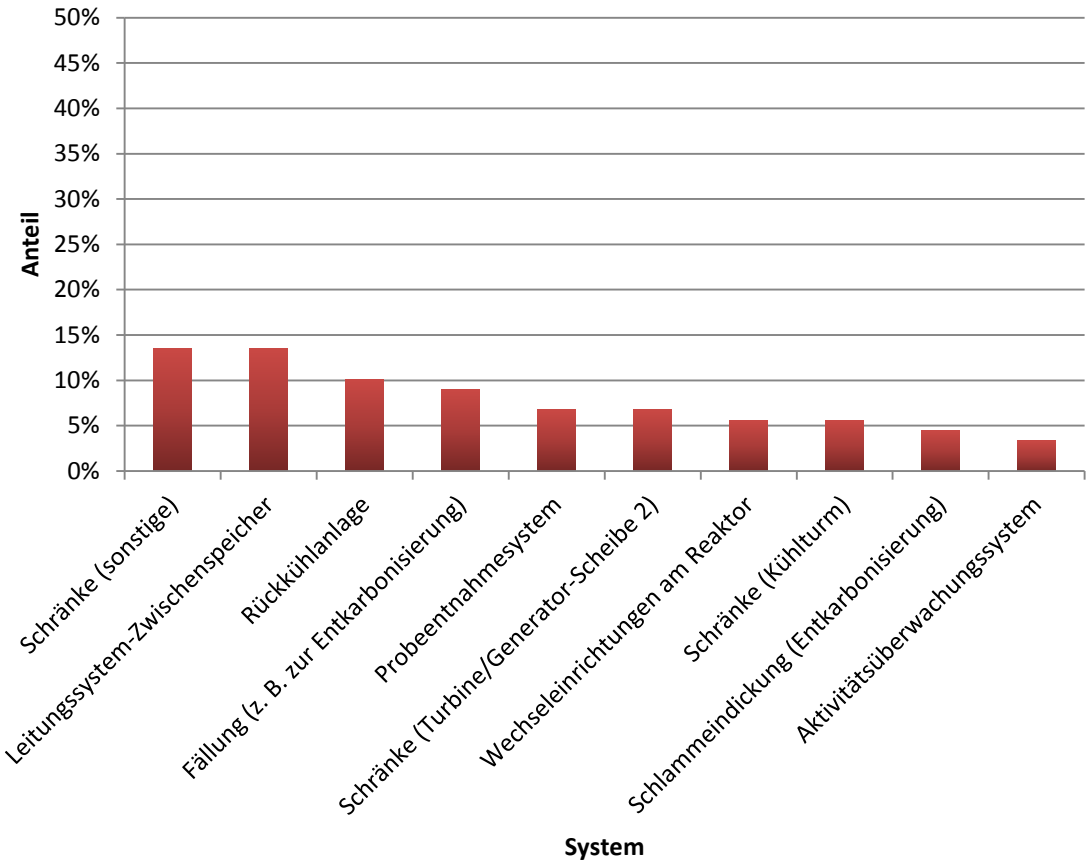

Abb. 4.47 Anteile der von Leittechnik-Ereignissen betroffenen Systeme in der Anlage DWR A

In Abbildung 4.48 sind die Elektrotechnik-Ereignisse nach dem jeweils betroffenen System aufgeschlüsselt dargestellt. Es ist erkennbar, dass in den meisten Fällen das Ereignis in einer lüftungstechnischen Anlage für die verschiedensten Bereiche aufgetreten ist. Hier zu nennen wären die lüftungstechnischen Anlagen für den konventionellen Bereich (ca. 18 %), dem Maschinenhaus/Rucksack (ca. 14 %), dem Schaltanlagengebäude (ca. 14 %), dem Reaktorgebäuderingraum (ca. 9 %) sowie der Kabel- und Rohrkanäle (ca. 9 %). Darüber hinaus sind ca. 14 % der Elektrotechnik-Ereignisse dem System des 660V-Normalnetzes des Kühlturmes zuzuordnen. Die anderen Systeme liegen bei einem Anteil von kleiner als 5 %. Da sich diese Auswertung nur auf wenige Ereignisse stützt ist die statische Aussagekraft relativ gering.

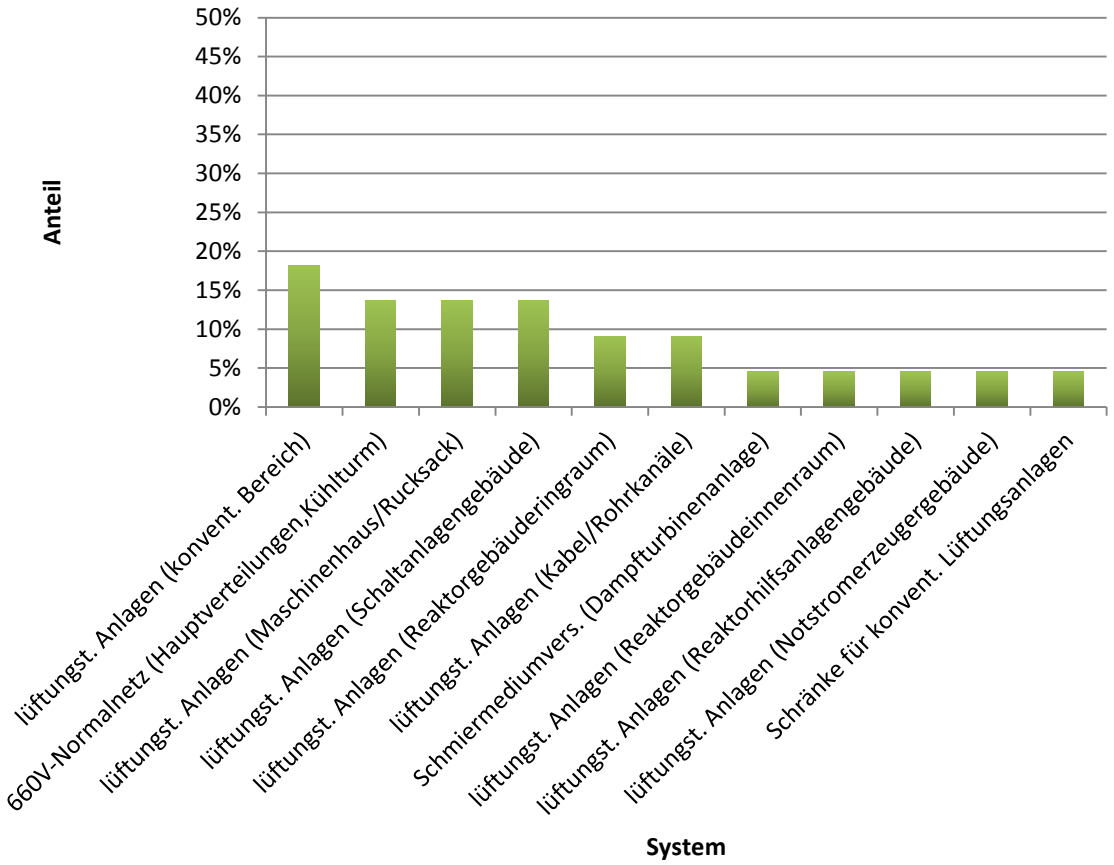

Abb. 4.48 Anteile der von Elektrotechnik-Ereignissen betroffenen Systeme in der Anlage DWR A

In Abbildung 4.49 sind die betroffenen Systeme der Messumformer-Ereignisse dargestellt. Es ist deutlich, dass die meisten Ereignisse in Systemen der Rückkühlanlage aufgetreten sind (ca. 16 %). Des Weiteren sind noch die Systeme der Borwasserlagerung mit ca. 9 % und die Systeme der Lagerung flüssiger radioaktiv kontaminierter Abfälle (Abfalllagerung) mit ca. 7 % zu nennen.

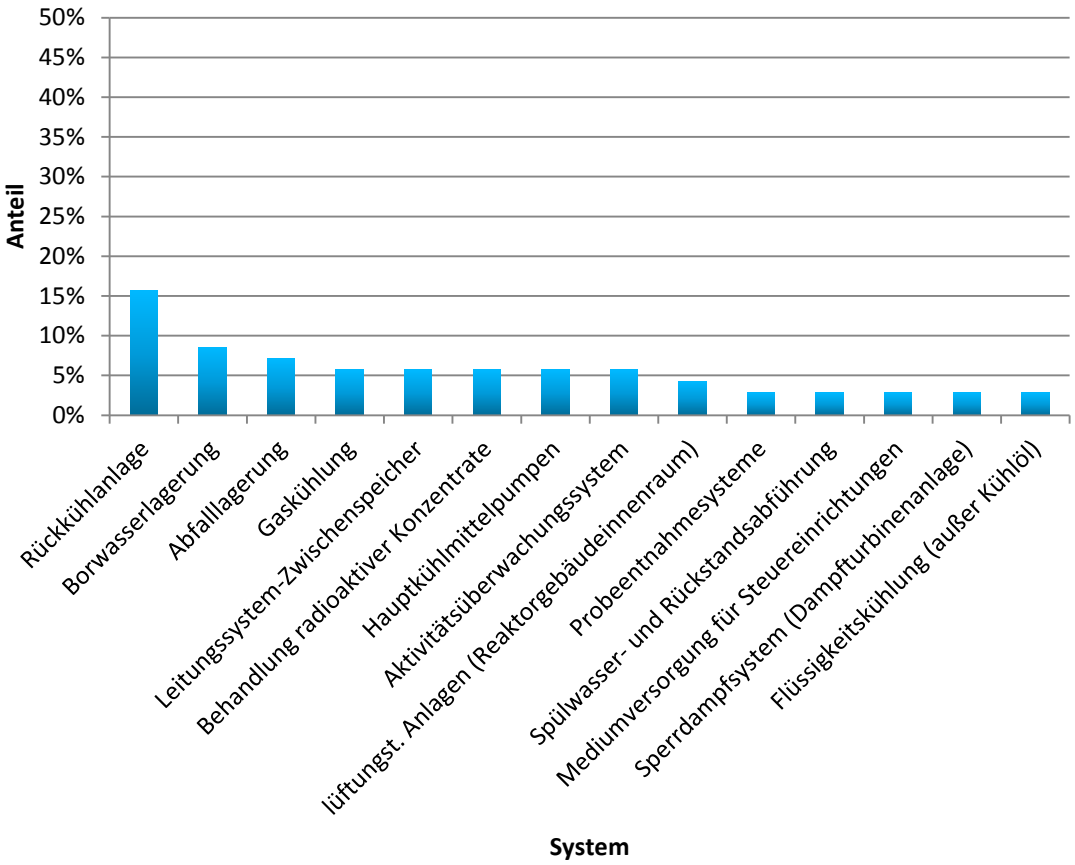

Abb. 4.49 Anteile der von Messumformer Ereignissen betroffenen Systeme in der Anlage DWR A

4.5.4.2 Auswirkungen

Genauso wie bei der Anlage DWR A konnten die Daten der Anlage DWR C hinsichtlich der Auswirkungen, welche durch die Ereignisse verursacht wurden, untersucht werden. In Abbildung 4.50 sind die jeweiligen Anteile der Auswirkungen für Leittechnik-Komponenten und Elektrotechnik-Komponenten sowie Messumformer dargestellt. Zur besseren Übersicht wurden die Auswirkungen, die für die Ereignisse der Leittechnik, der Elektrotechnik und der Messumformer einen Anteil von kleiner als 3 % aufweisen, nicht mit in das Diagramm aufgenommen.

Bei etwa 20 % der Ereignisse führte der Fehler von Leittechnik-Komponenten zu einem Betriebsversagen, bei ca. 10 % bewirkte der Fehler keine Veränderung. Eine gestörte Funktion lag ebenfalls in etwa 10 % der Fälle vor.

Im Bereich der Elektrotechnik lag der größte Anteil mit etwa 23 % bei sporadisch auftretenden Fehlern gefolgt von „Schaltet nicht um“ mit etwa 18 %, „fehlerhafter Abschaltung“ mit etwa 14 % und „Auslösung durch Schutzeinrichtung“ mit etwa 9 %. Der Ausfall ohne Veränderung lag mit etwa 9 % in einem ähnlichen Bereich wie bei den Leittechnik-Komponenten.

Die „sporadischen Fehler“ machten bei den Messumformern mit etwa 14 % den größten Anteil aus, gefolgt von „Betriebsversagen“ mit ca. 10 %, „Ausfall nach Max“ sowie „Toleranzüberschreitung“ mit etwa 9 % und „Fehlmessung“ mit etwa 7 %. Diese Ereignisse lassen sich zumeist auf Driftereignisse zurückführen.

Zu der Auswirkung „Sonstiges“ liegen keine näheren Informationen vor.

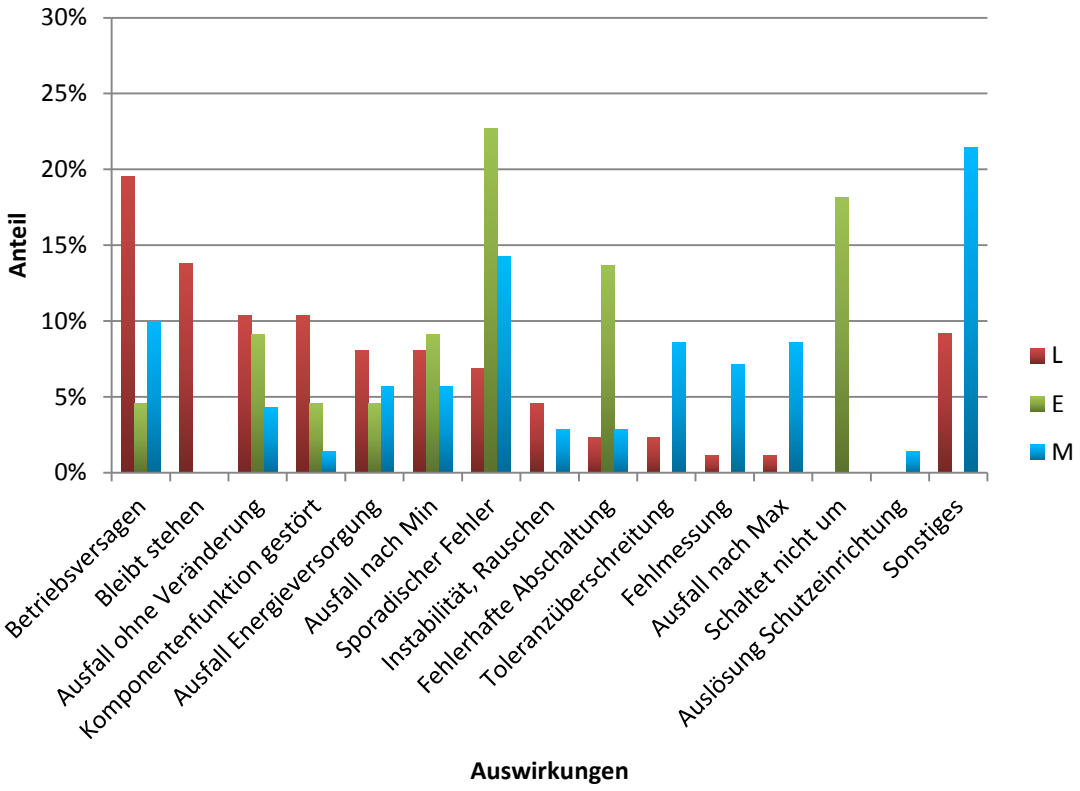

Abb. 4.50 Anteile der Auswirkungen der Ereignisse in der Anlage DWR C für die Komponenten der Elektro- und Leittechnik sowie für Messumformer

4.5.4.3 Fehlererkennung

Im Folgenden wird ausgewertet, wie die jeweiligen Ereignisse in der Anlage erkannt wurden. Hierfür sind in Abbildung 4.51 die jeweiligen Anteile der einzelnen Erkennungsarten „Prüfung“, „Anforderung“, „Betrieb“, „Begehung/Überwachung vor Ort“ und „Wartenüberwachung/Meldung“ getrennt für die verschiedenen Komponentenarten (L, E, M) aufgetragen.

Es ist deutlich erkennbar, dass die Ereignisse am häufigsten (ca. 42 %) durch Wartenüberwachung und Meldungen entdeckt wurden. Die anderen Fehlererkennungsarten waren in etwa gleichverteilt (ca. 10 – 20 %) und zeigten keine weiteren Auffälligkeiten.

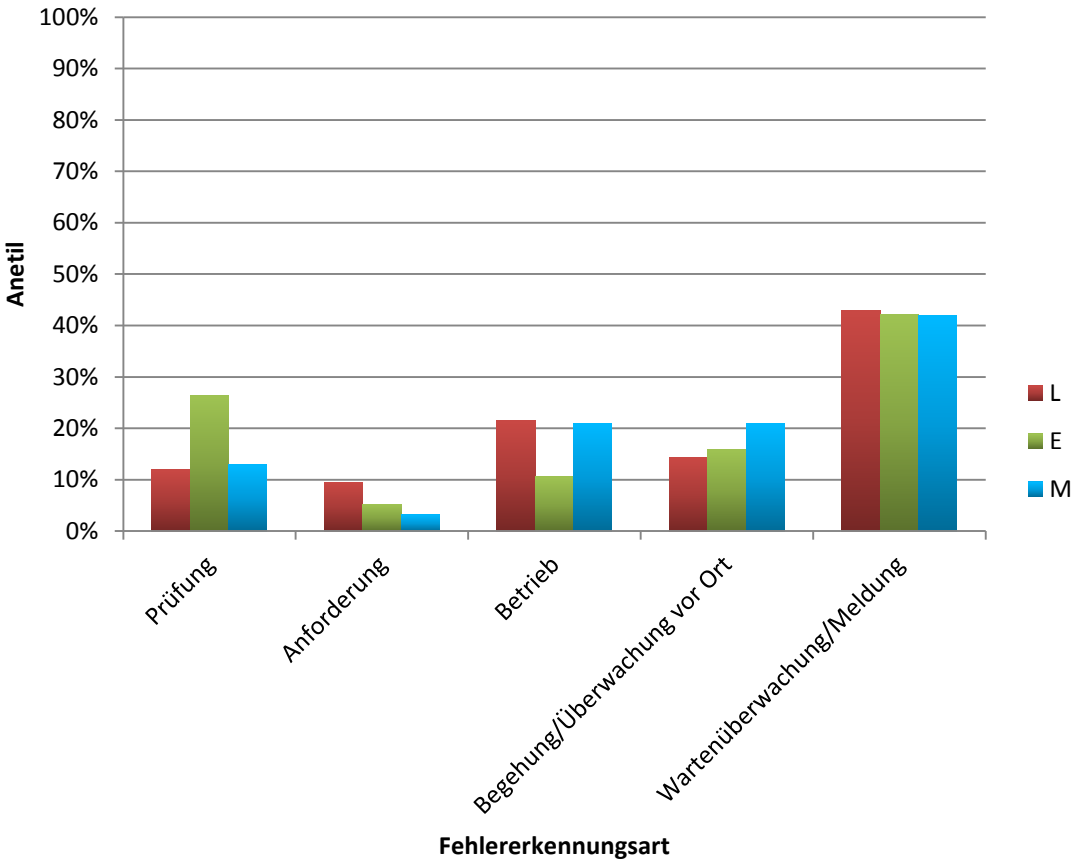

Abb. 4.51 Anteile der verschiedenen Fehlererkennungsarten in der Anlage DWR C für die Komponenten der Elektro- und Leittechnik sowie für Messumformer

In der Auswertung zur Anlage SWR A wurde bereits darauf hingewiesen (siehe Abschnitt 4.1.4.3), dass die Fehlererkennung bei Anforderung von besonderem Interesse

ist. In dem hier vorliegenden Fall liegt diese Fehlererkennungsart für die Ereignisse mit Leittechnik-Komponenten im Bereich von ca. 10 %, bei den Elektrotechnik-Ereignissen bei ca. 5 % und für die Messumformer bei ca. 3 %. Aufgrund dieser geringen Anteile wird diese Thematik im vorliegenden Bericht nicht weiter verfolgt.

4.5.4.4 Ursache

In der folgenden Auswertung geht es um die Ursache der vorliegenden Ereignisse der Anlage DWR C. In Abbildung 4.52 ist dafür für die Leittechnik-Komponenten, die Elektrotechnik-Komponenten und die Messumformer dargestellt, welche Anteile die jeweilige Ursache an den Ereignissen hat. Zur besseren Übersicht wurden die Ursachen, die in der Leittechnik, in der Elektrotechnik und bei den Messumformern einen Anteil von kleiner als 3 % aufweisen, nicht mit in das Diagramm aufgenommen.

Es zeigt sich, dass für die Leittechnik- und Elektrotechnik-Komponenten die höchsten Anteile (ca. 28 % bzw. ca. 50 %) bei einem Bauelementausfall ohne äußeren, erkennbaren Einfluss lagen. Für die Messumformer lag der Anteil dieser Ursache bei ca. 18 %.

Kleinere Anteile hatte die Ursache „Softwareausfall“. Diese Anteile lagen für die Leittechnik-Komponenten bei ca. 17 % und bei ca. 7 % für die Messumformer, wohingegen keine Ereignisse im Bereich der Elektrotechnik mit dieser Ursache vorlagen. In Abschnitt 5.1 wird nochmals auf die Thematik der Softwarefehler eingegangen.

Bei den Elektrotechnik-Ereignissen konnte die Ursache mit jeweils einem Anteil von 10 % auf „Alterung“ und „falschen Schalthandlungen“ zurückgeführt werden. Bei den Messumformern lagen erneut zumeist Driftereignisse mit einem Anteil von etwa 21 % vor.

Ebenfalls kann Abbildung 4.51 entnommen werden, dass in ca. 15 % der Fälle für alle Komponentenarten (L, E, M) die Ausfallursache nicht feststellbar war.

Zu der Ursache „Sonstiges“ liegen keine näheren Informationen vor.

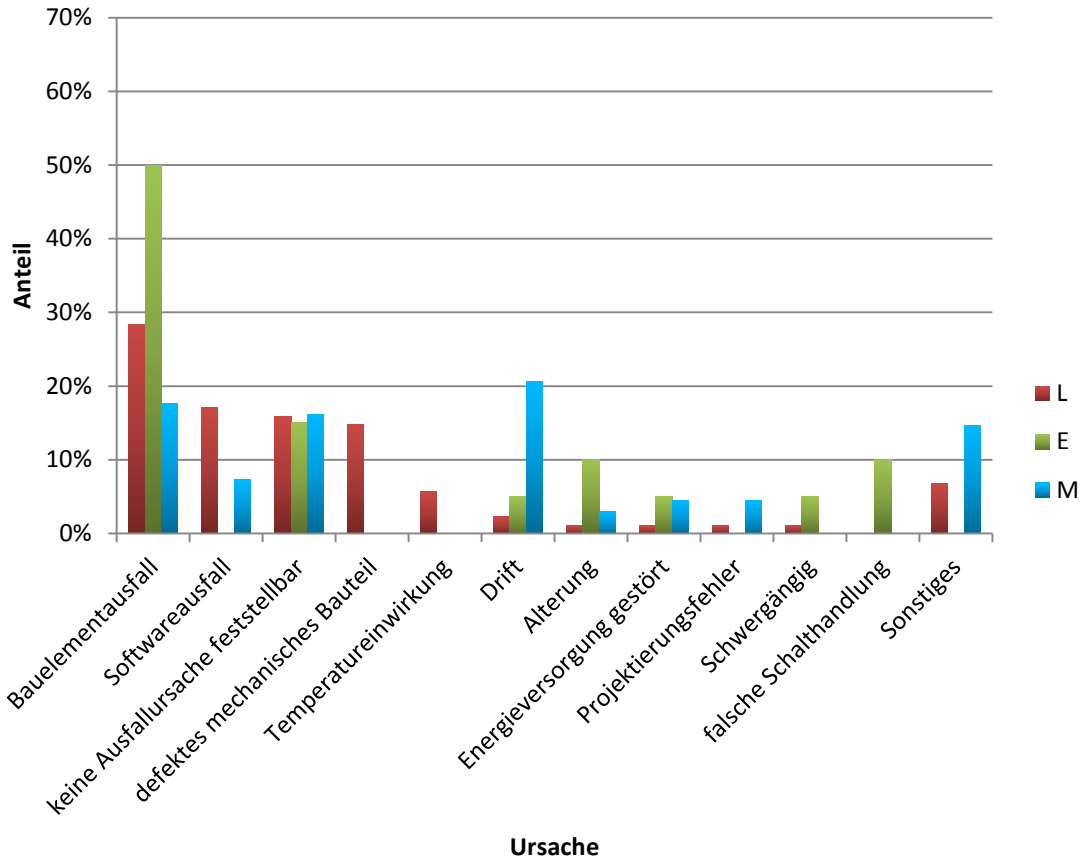

Abb. 4.52 Anteile der verschiedenen Ursachen für die Ereignisse in der Anlage DWR C für die Komponenten der Elektro- und Leittechnik sowie für Messumformer

4.5.4.5 Anlagenzustand bei Ereigniseintritt

Die Analyse der Betriebszustände der Anlage, in der die Ereignisse auftraten, folgt in diesem Abschnitt. Die entsprechenden Anteile der Anlagenzustände sind in Abbildung 4.53 zu finden.

Die Grafik verdeutlicht, dass fast alle Ereignisse (> 80 %) für die Komponentenarten L, E und M im Leistungsbetrieb aufgetreten sind. Daneben ist noch der Zustand „Revision“ zu nennen, in dem die Anteile für alle Komponentenarten (L, E, M) bei ca. 15 % liegen. Bei einer genaueren Betrachtung der letztgenannten Ereignisse zeigt sich, dass von diesen Ereignissen erwartungsgemäß mehr als die Hälfte bei Prüfungen bzw. wiederkehrenden Prüfungen (WKPs) entdeckt wurden. Aufgeschlüsselt nach der jeweili-

gen Komponentenart liegen diese Anteile bei etwa 45 % (L), 75 % (E) und 55 % (M). Nur sehr geringe Anteile entfallen auf die anderen Anlagenzustände.

In Abschnitt 5.6 wird für die Anlage SWR A die Anzahl der Ereignisse bei den jeweiligen Anlagenzuständen in Relation zu den zeitlichen Anteilen, die die einzelnen Anlagenzustände im Jahr einnehmen, gesetzt. Aufgrund der geringen Datendichte für die Anlage DWR C wird dieses hier nicht gemacht.

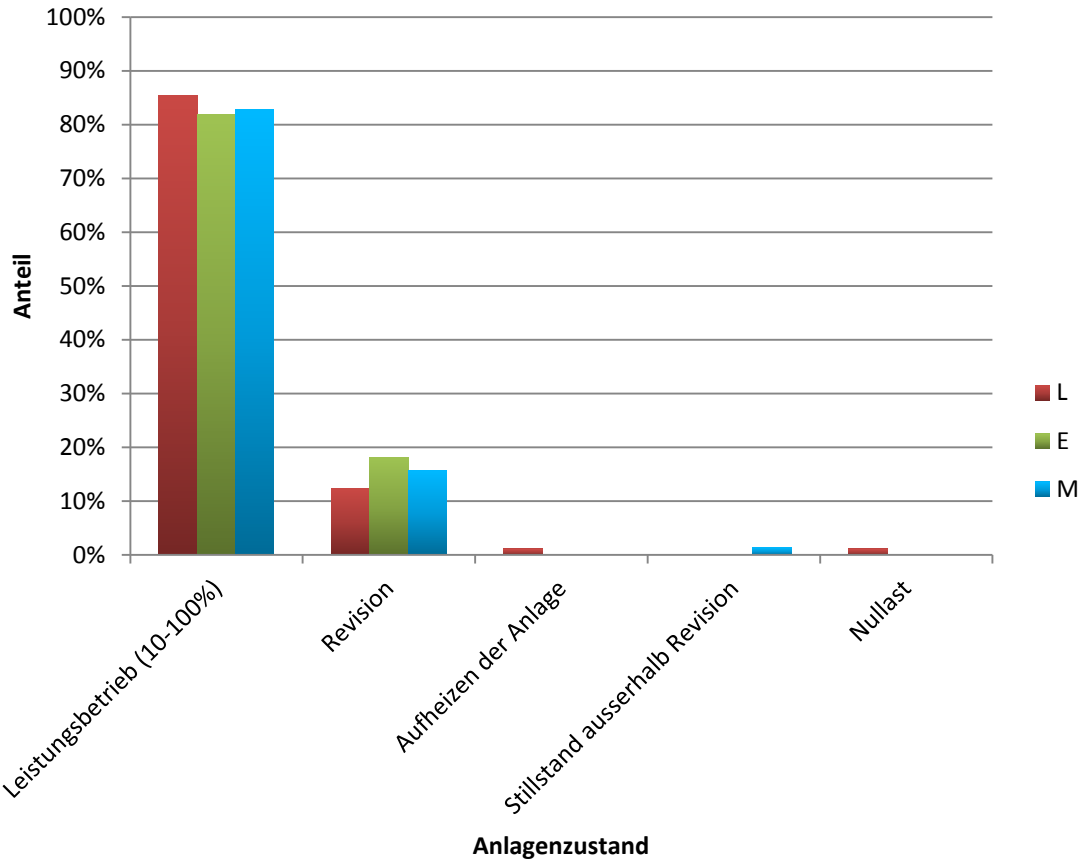

Abb. 4.53 Anteile der Anlagenzustände bei Ereigniseintritt in der Anlage DWR C für die Komponenten der Elektro- und Leittechnik sowie für Messumformer

5 Vertiefte Analyse der Auswertungen

Das folgende Kapitel enthält eine vertiefte Analyse zu den in Kapitel 1 durchgeführten Auswertungen. Die in diesen Auswertungen aufgeworfenen Fragen und die Thematiken, die interessante Erkenntnisse vermuten lassen, werden dafür genauer untersucht. Für diese Untersuchungen werden insbesondere entsprechend detaillierte Informationen hinzugezogen und es wurden Gespräche mit den Anlagen gesucht.

5.1 Softwarefehler

Ein besonderes Augenmerk liegt in diesem Bericht auf den Ereignissen, bei denen Komponenten aufgrund von Fehlern in der Software ausgefallen sind. Zu diesen Fehlern gehören nach Ansicht der GRS nicht nur reine Softwarefehler, sondern auch Fehler die an Bauteilen oder Komponenten, die für die Funktionsfähigkeit oder die Bedienung der Software nötig sind, aufgetreten sind. Aus diesem Grund hat die GRS die vorliegenden Ereignisse auf das Erfüllen der nachfolgenden Kriterien konservativ bewertet und entsprechend eingeteilt:

- RS: Ereignis aufgrund eines Softwarefehlers (z. B. Programmierungsfehler)
- HS: Ereignis aufgrund eines Softwarefehlers, der durch einen Fehler einer zugehörigen Hardware ausgelöst wurde (z. B. Pufferbatterie verursacht Programmverlust)
- KS: Ereignis aufgrund einer Komponente, die in direktem Zusammenhang zur Software steht und die ohne die Software nicht eingesetzt wäre (z. B. Touch-Display)
- Rest: Alle anderen Ereignisse

Auf Grundlage dieser konservativen Einteilung in RS, HS, KS und Rest werden in den folgenden Abschnitten die Ereignisse der Anlagen SWR A, DWR A und DWR C vertieft ausgewertet. Die vorliegende Datengrundlage bei den Anlagen SWR B und DWR B ist für diese Einteilung nicht ausreichend, so dass für diese Anlagen keine entsprechende Auswertung durchgeführt werden kann.

5.1.1 SWR A

Entsprechend der zusätzlichen Einteilung in RS, HS, KS und Rest ergeben sich für die Ereignisse der Leittechnik-Komponenten der Anlage SWR A die in Abbildung 5.1 gezeigten Anteile. Es ist deutlich zu erkennen, dass ca. 87 % der Ereignisse auf Fehler, die in keinem Zusammenhang mit der Software stehen, zurückzuführen sind. Dem gegenüber stehen die „Software-relevanten“-Ereignisse, wobei auf RS und KS jeweils ca. 4 % der Ereignisse fallen und auf HS ca. 6 %.

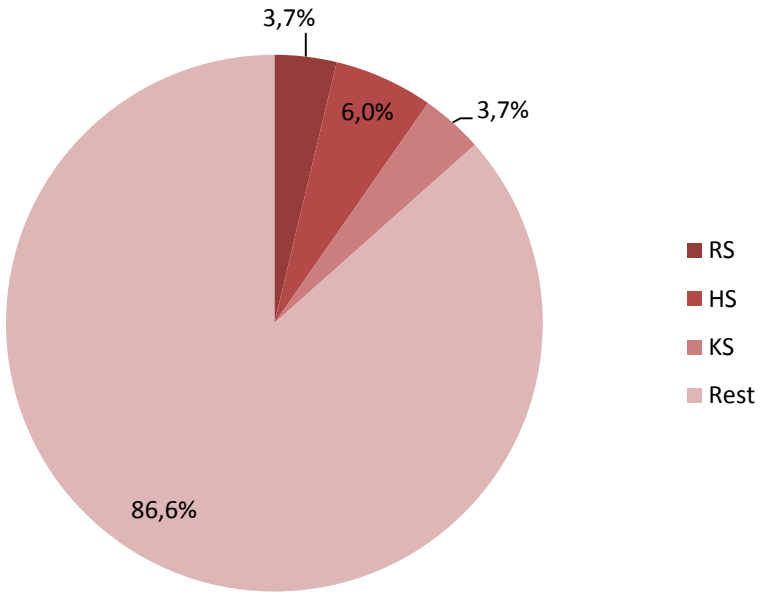

Abb. 5.1 Anteile der Ereignisse der Leittechnik-Komponenten an RS, HS, KS und Rest in der Anlage SWR A

Da in diesem Abschnitt die „Software-relevanten“ Ereignisse von Interesse sind, werden in Abbildung 5.2 ausschließlich diese Ereignisse betrachtet. Es zeigt sich, dass die Anteile von HS mit ca. 44 % am größten sind und RS sowie KS jeweils einen Anteil von ca. 28 % haben.

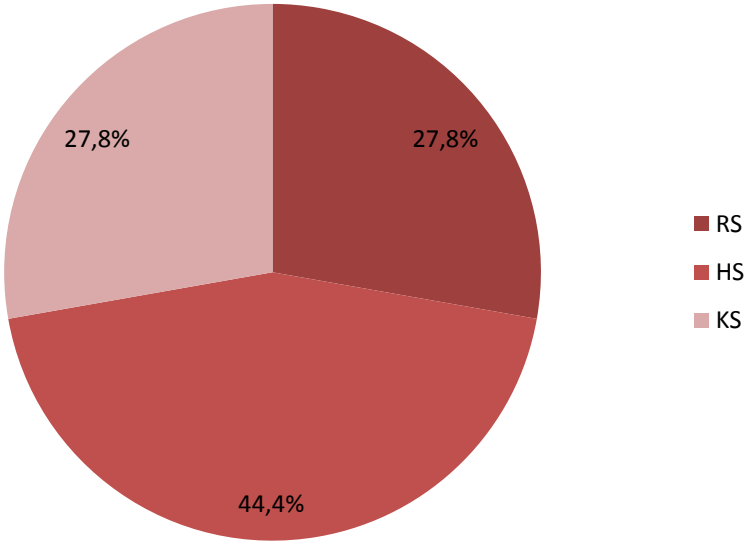

Abb. 5.2 Anteile von RS, HS und KS bei „Software-relevanten“ Ereignissen in der Leittechnik in der Anlage SWR A

Da im Rahmen dieses Projektes die reinen Softwarefehler (RS) von besonderem Interesse sind, werden im Folgenden diese Fehler und die ergriffenen Abhilfemaßnahmen an Beispielen erläutert:

- Baugruppeninterner Fehler im Diagnosepuffer
  → Baugruppe wurde ausgetauscht
- Kommunikationsstörung
  → Programm nach Urlöschen der CPU neu übersetzt und übertragen
- Kompletter Programmverlust der Sicherheitssteuerung trotz betriebsbereiter Pufferbatterien
  → Programm neu übertragen

Da es sich bei den Komponenten, an denen Softwarefehler aufgetreten sind, um nicht sicherheitstechnisch wichtige Komponenten handelt, wurde die Ursache oftmals nicht genau ermittelt. Daher liegen den Anlagen meistens keine weiteren Informationen zur Fehlerursache vor.

5.1.2 DWR A

Für die Ereignisse der Leittechnik-Komponenten der Anlage DWR A wird die Einteilung in RS, HS, KS und Rest ebenfalls vorgenommen. Die entsprechenden Anteile der Ereignisse an RS, HS und Rest können Abbildung 5.3 entnommen werden. Die Kategorie KS wurde bei diesen Ereignissen nicht vergeben. Ähnlich wie bei der Auswertung für die Anlage SWR A ist zu erkennen, dass der größte Anteil der Ereignisse (ca. 72 %) auf Fehler, die in keinem Zusammenhang mit der Software stehen, fällt. Demensprechend nehmen die „Software-relevanten"-Ereignisse einen Anteil von etwa einem Viertel der Ereignisse ein. Für RS bedeutet dies einen Anteil von ca. 24 % und für HS von ca. 4 %.

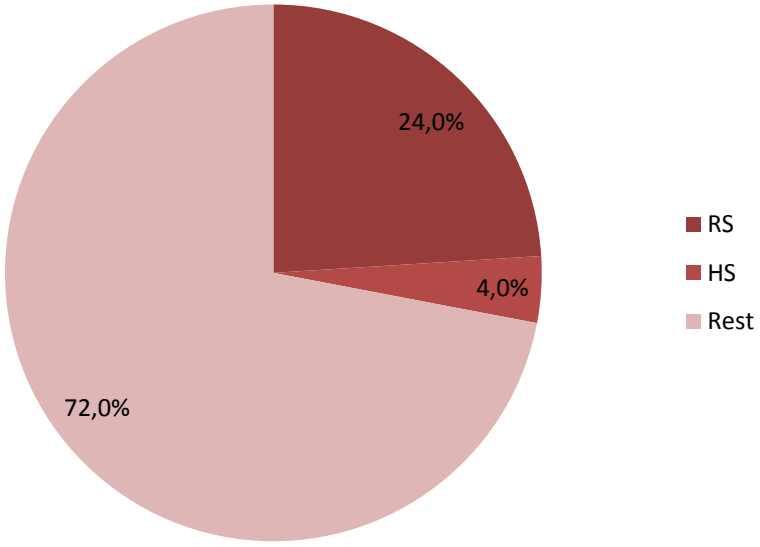

Abb. 5.3 Anteile der Ereignisse der Leittechnik-Komponenten an RS, HS und Rest in der Anlage DWR A

Bei einer ausschließlichen Betrachtung der „Software-relevanten" Ereignisse zeigt sich, dass ca. 86 % auf Softwarefehler (RS) und ca. 14 % auf einen die Software beeinflussenden Hardwareausfall (HS) entfallen (siehe Abbildung 5.4).

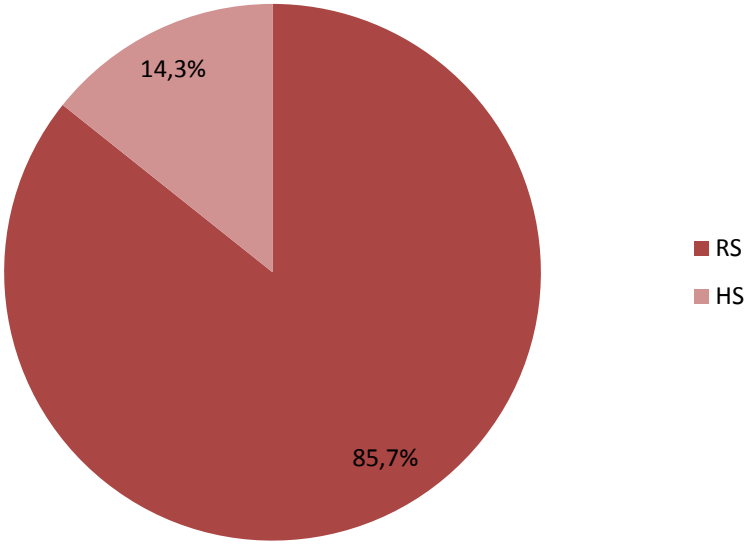

Abb. 5.4 Anteile von RS und HS bei „Software-relevanten“ Ereignissen in der Leittechnik in der Anlage DWR A

Da im Rahmen dieses Projektes die reinen Softwarefehler (RS) von besonderem Interesse sind, werden im Folgenden diese Fehler und die ergriffenen Abhilfemaßnahmen an Beispielen erläutert:

- Ausfall einer Systemfunktion eines Überwachungssystems
  → Ertüchtigten Softwarebaustein übertragen
- Automatisierungsprozessor wegen Speicherfehler ausgefallen
  → Urgelöscht und zurückgesetzt
- Siebbänder schalten sporadisch im Automatikbetrieb nicht zu
  → Programm der Steuerung angepasst
- Wartenmeldung steht nur ca. 20 s an und quittiert sich dann selbst
  → Programm geändert

Da es sich bei den Komponenten, an denen Softwarefehler aufgetreten sind, um nicht sicherheitstechnisch wichtige Komponenten handelt, wurde die Ursache oftmals nicht genau ermittelt. Daher liegen den Anlagen meistens keine weiteren Informationen zur Fehlerursache vor.

5.1.3 DWR C

Aufgrund der vorgenommen Einteilung der Ereignisse im Bereich der Leittechnik in RS, HS, KS und Rest ergeben sich für die Anlage DWR C die jeweiligen Anteile gemäß Abbildung 5.5. Wie bereits bei den vorangegangenen Einteilungen zeigt sich auch hier, dass der größte Anteil der Ereignisse aufgrund von Fehlern, die in keinem Zusammenhang mit der Software stehen, auftreten. Dieser Anteil liegt bei ca. 60 %. Somit haben die „Software-relevanten"-Ereignisse einen Anteil von insgesamt ca. 40 %. Dies teilt sich auf in ca. 20 % RS, ca. 12 % HS und ca. 8 % KS.

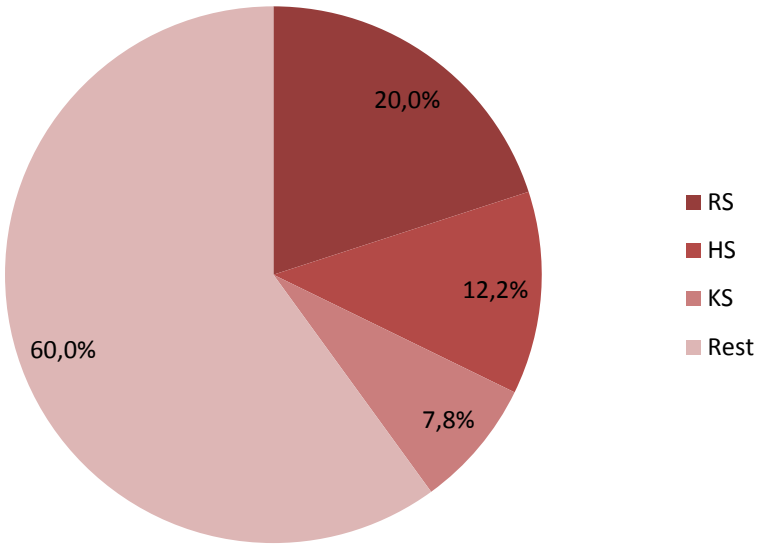

Abb. 5.5 Anteile der Ereignisse der Leittechnik-Komponenten an RS, HS, KS und Rest in der Anlage DWR C

Werden nur die „Software-relevanten" Ereignisse betrachtet, so liegt der Anteil von RS bei ca. 50 %, von HS bei ca. 31 % und von KS bei ca. 19 % (siehe Abbildung 5.6).

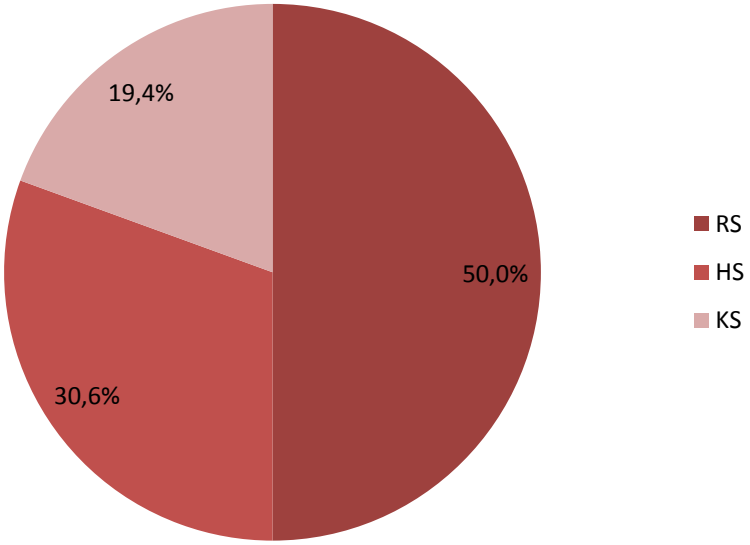

Abb. 5.6 Anteile von RS, HS und KS bei „Software-relevanten“ Ereignissen in der Leittechnik in der Anlage DWR C

Da im Rahmen dieses Projektes die reinen Softwarefehler (RS) von besonderem Interesse sind, werden im Folgenden diese Fehler und die ergriffenen Abhilfemaßnahmen an Beispielen erläutert:

- Steuerschrank in Störung
  → Software geladen und geprüft
- Baugruppe zeigt „Run“ und „Stop“ gleichzeitig an
  → Telegrammaufträge beim Kommunikationsprozessor neu geladen
- Ausfall der CPU
  → Busverbindungstelegramme neu geladen und synchronisiert
- Untergruppensteuerung in Störung (Rückmeldung „Ein“ fehlt)
  → Neustart der Steuerung
- Programmverlust der Betriebssteuerung
  → Software wurde wieder eingespielt

Da es sich bei den Komponenten, an denen Softwarefehler aufgetreten sind, um nicht sicherheitstechnisch wichtige Komponenten handelt, wurde die Ursache oftmals nicht

genau ermittelt. Daher liegen den Anlagen meistens keine weiteren Informationen zur Fehlerursache vor.

5.1.4 Meldepflichtige Ereignisse mit Softwarefehlern als Ursache

Die GRS untersucht im Auftrag des Bundesministeriums für Umwelt, Naturschutz, Bau und Reaktorsicherheit die nach AtSMV meldepflichtigen Ereignisse von Kernkraftwerken. Hierbei fielen in der Vergangenheit einige Ereignisse auf, bei denen Fehler in der Software die Ursache beziehungsweise die vermutliche Ursache waren. Diese meldepflichtigen Ereignisse werden im Folgenden kurz beschrieben.

5.1.4.1 Fehlerhafte sekundärseitige Lastabsenkung und nicht erfolgter Stabeinwurf

Während des Streckbetriebes sollte ein Gliederzug in der Excore-Neutronenflussinstrumentierung ausgetauscht werden. Hierzu wurden in der Reaktorleistungsleittechnik (TELEPERM XS-System) Simulierungen durchgeführt, die zu Fehlsignalen und daraus resultierend zu einer fehlerhaften sekundärseitigen Lastabsenkung führten. Außerdem konnten Steuerstäbe nicht durch betriebliche Anforderungen (wohl aber durch den Reaktorschutz) verfahren werden. Nach Rücknahme der Simulierungen funktionierte das System wieder ordnungsgemäß. Die nachfolgenden Untersuchungen zeigten, dass sich bei der gleichzeitigen Durchführung von mehreren Simulierungen (in allen sechs Ebenen des Systems) Fehlsignale bis zur Auslöseebene durchsetzen und die oben beschriebenen Auswirkungen nach sich zogen. /ME 00/

5.1.4.2 Absturz eines Brennelementes nach dem fehlerhaften Anheben

Beim Anheben eines Brennelementes mit der Brennelementwechselmaschine verhakte sich dieses mit einem nebenstehenden Brennelement. Dieses nebenstehende Brennelement wurde mit in die Höhe gezogen, rutschte schlussendlich ab und stürzte in seine obere Kerngitterposition zurück. Unter anderem war hierbei die automatische Überlastabschaltung der Steuerung der Brennelementwechselmaschine nicht erfolgt. Der Grund für den Ausfall der automatischen Lastabschaltung lag in den Folgen einer Nachrüstung einer PC-Schnittstelle an die Brennelementwechselmaschinensteuerung zum Anschluss eines externen Diagnose- und Wartungsgerätes (PC). Nach der Nach-

rüstung der PC-Schnittstelle kam es zu Diskrepanzen in der Lastmessung und es mussten Parameter nachgeladen werden (über die PC-Schnittstelle). Die dem Ereignis nachfolgende Untersuchung zeigte, dass es bei Benutzung der PC-Schnittstelle zu undefinierten Zuständen bis zur Blockierung der automatischen Überlastabschaltung kommen kann. Die PC-Schnittstelle wurde daher bis auf weiteres blockiert. /ME 01/

5.1.4.3 Temporäre Störungen von SYMPHONY MELODY Baugruppen

In einem Leittechnik-Schrank mit betrieblichen Regelungen trat eine Störung in der Buskommunikation von SYMPHONY MELODY Baugruppen auf. Hier führte ein Fehler in der Firmware von bestimmten Hardwaretypen von SYMPHONY MELODY Baugruppen zu einem sporadisch auftretenden Dauersenden von Signalen. Diese Signale blockierten den Kommunikationsbus und somit war eine Kommunikation der SYMPHONY MELODY Baugruppen untereinander nicht mehr möglich, was zu einem Ausfall der betroffenen leittechnischen Einrichtung führte. Im Begrenzungssystem waren ebenfalls Baugruppen des betroffenen Typs eingebaut, so dass prinzipiell auch sicherheitstechnisch wichtige Komponenten von der Fehlfunktion hätten betroffen sein können. /ME 05/

5.1.4.4 Nicht spezifikationsgerechtes Verhalten des SINUPERM N Mittelbereichsmesskanals

Bei einem in SINUPERM N ausgeführten Neutronenfluss-Messsystem kam es wiederholt zu Reaktorschnellabschaltungen im Bereich niedriger, ansteigender Reaktorleistungen. Nach Testreihen in der Revision zeigte sich ein nicht spezifikationsgerechtes Überschwingverhalten bei der Bildung des Signals „Relative Neutronenflussänderungsgeschwindigkeit“ im Neutronenfluss-Mittelbereichsmesskanal. Die Ursache lag in einem Programmierungsfehler in der Firmware. /ME 07/

5.1.4.5 Fehlerhafte Auslösung von Brandschutzklappen

Innerhalb eines Jahres kam es im Zusammenhang mit einer Störung in der Brandmeldeanlage (Siemens SM88) zum unberechtigten Auslösen von Brandschutzklappen (einmal 28 Stück und einmal 26 Stück). Eine nachfolgende Untersuchung zeigte, dass es in der Steuerung der Brandmeldeanlage aus unbekannter Ursache zu sporadisch

auftretenden Resets kommt. Bei Wiederanlaufen des Systems kommt es zu undefinierten Zuständen an den Ausgängen der Ausgabebaugruppen, die im Auslösen von Brandschutzklappen resultieren können. Dem Hersteller ist dieser Fehler bekannt und er empfiehlt den Einbau nachgeschalteter Baugruppen, die verhindern, dass undefinierte Zustände als Ausgangssignale weitergegeben werden. /ME 13/

5.2 Pufferbatterien

Wie die Auswertungen in Kapitel 1 gezeigt haben, sind in den Anlagen Softwarefehler aufgetreten, die durch Ausfälle von Pufferbatterien hervorgerufen wurden. Pufferbatterien kommen in den Anlagen beispielsweise in den CPUs der Simatic S7-Steuerungen zum Einsatz. Dort werden sie benötigt, um bei Ausfall der Spannungsversorgung den Inhalt des RAM-Speichers zu erhalten. Solange die Spannungsversorgung der Steuerung vorhanden ist, führt der Ausfall einer Pufferbatterie lediglich zur Anregung einer Meldung. Die Funktion der Steuerung wird aber durch diesen Ausfall nicht beeinträchtigt. Fällt die Pufferbatterie jedoch bei abgeschalteter Spannungsversorgung aus, führt dies dazu, dass der Inhalt des RAM-Speichers verloren geht. Ohne Speicherinhalt läuft die Steuerung bei Wiedereinschalten der Spannungsversorgung nicht an. Da die Steuerung bei abgeschalteter Spannungsversorgung außer Betrieb ist (CPU-Betriebszustand „Stopp“), wird der Ausfall der Pufferbatterie erst beim Zuschalten der Spannung durch das Nichtanlaufen der Steuerung erkannt. Die entsprechende Komponente bleibt also außer Betrieb.

Die in der Auswertung erkannten Ausfälle von Pufferbatterien wurden mit den Anlagen diskutiert. Die Gespräche haben gezeigt, dass größtenteils die folgenden Ursachen für diese Ausfälle verantwortlich sind:

- Chargenproblem
  Die Pufferbatterien einer Charge wiesen nicht die gewünschten Eigenschaften auf. Nach Entdeckung dieses Problems wurden die Batterien dieser Charge vollständig ausgetauscht.

- Ständig belastete Pufferbatterien
  Die Steuerung der Brennelementlademaschine wird nur während der Revisionszeit benötigt. In der restlichen Zeit wird diese nicht benutzt, so dass auch die entsprechende Spannungsversorgung nicht zugeschaltet ist. Daher werden außerhalb der Revisionszeiten die vorhandenen Pufferbatterien in der Lademaschinensteuerung

zum Erhalt des RAM-Speichers dauerhaft belastet. Dies führt dazu, dass die Batterien häufiger ausfallen und dadurch ein entsprechender Austausch erforderlich ist. Um die Ausfälle der Steuerungen zu verhindern, haben die Anlagen ein jährliches Austauschintervall anstatt den typischen 2 Jahren für diese Pufferbatterien eingeführt.

Der Verlust der Software aufgrund von ausgefallenen Pufferbatterien ist bei der Betrachtung der programmierbaren oder rechnerbasierten Komponenten als ein möglicher Ausfallmechanismus zu berücksichtigen.

5.3 Ausfallmechanismen

Zusätzlich zu den im vorherigen Abschnitt erwähnten Softwareausfällen aufgrund von ausgefallenen Pufferbatterien, hat die Auswertung der Daten gezeigt, dass Fehler in der Programmierung der Software auftreten können. Diese Fehler sind aber meist schwer zu detektieren, da sie beispielsweise nur sporadisch oder bei bestimmten Betriebszuständen auftreten. Beispiele für frühzeitig erkannte Programmierungsfehler stellen die Rückrufaktionen aus Abschnitt 5.5 dar. Beispiele für Ereignisse bei denen Ausfälle aufgrund von Programmierungsfehlern aufgetreten sind, sind in Abschnitt 5.1.4 beschrieben. Darüber hinaus ergaben sich aus der Datenauswertung keine weiteren Erkenntnisse für die programmierbaren oder rechnerbasierten Komponenten hinsichtlich weiterer unbekannter Ausfallmechanismen.

Geänderte Prüfprozeduren hätten unter Umständen Aufschlüsse über vorher unbekannte Ausfallmechanismen geben können. Nach Auskunft der Anlagen haben sich mit der Einführung von programmierbaren oder rechnerbasierten Komponenten aber einige der Prüfprozeduren für solche Komponenten vereinfacht bzw. sind nun weniger zeitaufwendig. Die Prüfprozeduren haben sich in dem Sinne vereinfacht, dass beispielsweise nicht mehr jedes Bauelement (z. B. UND- oder ODER-Gatter) in großen Verschaltungen geprüft werden muss, sondern durch den Einsatz von z. B. Mikroprozessoren nur noch deren Funktion einmal getestet werden muss (Funktion/keine Funktion). Andere Prüfprozeduren hingegen sind komplizierter geworden. Beispielsweise ist die Anzahl der Einstellungsmöglichkeiten programmierbarer oder rechnerbasierter Komponenten zum Teil angestiegen, wobei viele dieser Möglichkeiten überflüssig für die in der Anlage konkret genutzte Funktion sind.

5.4 Produktlebensdauer

Laut Auskunft der Anlagen werden Komponenten, soweit wirtschaftlich vertretbar, bevorzugt repariert. Aufgrund des komplexeren Aufbaus ist dies für die programmierbaren oder rechnerbasierten Komponenten oftmals nicht möglich. Des Weiteren werden in kürzeren Abständen Nachfolgeprodukte auf den Markt gebracht, was eine langfristige Ersatzteilbeschaffung erschwert. Aus diesem Grund hat sich die GRS dazu entschieden, die Ersatzteilbeschaffungslage der programmierbaren oder rechnerbasierten Leittechnik-Komponenten am Beispiel von Hersteller A zu untersuchen. In dieser Untersuchung wurden insbesondere Informationen zur Produktauslaufphase, Produktstreichung und Produktabkündigung eingeholt. Die Beschreibung der einzelnen Phasen erfolgt mit Hilfe der entsprechenden Definitionen von Hersteller A:

- Produktauslaufphase
  - Beginn der zehnjährigen Ersatzteilverfügbarkeit bzw. Reparaturverpflichtung
  - Dauer der Phase beträgt etwa ein Jahr
  - aktive Ankündigung
  - keine aktive Vermarktung der Neuteile mehr (allerdings kann das Produkt bis zur Produktstreichung normal bestellt werden)
- Produktstreichung
  - Produktion eingestellt
  - Produkt nur noch als Ersatzteil verfügbar solange wirtschaftlich sinnvoll
  - nur noch Austausch defekter Komponenten oder Reparatur
- Produktabkündigung
  - keine Produktion mehr
  - Produkt ist im Katalog nicht mehr verfügbar
  - keine technische Unterstützung oder Beratung mehr

Die Lebensdauer eines Produktes kann in eine aktive und eine passive Phase eingeteilt werden. Die aktive Phase des Produkts beginnt mit der Markteinführung und endet mit dem Beginn der Auslaufphase. Danach startet die passive Phase, welche mit der

Abkündigung des Produktes endet. Die passive Phase besteht normalerweise für einen Zeitraum von ca. 10 Jahren und teilt sich in die oben genannten Phasen auf. Diese Phasen können bei anderen Herstellern unterschiedlich aufgebaut sein und auch einen anderen Zeitraum einnehmen.

Um einen ersten Einblick über die derzeitige Ersatzteilbeschaffungslage zu erhalten, wurden aus den Daten der Anlage SWR A 1294 Leittechnik-Komponenten des Herstellers A ausgewählt, bei denen Produktlebensdauer näher betrachtet wurde. Hierbei ist zu beachten, dass Komponenten des gleichen Typs in der Anlage mehrfach verbaut sein können und somit hier dann auch mehrmals vorkommen können. Für diese Betrachtung wird für jede Komponente festgestellt, inwiefern sie einer Phase zugeordnet werden kann. Hierbei wird unterschieden in:

- „noch nicht angekündigt“
  Der Beginn der entsprechenden Phase ist noch nicht angekündigt.
- „angekündigt“
  Der Hersteller hat auf den kommenden Beginn der entsprechenden Phase hingewiesen.
- „aktiv“
  Die entsprechende Phase hat begonnen.
- „bereits beendet“
  Die entsprechende Phase ist beendet.

Für die ausgewählten Leittechnik-Komponenten sind die verschiedenen Anteile der Phasen in Abbildung 5.7 dargestellt. Die Farben wurden hier so gewählt, dass keine Unstimmigkeiten zu den oben gezeigten Abbildungen auftreten. Da in dieser Auswertung alle ausgewählten Komponenten enthalten sind und somit ein Typ mehrfach vorkommen kann, hat eine solche mehrfach eingebaute Komponente ein stärkeres Gewicht bei der Auswertung.

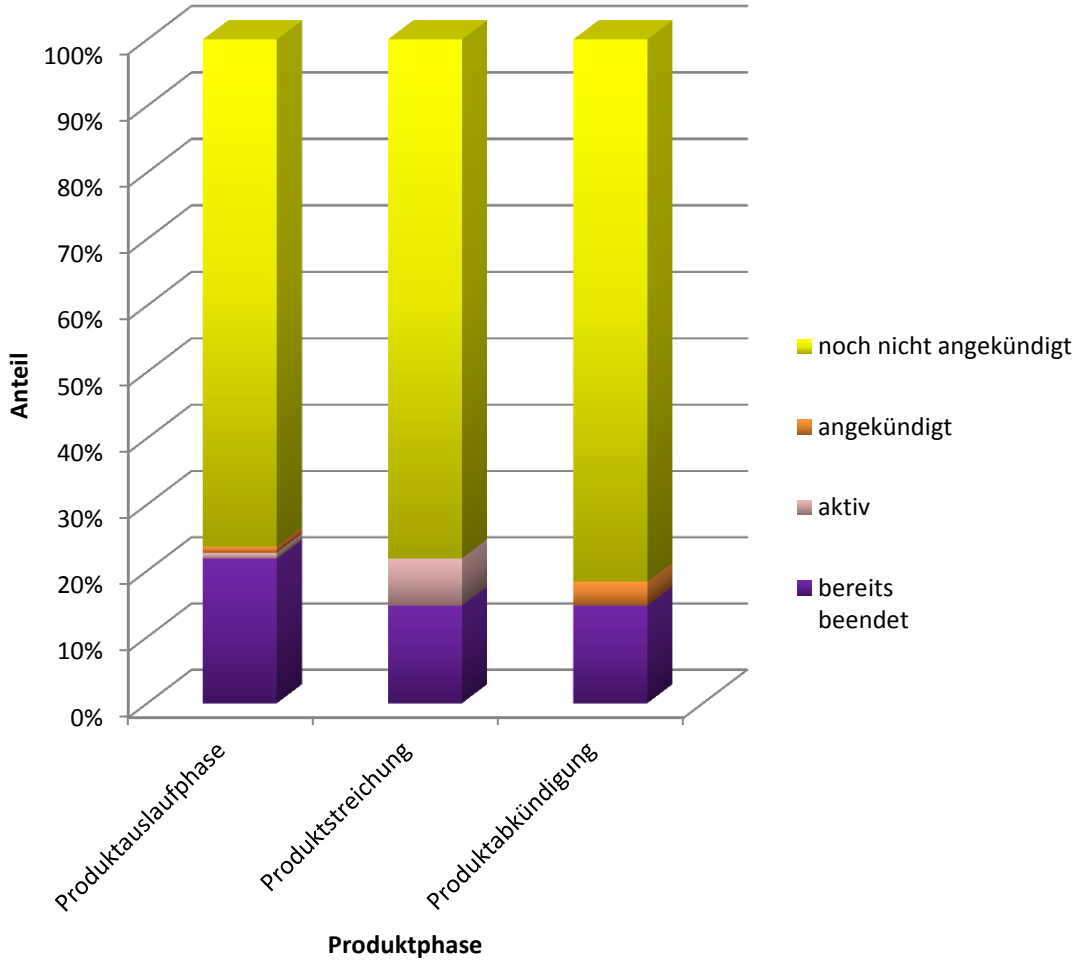

Abb. 5.7 Anteile der ausgewählten Leittechnik-Komponenten der Anlage SWR A an den einzelnen Produktphasen der Produktlebensdauer

Es ist deutlich zu erkennen, dass für die meisten Komponenten die passive Phase der Lebensdauer noch nicht angekündigt ist (> 75 %). Für die erste passive Phase, die Produktauslaufphase, ergibt sich aus dem Diagramm, dass für ca. 1 % der Komponenten diese Phase angekündigt ist, für ca. 1 % der Komponenten diese Phase aktiv ist und für ca. 22 % der Komponenten diese Phase bereits beendet ist. Für den Teil der Komponenten für die die Produktauslaufphase bereits beendet ist, zeigt sich im 2. Balken, dass die Phase „Produktstreichung“ bei ca. 7 % aktiv ist und bei weiteren ca. 15 % ebenfalls bereits beendet ist. Für diese ca. 15 % der Komponenten ist auch die Phase „Produktabkündigung bereits beendet. Für weitere ca. 4 % ist die Produktabkündigung angekündigt. Aus dieser Zusammenstellung ergibt sich, dass ca. 85 % der ausgewählten Leittechnik-Komponenten noch nicht abgekündigt sind und

somit eine Neubestellung oder zumindest die Ersatzteilbeschaffung bzw. Reparatur beim Hersteller dieser Komponenten weiterhin möglich ist.

Die oben erwähnte Wichtung durch mehrfach eingesetzte Komponenten des gleichen Typs ist in Abbildung 5.8 bereinigt worden. In dieser Grafik haben somit alle Typen das gleiche Gewicht.

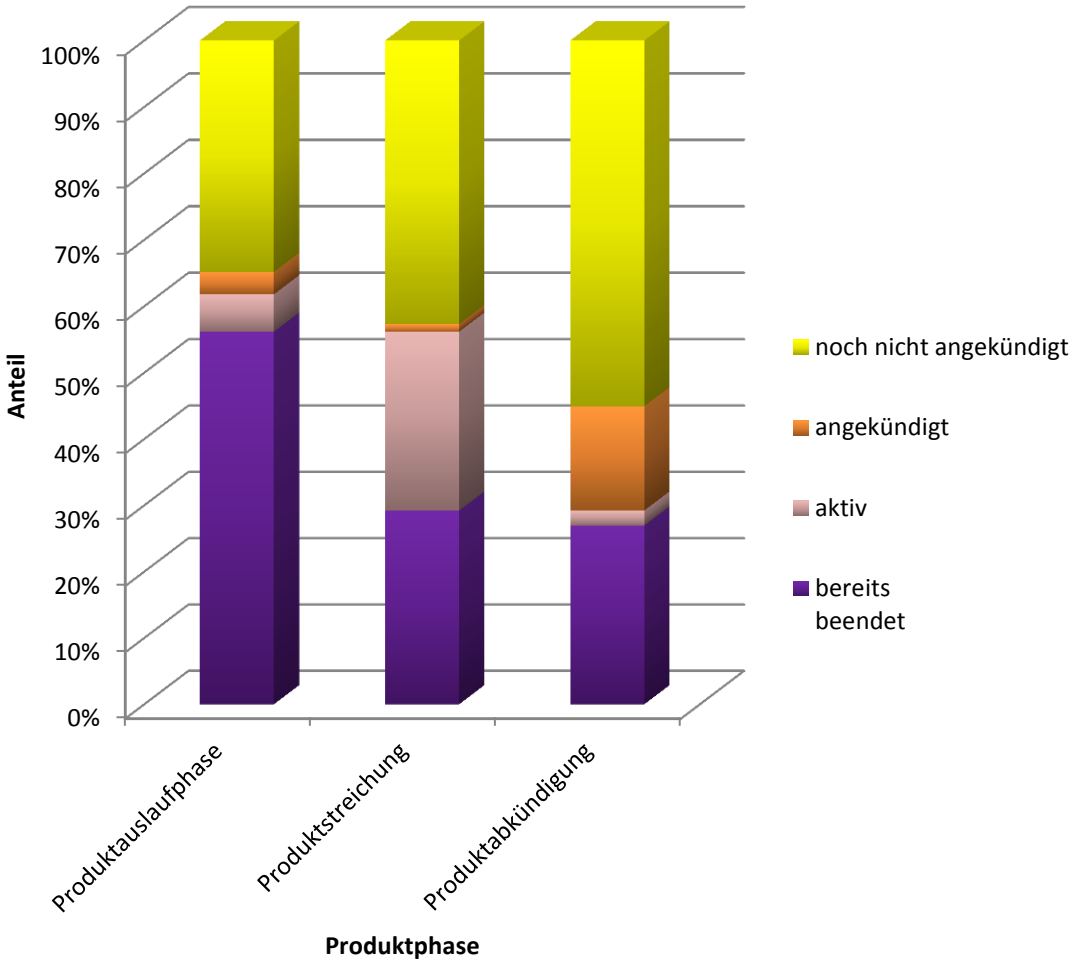

Abb. 5.8 Anteile der ausgewählten Leittechnik-Komponenten bereinigt um mehrfach eingesetzte Komponenten der Anlage SWR A an den einzelnen Produktphasen der Produktlebensdauer

Die korrigierte Auftragung der Daten zeigt ein geändertes Bild hinsichtlich der Ersatzteilsituation. Für ca. 29 % der untersuchten Komponententypen ist die Phase „Produktabkündigung“ bereits aktiv oder sogar schon beendet. Dies bedeutet für diese Komponenten, dass keine technische Unterstützung oder Beratung mehr gegeben ist

und dass keine Ersatzteile mehr bestellt werden können. Im Gegensatz dazu haben ca. 38 % der Komponenten die passive Phase der Lebensdauer noch nicht erreicht. Des Weiteren ist erkennbar, dass ca. 56 % der Komponententypen bereits die Produktauslaufphase beendet haben und davon sich in etwa die Hälfte aktiv in der Phase „Produktstreichung“ befinden. Zudem ist für ca. 16 % der Komponententypen die Produktabkündigung bereits angekündigt.

5.5 Rückrufaktionen

Im Rahmen der durchgeführten Auswertungen sind insbesondere zwei Rückrufaktionen der Hersteller A und C aufgefallen. Zu der Rückrufaktion des Hersteller A liegen keine weiteren Informationen vor. Die Rückrufaktion von Hersteller C war darin begründet, dass die Bürdenüberwachung unberechtigt angesprochen hat (unberechtigte Meldung der Bürdenüberwachung obwohl Bürde nicht überschritten wurde), wohingegen bei der Baugruppe selbst kein Fehler vorlag.

Bei beiden Rückrufaktionen wurde der bei den jeweiligen Komponenten vorgefundene Fehler durch ein Update der Firmware durch eine vorbeugende Instandhaltung behoben. Die Anlagen konnten zur Ursache der jeweiligen Fehler in der Firmware keine Aussage machen, so dass sich nur vermuten lässt, dass der Grund für die Rückrufaktionen Programmierungsfehler waren. Diese Art von Fehler stellt wie bereits erwähnt einen neuartigen Ausfall dar, welcher durch den Einsatz von programmierbaren oder rechnerbasierten Komponenten auftreten kann.

Im Allgemeinen wird eine neue Firmware von der Herstellerfirma geliefert. Dabei ist den Anlagen meistens nicht bekannt, welche Details sich in der neuen Firmware im Vergleich zur alten Firmware geändert haben. Für die nicht sicherheitstechnisch wichtigen Komponenten gibt es hierzu auch keine Anforderungen aus dem Regelwerk, so dass typischerweise auch keine weiteren Nachforschungen Seitens des Betreibers veranlasst werden. Für die sicherheitstechnisch wichtigen Komponenten sind jedoch Anforderungen vorhanden, so dass eine Firmware nur mit einer genehmigten Versionsnummer aufgespielt werden darf.

5.6 Anlagenzustand bei Ereigniseintritt

In diesem Abschnitt wird für die Anlage SWR A die Anzahl der Ereignisse bei den jeweiligen Anlagenzuständen in Relation zu den zeitlichen Anteilen, die die einzelnen Anlagenzustände im Jahr einnehmen, gesetzt. Hierfür wird zuerst einmal die Definition der hier vorkommenden Anlagenzustände aus den „Sicherheitsanforderungen an Kernkraftwerke“ aufgeführt /BMU B 12/:

- Leistungsbetrieb
  Die Betriebsphase eines Kernkraftwerks, in der eine gezielte nukleare Wärmeproduktion erfolgt (Betriebsphase A).

- Brennelementwechsel/Revision
  Flutraum vollständig geflutet (Betriebsphase E)

- Anfahren
  Das gezielte Überführen der Anlage in die Betriebsphase A (Leistungsbetrieb).

- Abfahren
  Gezieltes Überführen der Anlage von Betriebsphase A oder B in die Betriebsphase C.

- Abgeschaltet
  Heiß unterkritisch – Betriebliche Nachwärmeabfuhr über Nachkühlsystem nicht möglich (Betriebsphase B)

- Abgefahren
  Kalt unterkritisch – Betriebliche Nachwärmeabfuhr über Nachkühlsystem und Primärkreislauf druckdicht verschlossen (Betriebsphase C)/Nicht druckdicht verschlossener Primärkreis und Flutraum nicht vollständig geflutet (Betriebsphase D)

Die unterschiedlichen Zeiträume, die diese Anlagenzustände im Jahr einnehmen, wurden durch die Anlage abgeschätzt und durch die GRS mit den vorliegenden Betriebsberichten aus den Jahren 2000 bis 2009 abgeglichen. Da die einzelnen Zeiten in den Jahren leicht variieren, wurden für die folgende Betrachtung die jeweiligen Zeiten gemittelt. Für die einzelnen Anlagenzustände ergeben sich somit folgende Zeitannahmen:

- Leistungsbetrieb: 330 Tage

- Brennelementwechsel/Revision: 23 Tage

- Anfahren: 2 Tage
- Abfahren: 2 Tage
- Abgeschaltet/Abgefahren: 8 Tage

Die jeweiligen Anteile dieser Werte am gesamten Jahr sind in Abbildung 5.9 dargestellt. Die Farben wurden hier so gewählt, dass keine Unstimmigkeiten zu den oben gezeigten Abbildungen auftreten. Wie zu erwarten, nimmt der Leistungsbetrieb mit ca. 90 % den größten Anteil ein. Der Anlagenzustand „Brennelementwechsel/Revision“ nimmt zeitlich einen Anteil von ca. 6 % ein, wohingegen das Anfahren und Abfahren anteilig jeweils bei ca. 0,5 % liegt. Die Zustände „Abgefahren“ und „Abgeschaltet“ setzen sich zusammen zu ca. 2 %.

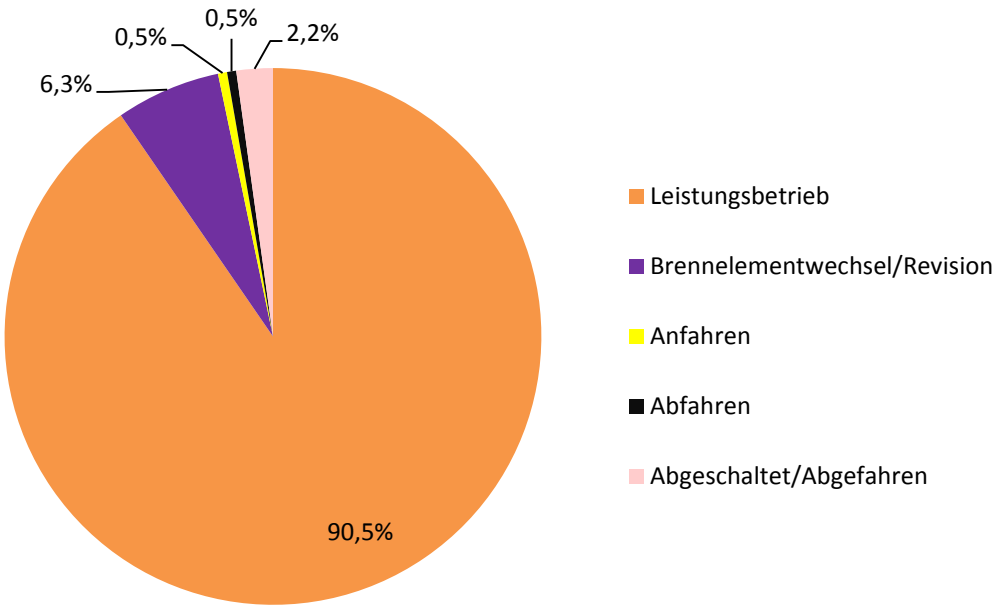

Abb. 5.9 Gemittelte Zeitanteile der verschiedenen Anlagenzustände der Anlage SWR A im Jahr

In Abbildung 5.10 ist der Anlagenzustand zum Zeitpunkt der Ereignisse normiert auf den Zeitanteil des jeweiligen Anlagenzustands am Gesamtjahr dargestellt. Unter der Annahme, dass die Ereignisse in den Anlagenzuständen entsprechend den Zeitanteilen der Anlagenzustände am Gesamtjahr gleichverteilt sind, wird ein Wert von 1 erwartet. Bei Werten von kleiner als 1 sind entsprechend weniger Ereignisse im jeweiligen Anlagenzustand aufgetreten, als unter der oben genannten Annahme erwartet. Dem-

gegenüber zeigen Werte größer 1 eine um den entsprechenden Faktor erhöhte Anzahl an aufgetretenen Ereignissen.

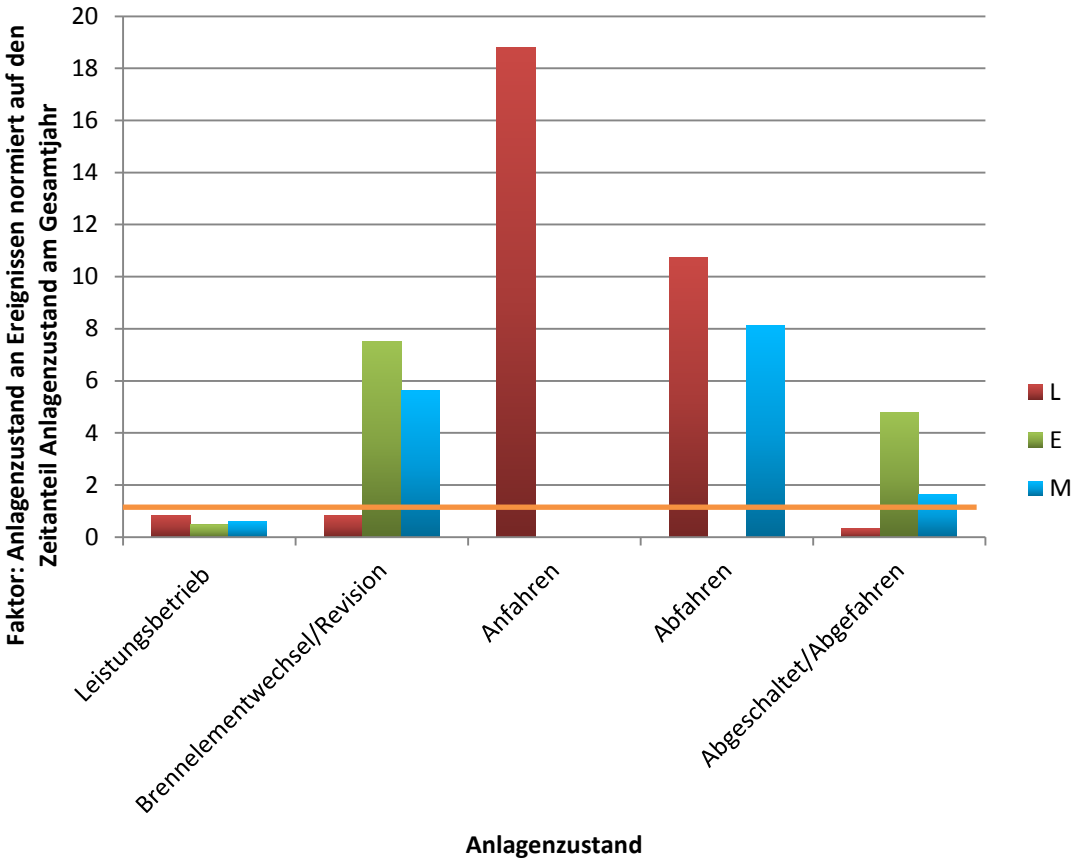

Abb. 5.10 Anlagenzustand zum Zeitpunkt der Ereignisse normiert auf den Zeitanteil des Anlagenzustands am Gesamtjahr in der Anlage SWR A für die Komponenten der Elektro- und Leittechnik sowie für Messumformer

Ein Grund für die Verteilung der Ereignisse liegt in der Betriebsweise der verschiedenen Komponentenarten und der Verteilung der jeweiligen Komponenten-Prüfungen in den verschiedenen Anlagenzuständen. Die meisten wiederkehrenden Prüfungen (WKP) werden beispielsweise bei Brennelementwechsel/Revision durchgeführt.

Des Weiteren ist in Abbildung 5.10 erkennbar, dass der Faktor der Ereignisanzahl für die Leittechnik-Komponenten während des Anfahrens der Anlage am größten ist. Ein möglicher Grund dafür könnte sein, dass in diesem Anlagenzustand auch Ereignisse auftreten können, die ggf. durch Arbeiten im Brennelementwechsel/Revision verursacht worden sind. Beispielsweise könnte ein benachbarter Schrankeinschub bei einem Test versehentlich beschädigt worden sein oder eine Parameterrückstellung nach einem

Test versehentlich fehlerhaft oder nicht durchgeführt worden sein. Genauere Untersuchungen zu den Ereignissen während des Anfahrens haben ergeben, dass diese im hier vorliegenden Fall ausnahmslos aus dem Jahr 2004 stammen und mit einem Generatorschaden korrelieren, der sich auf verschiedene Komponenten ausgewirkt hatte. Es handelt sich somit um einen Einzelfall auf den näher in Abschnitt 5.10 eingegangen wird. Der erhöhte Faktor der Ereignisanzahl für die Leittechnik-Komponenten beim Abfahren kann ebenfalls auf das Ereignis „Generatorschaden“ zurückgeführt werden. Der entsprechende Faktor für die Messumformer kann auf Drift- und Austauschereignisse zurückgeführt werden. Insbesondere wurden programmierbare oder rechnerbasierte Messumformer, die sich als anfällig für Strahlung erwiesen haben, durch analoge, ältere Typen ersetzt (siehe Abschnitt 5.7).

5.7 Umwelteinflüsse

Für diesen Abschnitt wurde für die programmierbaren oder rechnerbasierten Komponenten überprüft, ob die Umweltbedingungen/-einflüsse am jeweiligen Einsatzort negative Auswirkungen auf das Verhalten der Komponente (z. B. Ausfallrate, Ausfallmechanismen,…) haben. Hierzu wurden insbesondere die vorgelegten Fehlerbeschreibungen der Ereignisse analysiert. Dabei wurde u. a. auf solche Hinweise geachtet, die einen Einfluss von Umweltbedingungen wie z. B. Feuchtigkeits-, Hitze- und Strahlungs-Einflüsse aufzeigen.

Aus den vorliegenden Daten geht kein vermehrter Ausfall von leittechnischen Komponenten aufgrund einer erhöhten Strahlenbelastung, Feuchtigkeit oder Hitze hervor. Jedoch gab es einige Ereignisse, die eine unklare Ursache aufweisen bzw. wo keine Ursache gefunden wurde. Für diese kann also nicht gänzlich ausgeschlossen werden, dass es sich hierbei nicht doch um Ausfälle aufgrund einer Strahlenbelastung oder einem anderen Umwelteinfluss handelt. Bei Messumformern traten Ausfälle aufgrund von erhöhter Strahlenbelastung auf, welche im Bericht „Analyse zum Einsatz und Betrieb elektrotechnischer Einrichtungen“ /GRS 15/ genauer analysiert wurden.

5.8 Zeitliche Entwicklung der Fehlererkennung

Bisher bezogen sich alle Auswertungen auf den jeweiligen kompletten Betrachtungszeitraum. Im Folgenden wird untersucht, ob sich hinsichtlich der Erkennungsart der Er-

eignisse im zeitlichen Verlauf Änderungen ergeben haben. Dies könnte unter Umständen einen Rückschluss auf z. B. veränderte Prüfprozeduren geben.

Für die folgende beispielhafte Auswertung werden alle Ereignisdaten (L, E, M) der Jahre 2001 – 2012 (das Jahr 2000 wurde aufgrund der geringen Ereigniszahl nicht berücksichtigt) der Anlage SWR A zusammengefasst und in drei Gruppen in Abhängigkeit des Ereignisjahres unterteilt:

- Gruppe 1: Jahre 2001 – 2004
- Gruppe 2: Jahre 2005 – 2008
- Gruppe 3: Jahre 2009 – 2012

Bei einer derartigen Auswertung ist zu berücksichtigen, dass die gewählte Gruppeneinteilung das Ergebnis beeinflussen kann. Eine grafische Auftragung dieser Einteilung ist in Abbildung 5.11 dargestellt. Die Farben wurden hier so gewählt, dass keine Unstimmigkeiten zu den oben gezeigten Abbildungen auftreten.

Den größten Unterschied zwischen den Jahresgruppen ist bei der Fehlererkennungsart „vorbeugende Instandhaltung“ auszumachen. Hierbei ist die Gruppe 2 (2005 – 2008) besonders auffällig. Der erhöhte Anteil an Ereignissen in diesen Jahren ist auf mehrere Rückrufaktionen durch Hersteller (siehe dazu auch Abschnitt 5.5), welche eine erhöhte Anzahl von Instandhaltungsvorgängen zur Folge hatten, zurückzuführen.

Der erhöhte Anteil von ca. 54 % für Gruppe 3 (2009 – 2012) bei Prüfungen liegt in 85 % der Fälle an Driftereignissen bei Messumformern. Ansonsten finden sich keine Auffälligkeiten bei dieser Fehlererkennungsart.

Die weiteren Zahlen sind im Rahmen der statistischen Genauigkeit nicht auffällig. Dies lässt den Schluss zu, dass es nur geringe bis keine Änderungen bei Prüfprozeduren aufgrund von Ereignissen gegeben hat. Dies wurde auch in Gesprächen mit den Anlagen bestätigt.

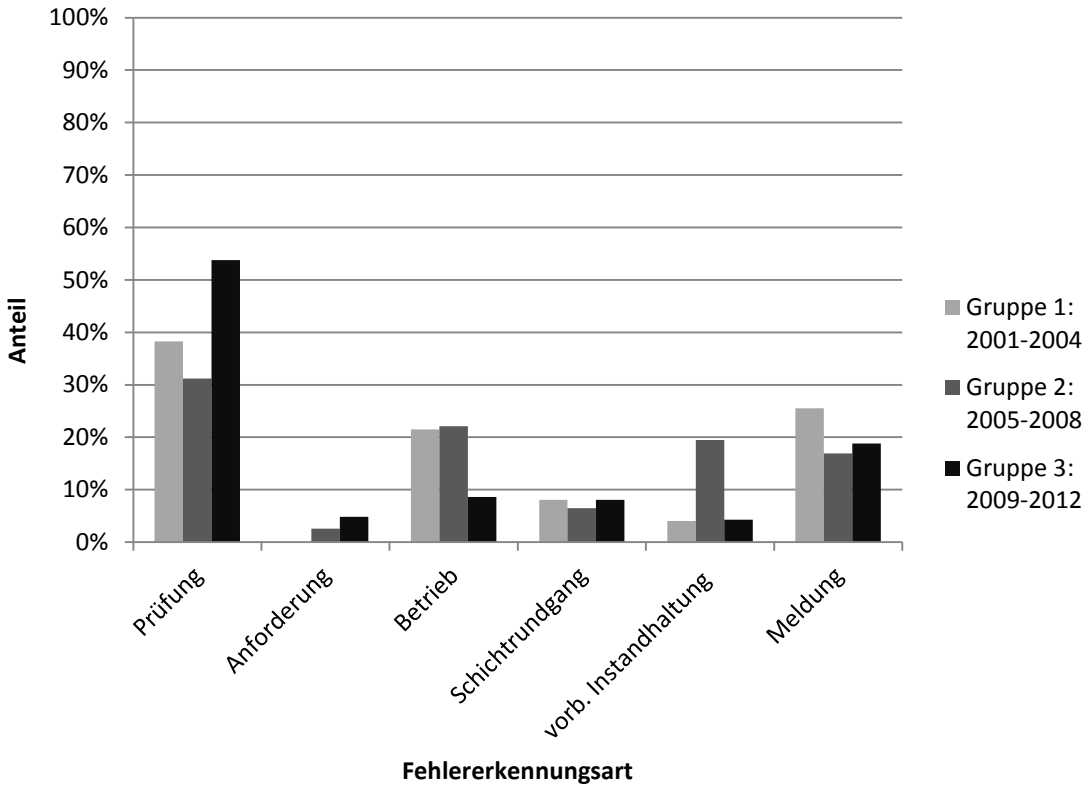

Abb. 5.11 Anteile der verschiedenen Fehlererkennungsarten in der Anlage SWR A bezogen auf die Ereignisjahrgruppe für die Gesamtanzahl der Ereignisse für die Komponenten der Elektro- und Leittechnik sowie für Messumformer

5.9 Mehrfachausfälle

Wie bereits mehrfach erwähnt, wird die Ersatzteilbeschaffung für die in den Anlagen eingebauten Komponenten immer schwieriger, weswegen die Komponenten derzeit bevorzugt repariert werden. In diesem Zusammenhang wird in diesem Abschnitt untersucht, ob einzelne Komponenten vermehrt an Ereignissen beteiligt waren und dadurch vermehrt repariert wurden. Mögliche Mehrfachausfälle könnten ggf. aufgrund von unbekannten Ausfallmechanismen oder Fehlern auftreten und ggf. vorhandene Reparaturmechanismen unwirksam machen (z. B. unbekannte Programmierungsfehler, die nur in ganz bestimmten Betriebszuständen auftreten). Möglich ist diese Untersuchung, am Beispiel der Anlage SWR A, weil dort den einzelnen Komponenten sog. Individuumsnummern bzw. Objektnummern zugeordnet sind. Diese Nummern werden für jede Komponente individuell vergeben, wodurch eine Verfolgung der Komponente über die Zeit und durch die Anlage möglich ist.

In Abbildung 5.12 ist für die einzelnen Komponenten (L, E, M) aus den Ereignissen aufgetragen in wie viele Ereignisse sie jeweils verwickelt waren. Die meisten Individuen treten nur bei einem Ereignis in Erscheinung. Für die Leittechnik-Komponenten bedeutet dies in ca. 93 % der Fälle, für die Elektrotechnik-Komponenten in ca. 80 % der Fälle und für die Messumformer in ca. 73 % der Fälle.

In dem zugrunde gelegten Betrachtungszeitraum sind bei ca. 16 % der Messumformer-Ereignisse und bei ca. 4 % der Leittechnik-Ereignisse zwei Ereignisse pro Individuum aufgetreten, wohingegen bei den Elektrotechnik-Ereignissen gar keine Individuen mit zwei Ereignissen gefunden wurden. 3 Ereignisse pro Individuum können bei ca. 1 % der Leittechnik-Ereignisse, bei ca. 13 % der Elektrotechnik-Ereignisse und bei ca. 8 % der Messumformer-Ereignisse verzeichnet werden. Für eine noch höhere Anzahl von Ereignissen (≥ 4) pro Individuum sind nur vereinzelte Fälle registriert.

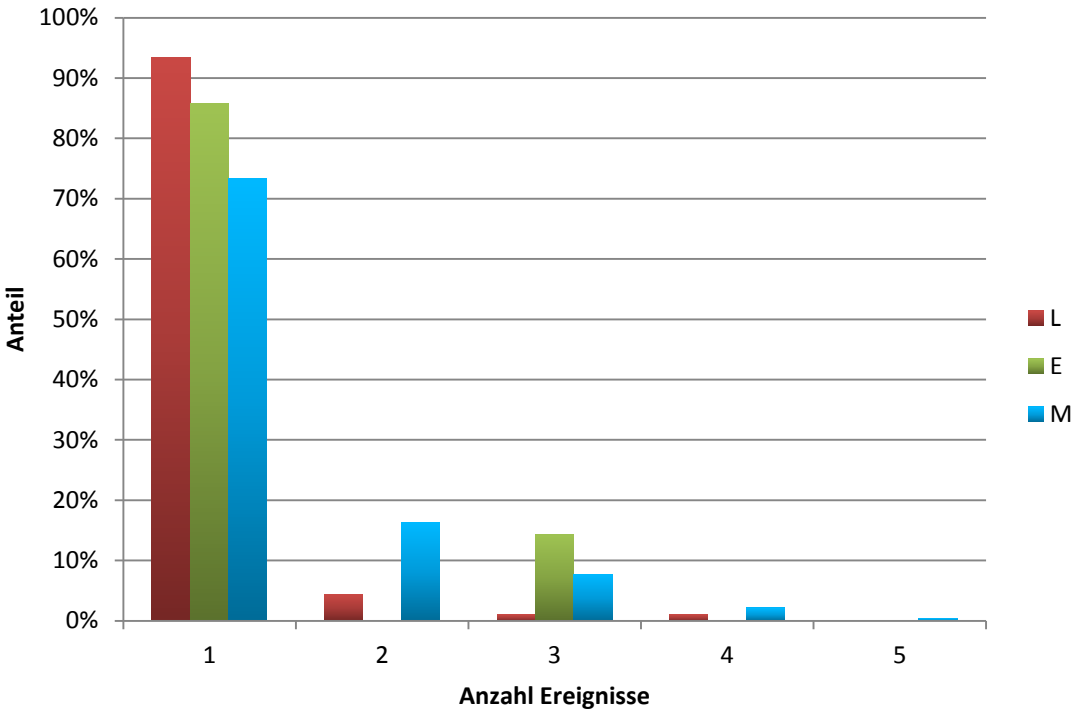

Abb. 5.12 Anteile der einzelnen Individuen hinsichtlich ihrer Anzahl an Ereignissen in der Anlage SWR A für die Komponenten der Elektro- und Leittechnik sowie für Messumformer

Die erhöhten Anteile an mehreren Ereignissen pro Individuum bei den Messumformern lassen sich mit dem bereits angesprochenen „Driften“ erklären. Driften bedeutet in diesem Zusammenhang, dass sich das Signal eines Messumformers mit der Zeit verän-

dert. Diese Veränderung wird hauptsächlich durch den mechanischen (analogen) Teil des Messumformers verursacht. Aufgrund dieser „Driftereignisse“ ist eine große Anzahl der Messumformer-Ereignisse auf die Neueinstellung/Justierung von Messumformern zurückzuführen. Da dieses „Driften“ bekannt ist, war zu erwarten, dass in dem vorliegenden Betrachtungszeitraum die Messumformer häufiger von Driftereignissen betroffen sind. Die erhöhten Anteile an mehreren Ereignissen pro Individuum bei den Leittechnik-Komponenten sind zurückzuführen auf Pufferbatterie-Fälle, welche bereits in Abschnitt 5.2 näher beschrieben wurden. Weitere Mehrfachausfälle beispielsweise aufgrund von Softwarefehlern wurden in den Ereignisdaten nicht gefunden.

Da die Komponenten nicht nur repariert werden, sondern auch ausgetauscht werden ist in Abbildung 5.13 ein Vergleich zwischen der Anzahl der ausgetauschten und der reparierten Komponenten für alle Komponentenarten (L, E, M) dargestellt.

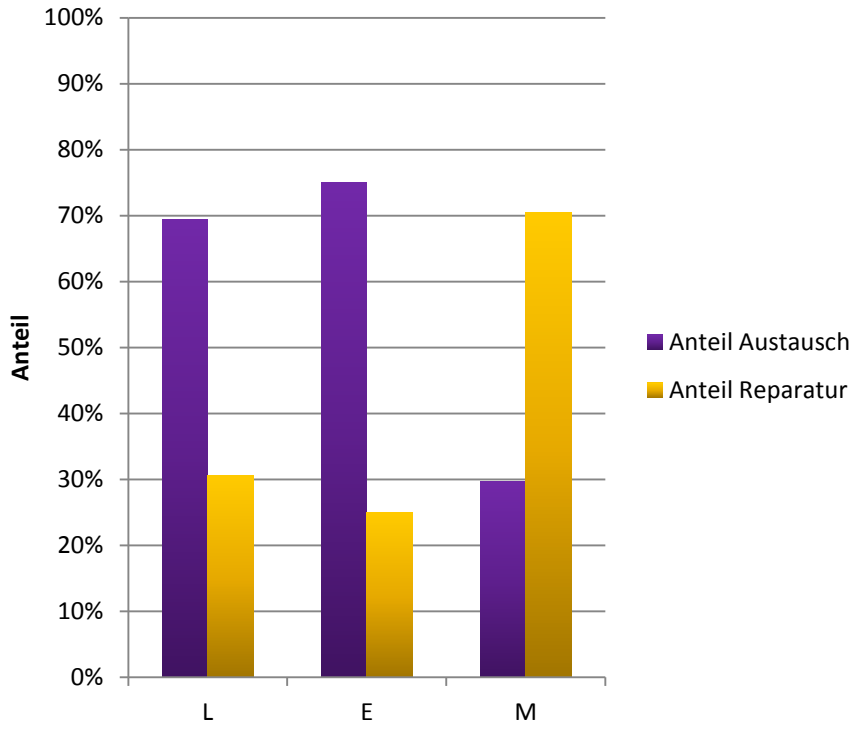

Abb. 5.13 Anteile der Ereignisse bei denen eine Komponente ausgetauscht wurde im Vergleich zum Anteil der Ereignisse, in denen eine Komponente repariert wurde aufgeschlüsselt für die Komponenten der Elektro- und Leittechnik sowie für Messumformer der Anlage SWR A

Bei den Messumformern liegt der Reparaturanteil, u. a. aufgrund der beschrieben Drift, gegenüber dem Austauschanteil mit etwa 70 % erwartungsgemäß hoch. Bei den ande-

ren Komponentenarten (L und E) dominieren die Ereignisse mit Komponentenaustausch.

Es hat sich gezeigt, dass einige Probleme, die bei den Komponenten aufgetreten sind, mit Hilfe eines Firmware-Updates (siehe Abschnitt 5.5) behoben wurden. Da dies auf ein Problem mit der Software hinweist, erschienen diese Fälle besonders interessant für dieses Projekt zu sein. Jedoch gestaltete sich eine Auswertung der vorliegenden Daten hinsichtlich der Ereignisse mit Firmware-Updates schwierig, da solche Ereignisse teilweise als Austausch und teilweise als Reparatur klassifiziert wurden. Darüber hinaus waren genauere Beschreibungen zu den Firmware-Updates nicht verfügbar.

5.10 Generatorschaden

In der Auswertung zum zeitlichen Verlauf der Ereignisse in der Anlage SWR A (Abschnitt 4.1.2) ist eine Häufung von Ereignissen im Jahr 2004 an leittechnischen Komponenten aufgefallen. Diese Häufung ist auf einen Generatorschaden zurückzuführen, auf den im Folgenden genauer eingegangen wird.

In Abbildung 5.14 sind dafür die Leittechnik-Ereignisse pro Leittechnik-Schrank im gesamten Betrachtungszeitraum aufgetragen, um ggf. örtliche Fehlerhäufungen zu analysieren. Dabei sind nur die Schränke berücksichtigt, in denen 4 oder mehr Ereignisse aufgetreten sind. Es zeigen sich zwei Schränke mit einer erhöhten Anzahl von Ereignissen (Schrank 1 mit 22 Ereignissen und Schrank 2 mit 16 Ereignissen).

Nur bei Schrank 1 zeigt sich bei einer genaueren Betrachtung eine zeitliche Korrelation der Ereignisse. Diese ist in Abbildung 5.15 grafisch dargestellt. Diesem Sachverhalt wurde weiter nachgegangen, wobei insbesondere die entsprechenden Systeminformationen und die jeweiligen Ereignisursachen genauer betrachtet wurden.

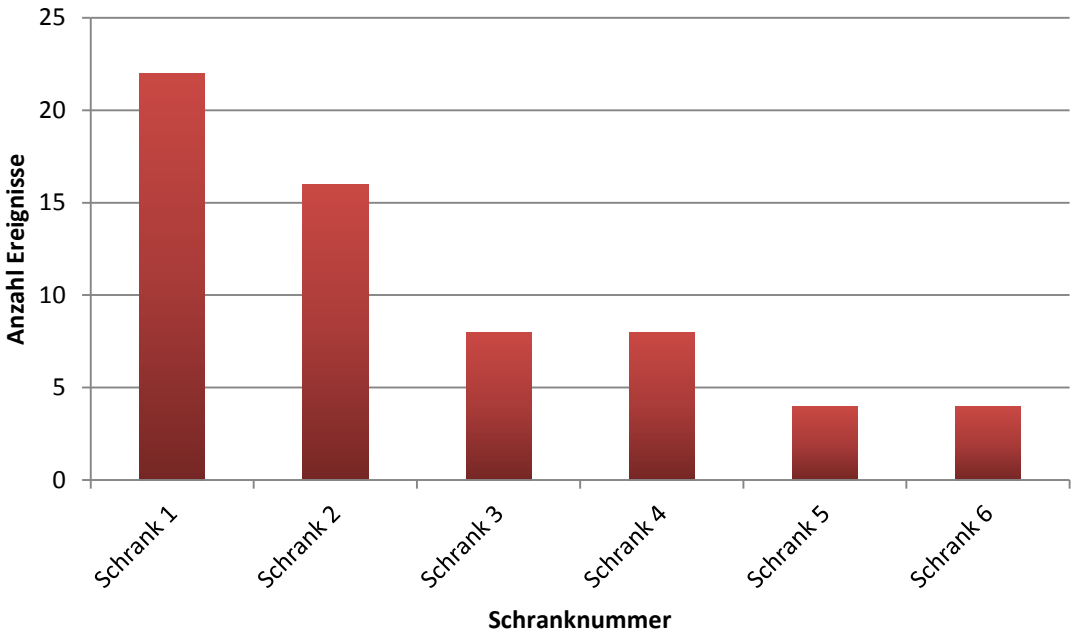

Abb. 5.14 Anzahl der Ereignisse mit Leittechnik-Komponenten der Anlage SWR A pro Leittechnik-Schrank

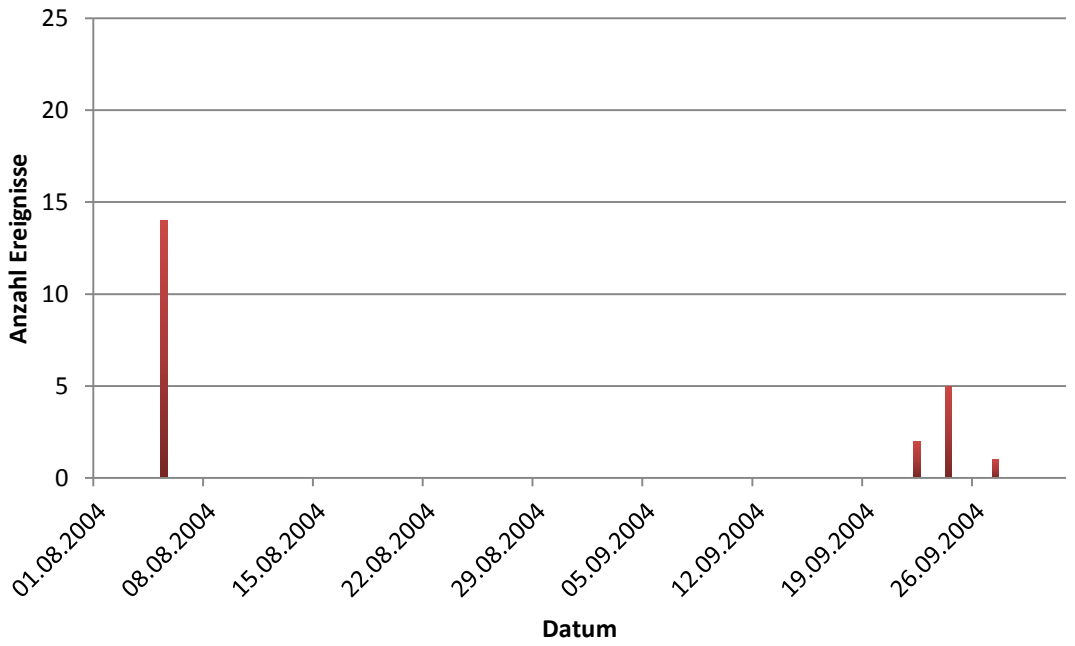

Abb. 5.15 Zeitlicher Verlauf der Leittechnik-Ereignisse in Schrank 1 (siehe Abb. 5.14)

Aus dem Betriebsbericht der Anlage SWR A lässt sich bezüglich der Daten aus Abbildung 5.15 entnehmen, dass sich im Rahmen der Anfahrphase im August 2004 nach 5 Minuten Netzbetrieb ein Kurzschluss im Generator hervorgerufen durch Feuchtigkeit ereignet hat. Dieser Kurzschluss hat dem Generator einen solchen Schaden zugefügt, dass er ausgetauscht werden musste. Nach knapp zwei Monaten kam es beim Wiederanfahren nach dem Generatortausch zu Lagerschwingungen in der Erregermaschine, woraufhin eine Hand-TUSA (Turbinen-Schnell-Abschaltung) durchgeführt wurde und das Wiederanfahren zunächst wieder abgebrochen wurde. Nach Durchführung geeigneter Maßnahmen wurde die Anlage wiederangefahren und der Generator mit dem Netz synchronisiert.

Nach Rücksprache mit der Anlage konnte die Vermutung bestätigt werden, dass die in Schrank 1 aufgetretenen Fälle mit dem Ausfall bzw. Austausch des Generators zusammenhängen. Durch den Kurzschluss im Generator wurden ebenfalls einige Leittechnik-Baugruppen zur Generator-Temperatur-Analyse mitgeschädigt und dann ausgetauscht. Nach dem Austausch des Generators wurden vor dessen Wiederinbetriebnahme die vorgesehenen Isolationsmessungen durchgeführt. Fälschlicherweise waren zu diesem Zeitpunkt bereits Leittechnik-Komponenten gesteckt, die dann durch diese Messungen zerstört wurden.

Die Auswertung macht deutlich, dass die gehäufte Anzahl der Ereignisse im Jahr 2004 in der Anlage SWR A nicht auf einen systematischen Fehler in Bezug auf die Software in den betroffenen programmierbaren oder rechnerbasierten Leittechnik-Komponenten, sondern auf den Kurzschluss im Generator und den Fehler beim Wiederanfahren mit neuem Generator zurückzuführen ist.

6 Zusammenfassung und Fazit

Aufgrund der Tatsache, dass in den deutschen Kernkraftwerken vermehrt programmierbare oder rechnerbasierte Komponenten zum Einsatz kommen, ist es notwendig Erkenntnisse über das Ausfallverhalten und die Ausfallhäufigkeiten dieser Komponenten zu erfassen und zu untersuchen. Ziel des Projektes war es aus solchen Untersuchungen neue Erkenntnisse zu Ausfallmechanismen zu erlangen, wodurch ggf. eine Grundlage für eine zukünftige Bewertung der Zuverlässigkeit solcher Komponenten gegeben werden kann.

Zunächst wurden im Rahmen der Aufbereitung des für dieses Vorhaben relevanten Stands von Wissenschaft und Technik die in nationalen und internationalen Regelwerken enthaltenen Anforderungen an die Auslegung von programmierbaren und rechnerbasierten leittechnischen Systemen zusammengestellt. Des Weiteren wurden Umrüstungsmaßnahmen auf programmierbare oder rechnerbasierte leittechnische Komponenten in deutschen und internationalen Kernkraftwerken beschrieben, wobei neben geplanten und bereits abgeschlossenen Umrüstungsmaßnahmen auch auf Neubauprojekte von Kernkraftwerken mit programmierbaren oder rechnerbasierten leittechnischen Komponenten eingegangen wurde. Die dabei eingesetzten programmierbaren oder rechnerbasierten Leittechniksysteme wurden ebenfalls näher beschrieben.

Für die Untersuchungen zu Ausfallmechanismen von programmierbaren oder rechnerbasierten Komponenten wurden für dieses Projekt umfangreiche Daten zu Ereignissen unterhalb der Meldeschwelle gesammelt und hinsichtlich verschiedener Fragestellungen ausgewertet. Diese Daten wurden von sechs kerntechnischen Anlagen zur Verfügung gestellt. Fragen, die sich aus den Auswertungen ergeben haben und durch die erfassten Daten nicht beantwortet werden konnten, wurden durch Vertreter der Anlagen in Gesprächen mit der GRS diskutiert. Falls notwendig wurden weitere Informationen zur Verfügung gestellt. Die im Rahmen dieser Arbeiten übermittelten Daten zu den programmierbaren oder rechnerbasierten Komponenten und den entsprechenden Ereignissen variieren in ihrer Anzahl und ihrem Detailierungsgrad zwischen den betrachteten Anlagen, weswegen die Ergebnisse nicht mit einander verglichen werden konnten. Neben den Diskussionen mit den Anlagen wurden die verschiedenen Komponentenhersteller kontaktiert und um weitere Informationen zu den Komponenten gebeten.

In dem vorliegenden Bericht werden insbesondere die Auswertungen für die programmierbaren oder rechnerbasierten leittechnischen Komponenten vorgestellt. Die entsprechenden Auswertungen für elektrotechnischen Komponenten und Messumformer sind im Bericht „Analyse zum Einsatz und Betrieb elektrotechnischer Einrichtungen“ /GRS 15/ zu finden.

Die Auswertungen haben gezeigt, dass zwar bereits einige leittechnische Komponenten durch programmierbare oder rechnerbasierte Modelle ersetzt wurden, ein großer Teil der Anlagentechnik aber noch mit herkömmlichen, konventionellen Komponenten betrieben wird.

Da in diesem Projekt hauptsächlich Ereignisse unterhalb der Meldeschwelle betrachtet wurden, sind zu den jeweiligen Fehlerursachen nur weniger detaillierte Informationen verfügbar, als dies bei den meldepflichtigen Ereignissen der Fall ist. Dies liegt daran, dass bei betrieblichen Komponenten in den meisten Fällen das Interesse der Anlagen nicht in der Fehlersuche liegt, sondern im Betrieb der Komponente, d. h. ist der Fehler beispielsweise durch einen Austausch behoben worden, wird meistens nicht nach der Ursache gesucht.

Im Allgemeinen kann zusammengefasst werden, dass die durchgeführten Auswertungen der erfassten Ereignisse kaum Auffälligkeiten hinsichtlich einer Problematik in Bezug auf die Softwareanteile oder die Programmierbarkeit gezeigt haben. Dennoch konnten neue Ausfallmechanismen und Fehlerursachen für programmierbare oder rechnerbasierte Komponenten identifiziert werden. Hier zu nennen wäre die nicht zu vernachlässigende Anzahl an Komponentenausfällen aufgrund von Programmierungsfehlern. Typischerweise wurden in diesen Fällen Firmware-Updates der Hersteller eingespielt, wonach die jeweiligen Fehler behoben waren. Die genauen Ursachen dieser Fehler konnte im Rahmen dieses Projektes jedoch nicht verifiziert werden. Zusätzlich dazu kam es in mehreren Fällen zu Softwareausfällen aufgrund von ausgefallenen/defekten Pufferbatterien.

Aufgrund der Auswertungen und Diskussionen kann aber auch positiv vermerkt werden, dass sich verschiedene Prüfprozeduren und Abläufe durch den Einsatz der programmierbaren oder rechnerbasierten Technik vereinfacht haben.

Abschließend kann aus den Ergebnissen der im Rahmen dieses Projektes durchgeführten Auswertungen folgendes Fazit gezogen werden:

1. Bei den vorliegenden Daten wurde keine besondere Häufung von Ausfällen von programmierbaren oder rechnerbasierten Komponenten entdeckt.

2. Einige Prüfprozeduren vereinfachen sich (z. B. entfallen komplexe Prüfvorgänge aller möglichen Schalterstellungen einer analogen Schaltung bei Einsatz eines Mikroprozessors, da dieser entweder funktioniert oder nicht), andere hingegen werden komplizierter (z. B. durch die vielzähligen Einstellungsmöglichkeiten programmierbarer oder rechnerbasierter Komponenten, wobei viele dieser Möglichkeiten sogar überflüssig für die in der Anlage konkret genutzte Funktion sind).

3. Einige der herkömmlichen Ausfallmechanismen und Fehlerursachen entfallen durch die programmierbare oder rechnerbasierte Technik, neue kommen jedoch hinzu.

4. Programmierungsfehler treten selten in Erscheinung, aber sie werden beobachtet.

5. Firmware-Updates werden von den Herstellerfirmen geliefert. Die Anlagen können beim Aufspielen der Updates durch Abgleichen der Versionsnummer die Firmware unterscheiden. Über den Inhalt der Updates, d. h. welche Fehler durch diese behoben werden, liegen den Anlagen üblicherweise keine Informationen vor.

Im Rahmen dieses Berichtes als auch im Rahmen des Berichtes „Analyse zum Einsatz und Betrieb elektrotechnischer Einrichtungen“ /GRS 15/ haben sich folgende offene Fragestellungen ergeben, die im Rahmen dieser Projekte nicht abschließend geklärt werden konnten:

- Einfluss von Strahlung auf programmierbare oder rechnerbasierte Speicherbausteine

  Einige der programmierbaren oder rechnerbasierten Komponenten werden in Bereichen erhöhter Strahlung eingesetzt. Es wäre wünschenswert, genau zu analysieren, ob erhöhte Strahlung zu neuartigen Ausfällen in der Elektronik führen kann. Halbleiterbausteine sind bekanntlich anfälliger gegenüber erhöhter Strahlung. Darüber hinaus ist es vorstellbar, dass es zu Speicheränderungen bei elektronischen Speicherchips (z. B. EPROM oder EEPROM) durch erhöhte Strahlung kommen kann /IGN 06/. Was dies im Einzelnen für programmierbare oder rechnerbasierte Komponenten bedeutet, ist unklar.

- Vorgänge bei Firmware-Updates in den Anlagen und beim Hersteller

  Durch die von extern gelieferten Firmware-Updates und deren Einspielung in grö-

ßerem Umfang ist ein Potential bezüglich gemeinsam verursachter Ausfälle und dem Einbringen von Schadsoftware gegeben. Hier wäre es wünschenswert, die Prozesse bei den verschiedenen Herstellern und beim Aufspielen neuer Software in den Anlagen zu untersuchen, um festzustellen, wie groß dieses Potential ist und welche Verbesserungen ggf. umzusetzen wären.

A Anhang: Auswertungstabelle

Im Folgenden wird die Auswertungstabelle am Beispiel der Anlage SWR A vorgestellt. Zur besseren Übersichtlichkeit wird ein Auszug aus dieser Tabelle aufgeteilt über die nächsten 6 Seiten (Abbildung A.1 bis Abbildung A.6) dargestellt. Die Tabelle beginnt mit den Ereignisdaten und danach folgen die Anlagendaten. Dabei beziehen sich die rot beschrifteten Spalten auf die ausgefallene Komponente (gekennzeichnet mit A_) und die blau beschrifteten Spalten auf die neu eingebaute Komponente (gekennzeichnet mit N_). Wurde die Komponente in dem jeweiligen Ereignis repariert sollten die Einträge der alten und der neuen Komponente identisch sein. Eine Erklärung der einzelnen Attribute (Spaltenüberschriften) ist in Tabelle 3.1 in Abschnitt 3.2 zu finden.

EREIGNISDATEN							
AEL_NR	AKZ	EBP	EIN_DAT	AUSF_ART	AUSF_ARTK	VANLZUST	VANLZUSTK
B0011/2006		+00HD03C 007 -A12	17.01.2006	AA	Ausfall aktiv (selbstmeldend. z.B. Störmeldung)	LB	Leistungsbetrieb
B0448/2007		+00HD04A 005 -A04	2007-10-23	AA	Ausfall aktiv (selbstmeldend. z.B. Störmeldung)	LB	Leistungsbetrieb
B0043/2012	=20VC12L 001 -B01		02.03.2012	KA	Kein Ausfall	LB	Leistungsbetrieb
B0505/2012	=20UB92L 001 -B01		16.07.2012	AV	Ausfall mit voller Ausgangsspannur	LB	Leistungsbetrieb
B0373/2000	=20XM12L 004 -A01	+20NB05A 008 -A01	31.12.2000			AB	Abfahren

Abb. A.1 Auszug aus der Auswertungstabelle für die Anlage SWR A (1 von 6)

VAUSF_ERK	VAUSF_ERKK	VAUSF_ERK_SONST	VAUSF_ERK_TEXT	VFEHLBES	VFEHLBESK	REPA_ART	REPA_ARTK	REPAA_DAT
F	Meldung, Anzeige			DA	Fehler dauernd	E	Sonstiges (Im Klartext erläutern)	20060117
F	Meldung, Anzeige			DA	Fehler dauernd	E	Sonstiges (Im Klartext erläutern)	20071023
F	Meldung, Anzeige			ZW	Fehler zeitweise	F	vorbeugende Instandhaltung (evtl. vorbeugende Reparatur)	20120227
F	Meldung, Anzeige			DA	Fehler dauernd	A	Austausch des ausgefallenen Betriebsmittels / Bauteils	20120716
L	WKP			DA	Fehler dauernd	B	Neueinstellung des ausgefallenen Betriebsmittels/Bauteils	20000322

Abb. A.2 Auszug aus der Auswertungstabelle für die Anlage SWR A (2 von 6)

REPAA_UHR	REPAE_DAT	REPAE_UHR	VAUSF_DAT	VAUSF_UHR	AEL_KURZ	AEL_ERROR	AEL_FEHLER
09:00	20060117	09:45	20060117	07:15	Baugruppe CMC60-2 gewechselt	CMC60-2 setzt Störmeldung ab - Baugruppe nicht ansprechbar;	Fehlerbild: Störlampe "rot": Dauerlicht, Betriebslampe "grün": dunkel; Die Baugruppe ist mit dem Melody-Analyser nicht mehr ansprechbar. Die redundante Baugruppe hat die Funktionen übernommen.
14:00	20071023	15:00	20071023	08:30	Baugruppe CMC60-2 gewechselt	CMC60-2 setzt Störmeldung ab - Baugruppe nicht ansprechbar	Fehlerbild: Störlampe "rot": Dauerlicht, Betriebslampe "grün": dunkel; Die Baugruppe ist mit dem Melody-Analyser nicht mehr ansprechbar. Die redundante Baugruppe hat die Funktionen übernommen. Baugruppe war schon einmal mit dem selben Fehler zur Reparatur.
14:00	20120228	15:30	20120224	09:56	IEM1 Brunnensonde nach oben ausgefallen	ASL800 ca. 5 Stunden nach oben ausgefallen/gestört	
09:30	20120716	13:00	20120706	09:36	IEM-Füllstandsmessung instandsetzen	Messung nach oben ausgefallen	
16:00	20000322	16:00	20000322	09:00	FMC67/Z E&H MU eingestellt, Grenzwert nicht angesprochen.		Grenzwert bei unterem Schaltpunkt nicht rückgeschaltet.

Abb. A.3 Auszug aus der Auswertungstabelle für die Anlage SWR A (3 von 6)

AEL_ARBEIT	VFEHLART	VFEHLARTK	ABLAUF_W
Fehlerbild: Störlampe "rot": Dauerlicht, Betriebslampe "grün": dunkel; Die Baugruppe ist mit dem Melody-Analyser nicht mehr ansprechbar. Die Redundante Baugruppe hat die Funktionen übernommen. Vorübergehend wurde die Baugruppe mit der Individium Nr. 5350 eingebaut (Herstellertyp und Sachnummer sind identisch). Die ausgebaute, defekte Baugruppe CMC6-2 mit der Ind. Nr. 5345 wird nach externer Reparatur wieder an diesem Einbauort eingebaut. Reparaturbericht ABB: Nicht lokalisierbarer Fehler auf der CPU-Karte, Leiterplatte muss ersetzt werden, Instandsetzung und Prüfung Am 14.03.2006 wurde die Baugruppe CMC60-2 mit der Ind. Nr. 5345 nach externer Reparatur wieder an diesem Einbauort eingebaut.	SAM	selbstmeldend mit Signaländerung Meldeteil	R
Fehlerbild: Störlampe "rot": Dauerlicht, Betriebslampe "grün": dunkel; Die Baugruppe ist mit dem Melody-Analyser nicht mehr ansprechbar. Die Redundante Baugruppe hat die Funktionen übernommen. Vorübergehend wurde die Baugruppe mit der Individium Nr. 5667 eingebaut (Herstellertyp und Sachnummer sind identisch). Die ausgebaute, defekte Baugruppe CMC6-2 mit der Ind. Nr. 5343 wird nach externer Reparatur wieder an diesem Einbauort eingebaut. Die Baugruppe CMC60-2 mit der Serien-Nr. 5343 war im Oktober 2006 wegen dem gleichen Fehler bei Fa. ABB zur Reparatur und wurde am 24.10.2006 nach erfolgter Reparatur wieder am selben Einbauort eingebaut. Die CMC60-2 soll auf Gewährleistung repariert werden. Leiterplatte defekt. FNET-Karte defekt, muss erneuert werden. Auf den neuen FNET-Karten wurde das Layout und die Bestückung geändert. Eine Mischung der Netzkarten CNET/FNET alter und neuer Hardwarestand ist nicht zulässig. Somit muss auch die CNET-Karte erneuert werden. Der Hardwarestand der kompletten CMC60-2 ändert sich auf HW 04.21. Prüfung der kompletten Baugruppe erforderlich. Die Baugruppe CMC60-2 mit der Ind.Nr. 5343 wurde am 20.03.2008 nach externer Reparatur wieder rückgebaut. Die Baugruppe arbeitete wieder fehlerfrei.	SAM	selbstmeldend mit Signaländerung Meldeteil	R
Messkreis laut MKP überprüft. Alle Werte innerhalb der Toleranz. Kein Fehler feststellbar. Messung vom 25.02.12 bis 01.03.12 nicht mehr ausgefallen ---> Sonde wurde nicht ausgetauscht.	SAF	selbstmeldend mit Signaländerung Funktionsteil	A
Füllstandssonde H&B gegen VEGAWELL 52 getauscht.	NPF	nicht selbstmeldend ohne Signaländerung Funktionsteil	V
MU neu eingestellt, Sonde abgeglichen (Kennlinie neu aufgenommen).	NAF	nicht selbstmeldend mit Signaländerung Funktionsteil	R

Abb. A.4 Auszug aus der Auswertungstabelle für die Anlage SWR A (4 von 6)

Anlagendaten alte (ausgefallene) Komponente									
A_BFS	A_AKZ	A_RAUM	A_HERSTELLER	A_HTA	A_BAUART	A_IND_NR	A_OBJEKT_NR	A_BAUJAHR	A_PLANERTYP
KGG-AH 00240*0174	+00HD03C 007 -A12	0G02.05	HARTMANN & BRAUN	CMC60-2/72262-5-9280162	MULTIFUNKTIONSBAUGRUPPE PROFIBUS	5345	1546917		
KGG-AH 00240*0174	+00HD04A 005 -A04	0G02.05	HARTMANN & BRAUN	CMC60-2/72262-5-9280162	MULTIFUNKTIONS-BAUGRUPPE PROFIBUS	5343	1551285		
KGG-BP 00240*0380	=20VC12L 001 -B01	2P01.42	HARTMANN & BRAUN	15933-2-0014	ASL 800	15933-540473	1066305		T47A
KGG-BP 00240*0381	=20UB92L 001 -B01	2F02.41	HARTMANN & BRAUN	15933-2-0018	ASL 800	15933-T-422709			
KGG-AX 00176*0002	+20NB05A 008	2F09.18	ENDRESS & HAUSER MESSTECHN.	FMC671Z	FUELLSTANDS-MESSGEREAT, MIKROPROZESS-GESTEUERT	V850186-EP6	1300802		T436

Abb. A.5 Auszug aus der Auswertungstabelle für die Anlage SWR A (5 von 6)

Anlagendaten neue (reparierte/neu eingebaute) Komponente									
N_BFS	N_AKZ	N_RAUM	N_HERSTELLER	N_HTA	N_BAUART	N_IND_NR	N_OBJEKT_NR	N_BAUJAHR	N_PLANERTYP
KGG-AH 00240*0174	+00HD03C 007 -A12	0G02.05	HARTMANN & BRAUN	CMC60-2/72262-5-9280162	MULTIFUNKTIONSBAUGRUPPE PROFIBUS	5345	1546917		
KGG-AH 00240*0174	+00HD04A 005 -A04	0G02.05	HARTMANN & BRAUN	CMC60-2/72262-5-9280162	MULTIFUNKTIONS-BAUGRUPPE PROFIBUS	5343	1551285		
KGG-BP 00240*0380	=20VC12L 001 -B01	2P01.42	HARTMANN & BRAUN	15933-2-0014	ASL 800	15933-540473	1066305		T47A
KGG-BP 01299*0005	=20UB92L 001 -B01	2F02.41	VEGA GRIESHABER KG	WELL52.XXX4ALD1CD2X	HÄNGEDRUCK-MESSUMFORMER		1663418		
KGG-AX 00176*0002	+20NB05A 008	2F09.18	ENDRESS & HAUSER MESSTECHN.	FMC671Z	FUELLSTANDS-MESSGEREAT, MIKROPROZESS-GESTEUERT	V850186-EP6	1300802		T436

Abb. A.6 Auszug aus der Auswertungstabelle für die Anlage SWR A (6 von 6)

B Anhang: Ausfallarten

Die vorliegenden Ereignisse von der Anlage SWR A wurden auch hinsichtlich der aufgetretenen Ausfallart der jeweiligen Komponente untersucht. Hierbei wurde die Ausfallart insbesondere in aktive und passive Ausfälle unterteilt. Der Unterschied zwischen diesen beiden Ausfallarten soll Abbildung B.1 verdeutlichen.

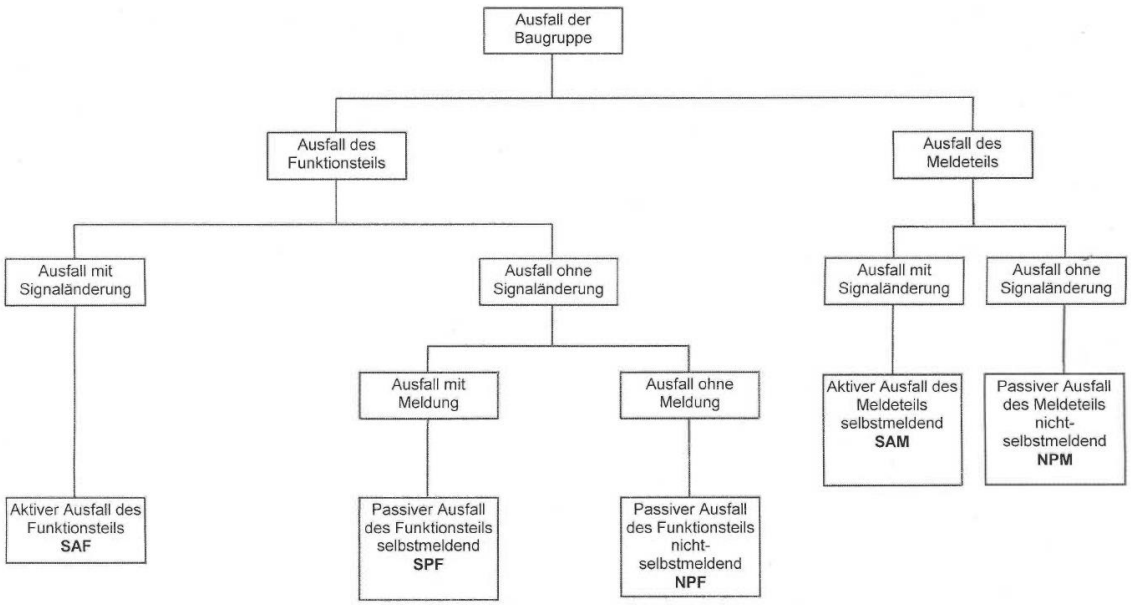

Abb. B.1 Einsortierung der Ausfallart für die Anlage SWR A

Die Abkürzungen, die in Abbildung B.1 genutzt werden, lauten wie folgt:

- Für den Funktionsteil gilt:
  - „SAF" = selbstmeldend, mit Signaländerung (aktiver Ausfall)
  - „SPF" = selbstmeldend, ohne Signaländerung (passiver Ausfall)
  - „NPF" = nicht selbstmeldend, ohne Signaländerung (passiver Ausfall)
- Für den Meldeteil gilt:
  - „SAM" = selbstmeldend, mit Signaländerung (aktiver Ausfall)
  - „NPM" = nicht selbstmeldend, ohne Signaländerung (passiver Ausfall)

Die Angabe der Signaländerung bezieht sich auf das Verhalten der Signalgröße im gestörten Funktions- oder Meldeteil der Komponente. Verursacht die Störung einen Sig-

nalzustandswechsel am Funktionsteilausgang gegenüber dem ungestörten Normalzustand, so liegt eine Signaländerung vor. Das gleiche gilt auch für dynamische Systeme, wie z. B. dem EDM-System, welche einen Taktausfall oder eine unzulässige Taktänderung als Anregebedingung erkennen. Ein veränderter Takt entspricht somit ebenfalls einer Signaländerung.

Das Meldeverhalten bezieht sich auf die Randbedingungen der Störungserkennung. Würde sich z. B. die Störung nur in Form einer lokalen Anzeige auf dem Gerät zeigen und diese Örtlichkeit nicht mit dem Ziel einer Störungserkennung regelmäßig begangen, so handelt es sich um eine nicht selbstmeldende Störung.

Im Gegensatz dazu sind die gezielte und wahrnehmbare Anregung einer Sammelmeldung und die damit initiierte Störungssuche als selbstmeldend zu bewerten.

Unter dem Funktionsteil sind die für die Aufgabenstellung der Komponente benötigten Einrichtungen zu verstehen. So gehört z. B. ein Einstellpotentiometer oder eine UND-Funktion, eine Verwendung in der Anlage vorausgesetzt, zu dem Funktionsanteil.

Unter Meldeteil werden die Komponenteneinrichtungen verstanden, die ausschließlich nur für die Generierung, Verknüpfung, Ausgabe und Anzeige von Meldungen dienen. Ein Defekt innerhalb der vorgenannten Geräteanteile wirkt sich somit nicht auf den Funktionsteil der Komponente aus.

Referenzen

/ABB 03/ Industrial Prozessleitsystem Melody, Übersicht; ABB; 2003

/ANP 02/ Advanced Nuclear Power, Framatome NP, Nr.5, September 2002

/ANP 03/ Advanced Nuclear Power, Framatome NP, “Moderne Elektro- und Leittechnik”, Nr.8, August 2003

/ARE/ Areva NP, Instrumentation and Control, TELEPERM XS

/ARE 06/ TELEPERM XS Systemübersicht; Areva NP GmbH; 2006

/ARE 10/ Ringhals 1: Improvement of the Reactor Protective System, Areva News Brief, Juli 2010

/AUT 10/ Development of the Ringhals 1 PSA with regard to the Implementation of a Digital Reactor Protection System, Stefan Authén, Erik Wallgren, Stefan Eriksson, Proceedings of the 10th International Probabilistic Safety Assessment & Management Conference (PSAM 10), Juni 2010

/ATW 10/ Kernkraftwerke in Deutschland Betriebsergebnisse 2010, atw International Journal of Nuclear Power, 2010

/BEN 03/ G. Bender (Framatome ANP), Linnenfelser (EnBW, KKP), „Erfahrungen mit der Inbetriebsetzung des Systems zur lokalen Kernüberwachung (LKU-System) im Kernkraftwerk Philippsburg 1“, Fachtagung der KTG-Fachgruppen „Betrieb“ und „Reaktorphysik und Berechnungsmethoden“, 13.–14. Februar 2003

/BFS 03/ Bundesamt für Strahlenschutz, Fachbereich Sicherheit in der Kerntechnik, Qualifizierungs- und Genehmigungsanforderungen zum Einsatz rechnergestützer Sicherheitsleittechik in kerntechnischen Anlagen – Statusbericht, F. Seidel, 2003

/BMU 12/ Sicherheitsanforderungen an Kernkraftwerke, Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit, November 2012

/BMU 13/ Interpretationen zu den Sicherheitsanforderungen an Kernkraftwerke, Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit, November 2013

/DIN 10/ DIN EN 61226, Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Kategorisierung leittechnischer Funktionen – August 2010

/DUK 08/ Duke Energy: License Amendment Request for Reactor Protective System/Engineered Safeguards Protective System Digital Upgrade, Technical Specification Change Number 2007-09, January 31, 2008

/EDF 10/ EDF press release, Progress Update on the Flamanville 3 EPR project, Juli 2010

/ELS 02/ O. Elsensohn, F. Fradet, J.C. Péron, B. Soubiès, „ FRENCH EXPERIENCE ON RENEWING I&C SYSTEMS IN NPP'S – Feedback from assessing nuclear instrumentation system (RPN) refurbishment at French CP0-series plants“, Eurosafe 2002

/EME/ Ovation Expert System Systembeschreibung; EMERSON

/ENR 10/ Licensing of safety critical software for nuclear regulators, Common position of seven European nuclear regulators and authorised technical support organisations, Revision 2010, BEL V (Belgium), BfS (Germany), CSN (Spain), ISTec (Germany), NII (United Kingdom), SSM (Sweden), STUK (Finland), 2010

/EON 09/ Kernkraftwerk Grafenrheinfeld zum 28. Brennelementwechsel, Pressemitteilung e.on, 05.03.2010

/GAS 10/ Assessment of the overall Instrumentration & Control architecture of the EPR FA3 project, Jean Gassino, Pascal Régnier, Institut de Radioprotection et de Sûreté Nucléaire, Eurosafe 2010

/GKN 00/ EnBW Kernkraft GmbH Kernkraftwerk Neckarwestheim – GKN, Revisionsbericht Block 1, 2000

/GKN 03/ GKN II, Betriebsbericht zur Information der Reaktor-Sicherheitskommission 2003

/GKN 05/ EnBW Kernkraft GmbH Kernkraftwerk Neckarwestheim – GKN, Revisionsbericht Block 1, 2005

/GKN 07/ EnBW Kernkraft GmbH Kernkraftwerk Neckarwestheim, GKN I – Revisionsbericht, 2007

/GKN 12/ EnBW Kernkraft GmbH Kernkraftwerk Neckarwestheim, GKN II – Revisionsbericht, 2012

/GKN 99/ GKN I, Betriebsbericht zur Information der Reaktor-Sicherheitskommission 1999

/GÖS 14/ Pressemitteilung des Kernkraftwerks Gösgen zur Jahresrevision, 6. Juni 2014

/GRS 15/ Sicherheitstechnische Analyse zum Einsatz und Betrieb elektrotechnischer Einrichtungen in deutschen Kernkraftwerken, Überwachung und Schutz gegen sicherheitstechnisch bedeutsame Einwirkungen aus dem Verbundnetz sowie anderen äußeren Quellen (3610R01363), ISBN 978-3-944161-37-2, GRS-356, 2015

/HAG 10/ Sicherheitsleittechnik – Aspekte bei Erneuerungsprojekten aus Sicht einer Genehmigungs- und Aufsichtsbehörde, M. Hagmann, Ministerium für Umwelt, Naturschutz und Verkehr Baden-Württemberg, 2.Symposium Digitale Sicherheitsleittechnik, September 2010

/HAN 05/ Ersatz des Reaktorschutz- und Regelsystems im Kernkraftwerk Beznau, Ch. Hangartner, atw 50. Jg. (2005) Heft 2 – Februar 2005

/HIM/ HIMax Produktkatalog; HIMA

/HIM 10/ HIMax Broschüre; HIMA; 2010

/HIM 12/ HIMA, HIMax news, HIMax Evolution Package II, 2012

/HOF 10/ A. Hofmann, ABB Referenzen Kerntechnik – Überblick, 7.12.2010

/HSE 11/ ONR-GDA-AR-11-022, Generic Design Assessment – New Civil Reactor Build, Step 4, Control and Instrumentation Assessment of the EDF and AREVA UK EPR™ Reactor, Revision 0, Office for Nuclear Regulation (An agency of HSE), November 2011

/HSK/ Aufsichtsverfahren beim Ersatz des Reaktorschutz- und Regelsystems im KKW Beznau 1 (Projekt PRESSURE), U. Meyer, U. Feer, M. Sutovsky, A. Voumard, H. Wand, Hauptabteilung für die Sicherheit der Kernanlagen (HSK)

/HUR 07/ Tim Hurst, Tow nuclear power I&C out of the „digital ditch“, Hurst Technologies Corp. , Januar 2007

/IAE 02/ IAEA safety guide NS-G-1.3, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, IAEA, März 2002

/IAE 05/ IAEA-TCM on Nuclear Power Plant Control and Instrumentation Programmes (TWG – NPPCI), Overview of I&C Activities in Sweden, M. Hansson, O. Andersson, Mai 2005

/IAE 08/ Instrumentation and Control (I&C) Systems in Nuclear Power Plants: A Time of Transition? NTR2008-Supplement, IAEA General Conference 52th Annual Regular Session, 2008

/IAE 09/ IAEA nuclear energy series NP-T-1.5, “Protection against Common Cause Failures in Digital I&C Systems of Nuclear Power Plants“, IAEA, November 2009

/IGN 06/ N. Ignat, B. Nicolescu, Y. Savaria, G. Nicolescu, Soft-Error Classification and Impact Analysis on Real-Time Operating Systems, EDAA 2006

/JAI 09/ JAIF, Mio Kimuro, Atoms in Japan, Shikoku Electric Shifts to Comprehensive Digital I&C System at Ikata-1 and -2, März 2009

/KBR 03/ Kernkraftwerk Brokdorf, RSK-Jahresbericht 2003

/KBR 08/ Kernkraftwerk Brokdorf, RSK-Jahresbericht 2008

/KBR 09/ Kernkraftwerk Brokdorf, RSK-Jahresbericht 2009

/KIN/ Regulatory Approach for Defense-in-Depth and Diversity of Digital I&C Systems in Nuclear Power Plants, Korea Institute of Nuclear Safety (KINS)

/KKE 09/ KKE ZA, Sicherheitsüberprüfung 2009 für das Kernkraftwerk Emsland Sicherheitstechnisch bedeutsame Nachrüstungen und maßgebliche Änderungen der Anlage seit der letzten Sicherheitsüberprüfung 1999-2008, Rev. a Juni 2012

/KKI 09/ E.On Kernkraft, Kernkraftwerk Isar 2, Sicherheitsüberprüfung 2009, Probabilistische Sicherheitsanalyse, Revision B

/KKK/ KKK, Betriebshandbuch, Teil 4

/KKU 98/ Kernkraftwerk Unterweser, zur Information der Reaktor-Sicherheitskommission 1998

/KON 10/ A PSA Model developed for the Digital Reactor Protection System of the Latest PWR in Japan, Keisuke Kondo, Haruo Fujimoto, Masahiro Yamashita, Proceedings of the 10th International Probabilistic Safety Assessment & Management Conference (PSAM 10), Juni 2010

/KRB 12/ KGG, Gundremmingen Block B/C, Betriebshandbuch, Teil 4

/KUK 09/ Application of Digital I&C Technology Overview and Outlook, Implementation at Japanese NPPs, Yutaka Kukita, Third Quadripartite Working Group Meeting on DIC, Oktober 2009

/KUN 06/ Construction and operation experience of digitalized safety systems of Japaneses ABWR, Susumo Kunito, TEPCO, Juni 2006

/KWB 02/ Kraftwerk Biblis, Betriebsbericht zur Information der RSK 2002

/KWB 03/ Kraftwerk Biblis, Betriebsbericht zur Information der RSK 2003

/KWB 09/ Kraftwerk Biblis, Betriebsbericht zur Information der RSK 2009

/KWG 04/ Gemeinschaftskernkraftwerk Grohnde, RSK-Jahresbericht 2004

/KWG 13/ Gemeinschaftskernkraftwerk Grohnde, RSK-Jahresbericht 2013

/LIN 09/ Erfahrungen mit digitaler Sicherheitsleittechnik in ausländischen KKWs – eine Übersicht, A. Lindner, Institut für Sicherheitstechnologie (ISTech) GmbH, TÜV Nord Symposium Digitale Leittechnik im Reaktorschutz, September 2009

/ME 00/ Meldepflichtiges Ereignis, „Fehlerhafte sekundärseitige Lastabsenkung und nichterfolgter Stabeinwurf“, GKN 1, 10.05.2000

/ME 01/ Meldepflichtiges Ereignis, „Absturz eines Brennelementes nach dem fehlerhaften Anheben“, KKK, 06.04.2001

/ME 05/ Meldepflichtiges Ereignis, „Temporäre Störungen von Symphony Baugruppen“, KKI 1, 31.01.2005

/ME 07/ Meldepflichtiges Ereignis, „Nicht spezifikationsgerechtes Verhalten des SINUPERM N Mittelbereichsmesskanals“, KWB-B, 04.09.2007

/ME 11/ KWB-B, Meldung eines meldepflichtigen Ereignisses in Anlagen nach §7 AtG zur Spaltung von Kernbrennstoffen, 02/2011, Ausfall des Messkreises 24YX03 X054 Leistungsbereich in der Neutronenfluss-Außeninstrumentierung, Februar 2011

/ME 13/ Meldepflichtiges Ereignis, „Fehlerhafte Auslösung von Brandschutzklappen im USUS infolge einer Störung in der Brandmeldeanlage 1F51“, KKP 1, 31.10.2013

/MIT 07/ Defense in Depth and Diversity Approach for the US-APWR Digital Safety System, Masafumi Utsumi, Mitsubishi Heavy Industries Ltd., IAEA Technical Meeting on Common Cause Failures in Digital Instrumentation and Control System of Nuclear Power Plant, Juni 2007

/MIT 14/ Mitsubishi Heavy Industries, Koji Ito, Development of Mitsubishi Computerized Human Machine Interface and Digital I&C system for PWR Plants The 17th International Workshop on Nuclear Safety & Simulation Technology (IWNSST17) January 21, 2014

/NEI 09/ Nuclear Engineering International, Feature, „Upgrading & uprating – A digital dream“, 25.06.2009

/NEI 10/ Nuclear Engineering International, News, „Areva to supply I&C system for Novovoronezh-2“, 26.01.2010

/NEI 10a/ Nuclear Engineering International, H.M. Hashemian, “Instrumentation and control – Digital I&C – USA’s first fully digital station”, 10.11.2010

/NEI 14/ Nuclear Engineering International, Fortum drops Areva-Siemens for Rolls-Royce at Loviisa, 22 May 2014

/NMU 11/ Sachstandsinformation Kernkraftwerk Grohnde (KWG), Niedersächsisches Ministerium für Umwelt und Klimaschutz, 15.04.2011

/NRC 08/ Official Transcript of Proceedings, Nuclear Regulatory Commission, Advisory Committee on Reactor Safeguards, NRC-2223, Juni 2008

/NRC 10/ US NRC News, No. 10.021: NRC approves major instrumentation and control upgrade for safety-related systems at Oconee Nuclear Plant, Februar 2010

/NRC 11/ US NRC regulatory guide 1.152, Revision 3, Criteria for use of Computers in Safety Systems of Nuclear Power Plants, Juli 2011

/NRC 12/ Guidance for Evaluation of Diversity and Defence-in-Depth in Digital Computer-Based Instrumentation and Control Systems, Branch Technical Position 7-19, Revision 6,US NRC, Juli 2012

/NUC 07/ Nuclear News, Instrumentation & Controls Special Section, Scott Patterson: Digital I&C Upgrades and regulatory guidance, Dezember 2007

/NUC 10/ NucNet News, Areva and Siemens win Slovakia Digital I&C Contract, April 2010

/NUR 04/ US NRC, NUREG/CR-6842, Advanced Reactor Licensing: Experience with Digital I&C Technology in Evolutionary Plants, April 2004

/NUR 07/ US NRC, NRC Standard Review Plan NUREG-0800, Section 7.8, Revision 5, Diverse Instrumentation and Control Systems, März 2007

/NUR 09/ NUREG/CR-6992; U.S.NRC; 2009

/NUR 10/ US NRC, NUREG/CR-7007, Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems, Februar 2010

/NUR 94/ Method for Performing Diversity and Defence-in-Depth Analyses of Reactor Protection Systems, NUREG/CR-6303, US NRC, Dezember 1994

/POU 09/ Description of the Digital I&C of the French Reactors, X. Pouget-Abadie, GPR, Third Quadripartie Working Group Meeting on DIC, Oktober 2009

/RAD 10/ Safety Critical FPGA-based NOO I&C Systems: Assessment, Development and Implementation, E. Bakhmach, A. Siora, V. Tokarev, V. Kharchenko, V. Sklyar, A. Andrashov, Radiy, 17th Pacific Basin Nuclear Conference, Oktober 2010

/ROL 10/ Rolls-Royce, Spinline 3 Digital Safety I&C Platform Overview, Januar 2010

/ROL 12/ Rolls-Royce, Spinline, A Rolls-Royce modular I&C digital platform dedicated to nuclear safety, Technical Sheet, 2012

/RSK 97/ Reaktorsicherheitskommission (RSK), RSK-Leitlinien für Druckwasserreaktoren, Verband der Technischen Überwachungs-Vereine e.V. (VdTÜV), Essen, Fassung 01.97, 1997

/SCH 01/ SPINLINE 3 inside, nuclear reactor instrumentation and control, Informationsbroschüre; Schneider Electric; 2001

/SIE 02/ Siemens, TELEPERM XP, System Overview, The Process Control System for Economical Power Plant Control, 2002

/SIE 06/ Simatic, Kommunikation mit Simtic, Systemhandbuch, September 2006

/SIE 11/ Simatic, S7-400 Automatisierungssystem S7-400, Baugruppendaten Ausgabe August 2011

/SIE 11a/ Siemens Broschüre, Simatic Technology für technische Aufgaben – Zählen/Messen, Nockensteuern, Regeln, Motion Control, April 2011

/SIV 11/ Vladimir Sivokon, Oleg Bozhenkov, Current approaches to NPP I&C development and implementation in Russia, IAEA TWG NPP I&C, 24-26 May 2011

/STU 12/ Inspection of I&C systems and equipment, Safety and regulation of nuclear power plants – regulatory project management for a new build, STUK, September 2012

/TEC 08/ Tecnoticias, News Bulletin of Tecnatom, s. a., Number 32, Juli 2008

/TÜV 01/ /TÜV Süddeutschland, Kernkraftwerk Isar 1, Gutachterliche Stellungnahme zum 2. Realisierungsschritt des Bedien- und Beobachtungssystems für die Warte (Bedienen), Juni 2001

/TÜV 07/ TÜV Nord SysTec, Kernkraftwerk Brunsbüttel, Stellungnahme zur GRS-Weiterleitungsnachricht 20 06/05 vom 09.10.2006, Oktober 2007

/TÜV 08/ TÜV Süd Industrie Service, Kernkraftwerk Gundremmingen (KRB II), Block B und C, GRS-Weiterleitungsnachricht Nr. 20 06/05 „Temporäre Störung von Symphony-Baugruppen“ im Kernkraftwerk Isar 1 am 26.01.2005, Februar 2008

/TÜV 09/ TÜV Nord SysTec GmbH & Co. KG, Kraftwerk Biblis Block A, Aufsichtsverfahren nach §19 AtG, Stellungnahme zur GRS-Weiterleitungsnachricht Nr. 20 06/05 und Abschlussmeldung, Juli 2009

/TÜV 10/ TÜV Süd Industrie Service GmbH, Kraftwerk Biblis, Block B (KWB B), Aufsichtsverfahren nach §19 AtG, Weiterleitungsnachricht der GRS 20 06/05 „Temporäre Störung von Symphony-Baugruppen“ im Kernkraftwerk Isar 1 am 26.01.2005, Abschlussstellungnahme, April 2010

/UMB 07/ Umweltministerium Baden-Württemberg, Genehmigung für die Vornahme von Veränderungen im Kernkraftwerk Philippsburg, Block 2, 2007

/USP 70/ Magnetic Laddic Core Device, United States Patent Office, 3,531,784, September 1970

/VdT 08/ Stellungnahme des VdTÜV zu den erforderlichen Vorsorgemaßnahmen gegen systematisches Versagen von digitalen leittechnischen Einrichtungen in kerntechnischen Anlagen, die Leittechnikfunktionen der Kategorie 1 ausführen, 38. Sitzung des VdTÜV FAK LE, Januar 2008

/VGB 08/ VGB, Elektro- und Leittechnik in Kernkraftwerken, Innovative und verlässliche Lösungen für die Elektro- und Leittechnik in Kernkraftwerken, VGB PowerTech 08/2008

/VNI/ Federal State Unitary Enterprise, All-Russia Research Institute of Automatics (VNIIA), Software and hardware for automatic process control systems at heat and nuclear power plants, http://vniia.ru/eng/asutp/index.html [abgerufen am 02.10.2014]

/WAA 09/ Temelin Safety Systems Overview, H. Waage, TÜV Nord Symposium Digitale Leittechnik im Reaktorschutz, September 2009

/WES 04/ Ovation Product Family, Westinghouse Electric Company, Juni 2004

/WLN 04/ GRS, Weiterleitungsnachricht zu Ereignissen in Kernkraftwerken der Bundesrepublik Deutschland (WLN 20 04/11A), Ergänzung zur Weiterleitungsnachricht 20 04/11 Abweichungen im Betrieb der Brennelementwechselbühne im Kernkraftwerk Brunsbüttel, März 2004

/WLN 06/ GRS, Weiterleitungsnachricht zu Ereignissen in Kernkraftwerken der Bundesrepublik Deutschland (WLN 20 06/05), Temporäre Störung von Symphony-Baugruppen im Kernkraftwerk Isar 1 am 26.01.2005, Oktober 2005

/XU 10/ Design Optimization and Operational Experiences of Digital Safety I&C in Tianwan NPP/China, Xu X., Li, Y. and Ding, Y., 2. Symposium Digital Safety I&C, September 2010

/YAS/ German-Ukrainian Collaboration in the Assessment of Digital I&C Systems for Safety Applications in NPPs, M. Yastrebenetsky, D. Wach, B. Mulka, S. Vinogradskaia

/YAS 07/ Ukrainian State Scientific Technical Center on Nuclear and Radiation Safety, M. Yastrebenetsky, V. Sklyar, „Experience of CCF Defence for Digital I&C of Ukrainian NPP“, IAEA Technical Meeting Common Cause Failures in Digital Instrumentation and Control Systems of Nuclear Power Plants, 2007

Abbildungsverzeichnis

Tabellenverzeichnis

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH

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

Forschungszentrum
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 978-3-944161-36-5