Dokumentationsunterlage zur Regeländerung

KTA 3501

Reaktorschutzsystem und Überwachungseinrichtungen des Sicherheitssystems

Fassung 2015-11

Inhalt

1 Auftrag des KTA

Der UA-EL hat die Regel KTA 3501 im Jahr 2005 nach Abschnitt 5.2 der Verfahrensordnung des KTA überprüft. Er hat festgestellt, dass die Regel an den Stand von Wissenschaft und Technik anzupassen sei und den KTA um einen entsprechenden Beschluss gebeten.

Der Kerntechnische Ausschuss fasste auf seiner 59. Sitzung am 22. November 2005 die folgenden Beschlüsse:

Beschluss-Nr.: 59/8.2.2/1 vom 22. November 2005

Der Unterausschusses ELEKTRO- UND LEITTECHNIK (UA-EL) wurde beauftragt, federführend den Entwurf zur Änderung der Regel

KTA 3501 Reaktorschutzsystem und Überwachungseinrichtungen des Sicherheitssystems (Fassung 6/85)

mit einer Dokumentationsunterlage durch ein Arbeitsgremium erarbeiten zu lassen.

Beschluss-Nr.: 59/8.2.2/2 vom 22. November 2005

Der Unterausschusses ELEKTRO- UND LEITTECHNIK (UA-EL) wurde beauftragt, den Entwurfsvorschlag zur Änderung der Regel KTA 3501 zu prüfen und eine Beschlussvorlage für den KTA zu erarbeiten.

Die Geschäftsstelle wurde beauftragt, diesen Beschluss zur Regel KTA 3501 dem Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit zur Veröffentlichung im BAnz. zuzuleiten.

Die Beschlüsse des KTA wurden in einer Sitzung am 1. Februar 2005 von einem Arbeitskreis KTA 3501 vorbereitet. Der Arbeitskreis stellte den folgenden Änderungs- und Ergänzungsbedarf zusammen und erstellte einen Entwurf für das Inhaltsverzeichnis:

Zusammenstellung des Änderungs- und Ergänzungsbedarfs der KTA 3501 bzgl. des Einsatzes rechnerbasierter Leittechnik KTA-Dok.-Nr. 3501/05/1

Die Regeländerungsentwurfsvorlage der KTA 3501 sollte neben redaktionellen Verbesserungen gegenüber der Regel KTA 3501 (Fassung 6/85) folgende wesentliche Änderungen aufweisen:

- Der Titel der Regel soll in „Leittechnik des Sicherheitssystems“ geändert werden, um den Bezug zu dem heute verwendeten Begriff „Sicherheitssystem“ herzustellen.
- Die Kategorisierung der Leittechnik des Sicherheitssystems soll funktional, entsprechend DIN IEC 61226, erfolgen.
- Die bestehenden Regelungen der KTA Regel 3501 sollen substanziell erhalten bleiben, da die bisherige Form geeignet und bewährt ist, um analoge Leittechnik des Sicherheitssystems zu bewerten. Es sollen aber Ergänzungen für die Bewertung rechnergestützter Systeme eingearbeitet werden.
- Der Anwendungsbereich der Regel soll alle Systeme die Funktionen der Kategorie A ausführen und die Funktionen der Kategorie B und C ausführen, die bislang auch in der KTA 3501 behandelt wurden, umfassen. Die davon betroffenen Funktionen der Kategorien B und C sind einzeln zu benennen und zu kategorisieren.
- Grundsätzliche Anforderungen übergeordneter oder mitgeltender Normen und Regeln (z. B. die funktionale Kategorisierung nach DIN IEC 61226) sollen übernommen werden.
- Die vorhandene hardwareorientierte Untergliederung der Systeme ist durch den „Systemgedanken“ zu ergänzen. Die Gerätequalität ist dabei auf die Systemqualität, bestehend aus der Gerätequalität und der funktionalen Qualität (z. B. durch Systemaufbau und Software) zu erweitern.

- Für die Gerätequalität kann auf die Typprüfungen gemäß KTA 3503 und KTA 3505 verwiesen werden.
- Für die Software sind Festlegungen gemäß DIN IEC 60880 und DIN EN 61508 zu treffen.
- Die Systemaspekte werden in der Regel KTA 3506, „Systemprüfung der leittechnischen Einrichtungen des Sicherheitssystems in Kernkraftwerken“ behandelt. Diese Regel ist deshalb zeitgleich und parallel zu überarbeiten.
- Die Kategorisierung der Gefahrenmeldeeinrichtungen soll entsprechend DIN IEC 61226 erfolgen.
- Die Änderungen und Ergänzungen sollen abschnittsweise eingearbeitet werden. Es soll keine neue Parallelregel für rechnergestützte Systeme entstehen.
- Das Kapitel 12 der KTA 3501 soll ersatzlos gestrichen werden.

Entwurfsvorschlag des Arbeitskreises für das Inhaltsverzeichnisses KTA-Dok.-Nr. 3501/05/1

Titelvorschlag des Arbeitskreises: KTA 3501 „Leittechnik des Sicherheitssystems“

Grundlagen

1 Anwendungsbereich

2 Begriffe
2.1 Definitionen
2.2 Kategorisierung

3 Aufgabenstellung der Leittechnik des Sicherheitssystems der Kategorie A
3.1 Grundsätzliche Anforderungen
3.2 Ereignisabläufe und ihre Auswirkungen
3.3 Ausgangszustand der Anlage
3.4 Erfassung der Störfälle
3.5 Unterstützende Systeme der Kategorien B und C (ebenfalls entspr. KTA 3501 auszuführen)

4 Auslegungsgrundlagen für Leittechnik für Sicherheitssysteme die Funktionen der Kategorie A ausführen und unterstützende Systeme die Funktionen der Kategorien B und C ausführen
4.1 Grundsätzliche Anforderungen
4.2 Versagenauslösende Ereignisse
4.3 Auslegung gegen versagenauslösende Ereignisse außerhalb der Reaktoranlage
4.4 Ausfallkombinationen
4.5 Anregung von Schutzaktionen
4.6 Redundanz und Unabhängigkeit
4.7 Trennung des Reaktorschutzsystems von anderen Systemen
4.8 Betrieb des Reaktorschutzsystems bei Instandhaltungsarbeiten
4.9 Abstimmung zwischen dem Reaktorschutzsystem und den aktiven Sicherheitseinrichtungen
4.10 Überwachung auf Funktionsbereitschaft und Prüfbarkeit
4.11 Schutzbegrenzungen
4.12 Funktionsgruppensteuerungen des Reaktorschutzsystems
4.13 Ermittlung der Grenzwerte zur Auslösung von Schutzaktionen
4.14 Handeingriffe

5 Aufbau der Leittechnik des Sicherheitssystems
5.1 Systemqualität
5.1.1 Gerätequalität
5.1.2 Funktionale Qualität
5.1.2.1 Systemaufbau (defence in depth, common cause)
5.1.2.2 Softwarequalität (Software, Firmware)
5.2 Umgebungseinflüsse
5.3 Räumliche Anordnung, Trennung zueinander redundanter Einrichtungen
5.4 Mechanischer Aufbau
5.5 Aufbau von Untersystemen des Sicherheitssystems
5.6 Schaltung

6 Aggregateschutz

7 Zustandsbegrenzungen

8 Lüftungstechnische Anlagen zur Kühlung der Leittechnik des Sicherheitssystems

9 Elektrische Energieversorgung

10 Gefahrenmeldeeinrichtungen
10.1 Allgemeines

2 Beteiligte Fachleute

2.1 Zusammensetzung des KTA-Unterausschusses ELEKTRO- und LEITTECHNIK (UA-EL)

- aus Datenschutzgründen in dieser Datei gelöscht -

2.2 Zusammensetzung des Arbeitsgremiums

- aus Datenschutzgründen in dieser Datei gelöscht -

2.3 Zugezogene Fachleute

- aus Datenschutzgründen in dieser Datei gelöscht -

2.4 Mitarbeiter der KTA-Geschäftsstelle

Dr. G. Roos	KTA-Geschäftsstelle, Salzgitter, (bis Juli 2007)
Dipl.-Ing. H.-J. Schwarzberg	TÜV NORD EnSys GmbH & Co. KG, Hannover, (von Nov. 2007 bis April 2009)
Dipl.-Ing. R. Piel	KTA-Geschäftsstelle, Salzgitter (seit April 2009)

3 Verlauf des Regeländerungsverfahrens

3.1 Erstellung des Regeländerungsentwurfsvorschlages

(1) Das Arbeitsgremium KTA 3501 erarbeitete den Regeländerungsentwurfsvorschlag in 19 Sitzungen; die Sitzungen fanden statt:

1. Sitzung am 11. Juli 2006 bei der GRS in Braunschweig
2. Sitzung am 2./ 3. November 2007 bei der EKK in Hannover
3. Sitzung am 1./2. Februar 2007 bei der GRS in Köln
4. Sitzung am 4./5. Juli 2007 bei der ISTec in Garching
5. Sitzung am 26./27. November 2007 bei der KSG / GfS in Essen-Kupferdreh
6. Sitzung am 23./24. April 2008 bei der ISTec in Garching
7. Sitzung am 14./15. Oktober 2008 bei der EnKK in Neckarwestheim
8. Sitzung 28./29. April 2009, Hochschule Zittau
9. Sitzung 22./23. September 2009, TÜV SÜD Mannheim
10. Sitzung 23./24. Februar 2010, TÜV SÜD München
11. Sitzung 27. April 2010, E.ON Kernkraft Hannover
12. Sitzung 29. Juni 2010, ISTec Garching
13. Sitzung 7./8. September 2010 bei Westinghouse in Mannheim
14. Sitzung 11./12. Januar 2011 bei der VENE in Brunsbüttel
15. Sitzung 5./6. April 2011 bei der GRS in Köln
16. Sitzung 28./29. Juni 2011 beim TÜV NORD in Hamburg
17. Sitzung 27./28. September 2011 bei der EnKK in Neckarwestheim
18. Sitzung 6.-8. Dezember 2011 bei Westinghouse in Mannheim
19. Sitzung 24./25. Januar 2012 bei der GRS in Berlin

(2) Im Nachgang zur 19. Sitzung am 24./25. Januar 2012 wurde am 10. Februar 2012 der Regeländerungsentwurfsvorschlag KTA 3501 (Fassung 2012-02) in einer Abstimmung per Umlaufverfahren mehrheitlich zur Vorlage an den Unterausschuss ELEKTRO UND LEITTECHNIK (UA-EL) verabschiedet.

(3) Der Unterausschuss ELEKTRO UND LEITTECHNIK (UA-EL) hat am 5. März 2012 in einer Abstimmung per Umlaufverfahren mit 5/6-Mehrheit (Dafür: 14 / Dagegen: 1) beschlossen, den Regeländerungsentwurfsvorschlag KTA-Dok.-Nr. 3501/12/1 für den Fraktionsumlauf freizugeben.

(4) Der Regeländerungsentwurfsvorschlag KTA 3501 (2012-03) hat vom 15. März 2012 bis zum 15. Juni 2012 den Fraktionen des KTA zur Prüfung vorgelegen. Es gingen 426 Stellungnahmen ein, von folgenden Einwendern:

1. AREVA, Schreiben vom 01.06.2012
2. EKK, Schreiben vom 15.06.2012
3. BMUB, Schreiben vom 15.06.2012
4. Götz, SMUL, Schreiben vom 02.05.2012
5. RSK-EE, Schreiben vom 15.06.2012
6. RSK-AST, Schreiben vom 15.06.2012
7. RWE Power AG, Schreiben vom 15.06.2012
8. Scharlaug, MJKE SH, Schreiben vom 15.06.2012
9. Seidel, Bfs, Schreiben vom 14.06.2012
10. TÜV SÜD Energietechnik, Schreiben vom 15.06.2012
11. VdTÜV, Schreiben vom 02.07.2012

(5) Das Arbeitsgremium hat über die eingegangenen Stellungnahmen auf folgenden Sitzungen beraten:

20. Sitzung am 04./05. September 2012 bei der GRS in Köln
21. Sitzung am 29./30. Oktober 2012 beim TÜV NORD in Hamburg
22. Sitzung am 8./9. Januar 2013 bei der EnKK in Neckarwestheim
23. Sitzung am 27./28. Februar 2013 bei der EKK in Hannover
24. Sitzung am 17./18. April 2013 bei der GRS in Berlin
25. Sitzung am 16./17. Mai 2013 bei der GRS in Köln
26. Sitzung am 19./20. Juni 2013 beim TÜV NORD in Hamburg
27. Sitzung am 17.-19. Juli 2013 bei der EnKK in Neckarwestheim.

(6) Nach Bearbeitung der Einwendungen hat das Arbeitsgremium einstimmig beschlossen den Regeländerungsentwurfsvorschlag in der Fassung vom 19. Juli 2013 dem UA-EL zur Prüfung vorzulegen und ihm zu empfehlen, dem KTA vorzuschlagen diesen als Regeländerungsentwurf (Gründruck) zu verabschieden.

3.2 Erarbeitung des Regeländerungsentwurfes

(1) Der UA-EL hat auf seiner 74. Sitzung am 4. September 2013 den Regeländerungsentwurfsvorschlag geprüft und mit einer Gegenstimme beschlossen, dem KTA die Verabschiedung der Fassung September 2013 (KTA-Dok.-Nr. 3501/13/1) als Regeländerungsentwurf zu empfehlen.

(2) Der KTA entsprach dieser Empfehlung nicht und hat auf seiner 68. Sitzung am 19. November 2013 die Regeländerungsentwurfsvorlage an den UA-EL zurück verwiesen. Im KTA wurde die nötige 5/6-Mehrheit nicht erreicht.

(3) Zur Konkretisierung der Einwände aus der KTA-Sitzung und aufgrund des unterschiedlichen Abstimmungsverhaltens der Fraktionen auf Fachebene und übergeordneter Ebene, fand auf Einladung von Hagmann am 29. Januar 2014 eine Interimssitzung statt, um die strittigen Punkte herauszustellen und zu konkretisieren. Eingeladen waren die Einwender aus der 68. KTA-Sitzung und die Obleute des AG KTA 3501. Das Ziel dieser Sitzung war, zu eruieren, auf welchem Weg eine Weiterbearbeitung erfolgen sollte, um eine Verabschiedung als Gründruck im November 2014 erreichen zu können.

(4) Auf der Interimssitzung ist neben einer Auflistung der zusätzlich zu bearbeitenden Einwendungen auch ein Zeitplan vorgeschlagen worden, der eine Verabschiedung zum Gründruck im November 2014 möglich machen sollte.

Zeitplan:

Termin	Aufgabe	Verantwortliche/r
31.03.2014	Abgleich der Inhalte und Formulierungen, die bereits in den Interpretationen der SiAnf vorhanden sind,	Sommer (GRS)
31.03.2014	Textvorschlag RWE zu 4.1.1 und 4.1.2 - Erstellung Textvorschlag	Noack (RWE)
31.03 .2014	- Berücksichtigung der RSK-EE-Einwendungen - Erstellung Textvorschlag	Reßing (für RSK)
02.04.2014	Zusammenführen der Textvorschläge	Piel
30.04.2014	Kommentierung der Änderungen (Insbesondere Abschnitt 4.1.3.1)	Graf (AREVA), Berger (WEG)
30.06 2014	Diskussion und Fertigstellung des ÄEV KTA 3501	AG KTA 3501
01.07.2014	Diskussion des ÄEV KTA 3501	UA-EL
02.09.2014	Empfehlung für den KTA zum Gründruck	UA-EL

(5) Das AG KTA 3501 benötigte für die Bearbeitung etwas mehr Zeit als geplant und hat über die Einwendungen und Textvorschläge sowie über die eingegangenen Stellungnahmen auf folgenden Sitzungen beraten:

28. Sitzung am 13./14. Mai 2014 bei der GRS in Garching

29. Sitzung am 8./9. Juli 2014 bei Westinghouse in Mannheim

30. Sitzung am 19. August 2014 bei der GRS in Köln.

(6) Nach Bearbeitung der Einwendungen hat das Arbeitsgremium einstimmig beschlossen die Regeländerungsentwurfsvorlage in der Fassung vom 19. August 2014 dem UA-EL zur Prüfung vorzulegen und ihm zu empfehlen, dem KTA vorzuschlagen diesen als Regeländerungsentwurf (Gründruck) zu verabschieden.

(7) Über den Stand der Bearbeitung wurde der UA-EL auf seiner 75. Sitzung am 1. Juli 2014 informiert. Auf seiner 76. Sitzung am 2. September 2014 wurde die Regeländerungsentwurfsvorlage geprüft und einstimmig beschlossen, dem KTA die Verabschiedung der Fassung September 2014 (KTA-Dok.-Nr. 3501/14/1) als Regeländerungsentwurf zu empfehlen.

3.3 Erarbeitung der Regeländerung

(1) Der KTA hat die Regeländerungsentwurfsvorlage auf seiner 69. Sitzung am 11. November 2014 als Regeländerungsentwurf in der Fassung 2014-11 verabschiedet. Auf der KTA-Sitzung wurde von der RSK eingewendet, dass bezüglich des Absatzes 4.1.1 (2) noch Klarstellungsbedarf bestehe: Eine unabhängige Überlagerung (Gleichzeitigkeit) einer Einwirkung von innen („versagensauslösendes Ereignis innerhalb der Reaktoranlage“ gemäß 4.1.2.2 des Entwurfs der KTA 3501) mit einem Störfall müsse nicht unterstellt werden, dies gehe aber aus dem vorliegenden Text nicht eindeutig hervor. Der KTA beauftragte deshalb den UA-EL und das zuständige Arbeitsgremium, die von der RSK geäußerten Vorbehalte gegen 4.1.1 (2) im Rahmen des Gründruckverfahrens einvernehmlich zu klären. Hierzu sei im März 2015 beim UA-PG Zwischenbericht zu erstatten. Die Bekanntmachung des Regeländerungsentwurfes erfolgte im Bundesanzeiger am 5. Dezember 2014.

(2) Der Absatz (2) des Abschnittes 4.1.1 wurde am 6. Februar 2015 vom Arbeitsgremium und zusammen mit einem Vertreter der RSK diskutiert und einstimmig verabschiedet. Das Ergebnis der Sitzung wurde in der RSK und im UA-PG vorgestellt.

(3) Der Regeländerungsentwurf KTA 3501 (2014-11) hat vom 01.Januar.2015 bis zum 31. März 2015 der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegen. Es sind insgesamt 4 Stellungnahmen zum Regeländerungsentwurf eingegangen von folgenden Einwendern:

TÜV NORD	31.03.2015
Piel KTA-GS	31.03.2015.

(4) Da es sich nur um 4 vorwiegend redaktionelle Einwendungen handelte, wurden diese im Umlaufverfahren (per E-Mail) bearbeitet. Es wurde einstimmig beschlossen, den Regeländerungsvorschlag in der Fassung 2015-04 dem UA-EL zur Prüfung vorzulegen und ihm zu empfehlen, dem KTA vorzuschlagen, diesen als Regeländerung (Weißdruck) zu verabschieden.

(5) Der UA-EL hat auf seiner 78. Sitzung am 1. September 2015 die Regeländerungsvorlage geprüft und einstimmig beschlossen, dem KTA die Verabschiedung der Fassung September 2015 (KTA-Dok.-Nr. 3501/15/1) als Regeländerung zu empfehlen.

(6) Der KTA entsprach dieser Empfehlung und hat auf seiner 70. Sitzung am 10. November 2015 die Regeländerungsvorlage als Regel (Regeländerung) KTA 3501 in der Fassung 2015-11 aufgestellt. Die Bekanntmachung erfolgte im Bundesanzeiger vom 26. November 2015, der Volltext der Regel wurde im Bundesanzeiger vom 8. Januar 2016 veröffentlicht.

4 Berücksichtigte Regeln und Unterlagen

4.1 Abgleich der KTA 3501 mit den SiAnf (2015-03) und deren Interpretationen (2015-03)

(1) Die Schnittstellen der KTA 3501 mit den SiAnf und deren Interpretationen wurden einander gegenüber gestellt und auf Umsetzung und Konsistenz geprüft. Eine ausführliche Darstellung des Abgleiches befindet sich in „Abgleich mit den SiAnf und deren Interpretationen“ KTA-Dok.-Nr. 3501/15/3.

(2) Soweit Widersprüche festgestellt wurden, wurde der Regeltext entsprechend angepasst. An mehreren Stellen wurden Unterschiede festgestellt, die aber nicht als widersprüchlich zu den SiAnf und deren Interpretationen gewertet wurden.

4.2 Nationale Unterlagen

Neben dem im Anhang A zur KTA 3501 „*Bestimmungen auf die in dieser Regel verwiesen wird*“ aufgeführten Regeln wurden folgende Unterlagen bei der Regelüberarbeitung berücksichtigt:

- DIN EN 60671 VDE 0491-100: (2011-12) Kernkraftwerke - Leittechnik für Systeme mit sicherheitstechnischer Bedeutung - Prüfungen zur Sicherstellung der Funktionsfähigkeit (IEC 60671:2007); Deutsche Fassung EN 60671:2011
- DIN IEC 60780 (2000-12): Kernkraftwerke - Elektrisches Gerät des Sicherheitssystems - Qualifizierung (IEC 60780:1998)
- DIN EN 60987 2010-03): Kernkraftwerke - Leittechnische Systeme mit sicherheitstechnischer Bedeutung - Anforderungen an die Hardware-Auslegung rechnerbasierter Systeme (IEC 60987:2007, modifiziert); Deutsche Fassung EN 60987:2009
- DIN EN 60880 VDE 0491-3-2 (2010-03-00): Kernkraftwerke - Leittechnik für Systeme mit sicherheitstechnischer Bedeutung - Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie A (IEC 60880:2006); Deutsche Fassung EN 60880:2009
- DIN EN 61226 VDE 0491-1 (2010-08-00): Kernkraftwerke - Leittechnische Systeme mit sicherheitstechnischer Bedeutung - Kategorisierung leittechnischer Funktionen (IEC 61226:2009); Deutsche Fassung EN 61226:2010
- DIN IEC 61513 VDE 0491-2 (2010-04-00): Kernkraftwerke - Leittechnik für Systeme mit sicherheitstechnischer Bedeutung - Allgemeine Systemanforderungen (IEC 45A/790/CDV:2009)
- DIN IEC 62671 VDE 0491-3-6 (2012-01-00): Kernkraftwerke - Leittechnik mit sicherheitstechnischer Bedeutung - Auswahl und Verwendung industrieller digitaler Einheiten begrenzter Funktionalität (IEC 45A/845/CDV:2011)
- DIN EN 61508-3 VDE 0803-3 (2011-02-00): Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer / programmierbarer elektronischer Systeme - Teil 3: Anforderungen an Software (IEC 61508-3:2010); Deutsche Fassung EN 61508-3:2010
- DIN IEC 60050-351 (2009-06): Internationales Elektrotechnisches Wörterbuch - Teil 351: Leittechnik (IEC 60050-351:2006)
- DIN ISO 10007 (2004-12-00): Qualitätsmanagement - Leitfaden für Konfigurationsmanagement (ISO 10007:2003)
- VDI/VDE 3527 (2002-07-00): Kriterien zur Gewährleistung der Unabhängigkeit von Sicherheitsfunktionen bei der Leittechnik-Auslegung
- VDI/VDE 3528 Blatt 1 (2011-08-00): Anforderungen an Serienprodukte und Kriterien für deren Einsatz in der Sicherheitsleittechnik in Kernkraftwerken - Allgemeiner Teil

4.3 Internationale Unterlagen

Neben dem im Anhang A zur KTA 3501 „*Bestimmungen auf die in dieser Regel verwiesen wird*“ aufgeführten Regeln wurden folgende Unterlagen bei der Regelüberarbeitung berücksichtigt:

- IAEA Safety Guide „Instrumentation and Control Systems Important to Safety in Nuclear Power Plants”, Safety Standards Series No. NS-G-1.3 (2002-03)
- IAEA Safety Guide „Software for computer based systems”, Safety Standards Series No. NS-G-1.1 (2000-11)
- IEEE Std 603-1998 Standard criteria for safety systems for nuclear power generating stations
- IPC A 610 D (2005-02) “Acceptability of Electronics Assemblies”
- NUREG/CR-6303 UCRL-ID-119239 (1994-12): Method for Performing Diversity and Defence-in-Depth Analyses of Reactor Protection Systems by G.C. Preckshot

4.4 Weitere Unterlagen

Neben dem im Anhang A zur KTA 3501 „*Bestimmungen auf die in dieser Regel verwiesen wird*“ aufgeführten Regeln wurden folgende Unterlagen bei der Regelüberarbeitung berücksichtigt:

- „Sicherheitskriterien für Kernkraftwerke Revision D (2009-04): Kriterien für die Leittechnik und Störfallinstrumentierung“ (Modul 5)
- Weiterleitungsnachricht der GRS WLN 2006-07 „Nichtzuschalten von zwei Notstromdieseln nach Ausfall der 400kV-Netzanbindung“, Ereignis im schwedischen Kernkraftwerk Forsmark, Block 1 am 25.07.2006

- Abschlussbericht zum BMU-Vorhaben SR 2471: Fachberatung zur Um- und Nachrüstung der Sicherheitsleittechnik in deutschen Kernkraftwerken: Zuverlässigkeitsbewertung von rechnergestützter Sicherheitsleittechnik in kerntechnischen Anlage - Digitale Leittechnik, Arbeitspunkt A.3: „Anforderungen an die Instandhaltung und Modifikation von rechnergestützten Komponenten und Teilsystemen der Sicherheitsleittechnik im Hinblick auf deutsche Belange“ (ISTec-A-899 April 2006)
- Abschlussbericht zum BMU-Vorhaben SR 2586: Fachberatung zur Um- und Nachrüstung der Sicherheitsleittechnik in deutschen Kernkraftwerken: Sicherheitstechnische Bewertung zum Einsatz und Betrieb rechnergestützter Sicherheitsleittechnik in deutschen Kernkraftwerken, Arbeitspunkt A.3: „Analyse und Bewertung der Komplexität der Software und Software-basierter Sicherheitsleittechnik“ (ISTec - A – 1311 August 2010)
- Darstellung der Beratungsergebnisse der RSK-Arbeitsgruppe EINSATZ RECHNERBASIERTE LEITTECHNIK (ERL) vom 20.09.2011: „Rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken“
- Stellungnahme des VdTÜV zu den erforderlichen Vorsorgemaßnahmen gegen systematisches Versagen von digitalen leittechnischen Einrichtungen in kerntechnischen Anlagen, die Leittechnikfunktionen der Kategorie 1 ausführen 06.03.2008
- Positionsdarstellung des VGB zum Einsatz digitaler Sicherheitsleittechnik im Reaktorschutz in Kernkraftwerken VGB AG DigSILT November 2008
- MERKBLATT zum Verständnis und über Inhalt, Aufbau und äußere Form von sicherheitstechnischen Regeln des Kerntechnischen Ausschusses (KTA), (2011-11)

5 Erläuterungen der vorgenommenen Änderungen

Generell wurden ersetzt:

- „Sachverständige (nach § 20 Atomgesetz)“ durch die im Abschnitt 2.3 g) des KTA-Merkblattes vorgeschlagene Formulierung „durch die atomrechtliche Behörde oder einen von ihr nach § 20 AtG zugezogenen Sachverständigen“ ersetzt

- „Reaktorschutz“ durch „A-Funktions-Einrichtungen“;

Neben rein redaktionellen Änderungen wurde der Regeltext in folgenden Punkten geändert:

Zu „Titel der Regel“

Eine Änderung des Titels in „Sicherheitsleittechnik“ wurde diskutiert, aber nicht umgesetzt.

Für die Änderung des Titels spricht, dass die Einführung des Begriffes Sicherheitsleittechnik eine Abstufung der Anforderungen ermöglichen würde. Der Begriff „Sicherheitsleittechnik“ stammt aus den RSK-LL und umfasst die gesamte sicherheitsrelevante und sicherheitskritische Leittechnik. Die KTA 3501 würde mit den aktuellen Fassungen der KTA 3503 und der KTA 3505 harmonisiert und darüber hinaus dem im IEC und EN (CENELEC) etablierten Vorgehen entsprechen und insofern dem Stand von Wissenschaft und Technik.

Gegen eine Änderung des Titels spricht, dass unter Reaktorschutzsystem nicht nur die Sicherheitsleittechnik verstanden werden kann, sondern auch die dazugehörenden verfahrenstechnischen Komponenten. Diese werden implizit z. B. bei den Ausfallkombinationen angesprochen. In den Sicherheitsanforderungen (Hauptteil) wird der Begriff „Sicherheitsleittechnik“ nicht und der Begriff „Reaktorschutzsystem“ einmal verwendet, ohne konzeptionelle Inhalte.

Um dem Auftrag des KTA gerecht zu werden, der den Titel „Leittechnik des Sicherheitssystems“ vorschlug, und dem Umstand Rechnung zu tragen, dass das Reaktorschutzsystem sich nicht auf Leittechnik beschränkt, wurde auf die Änderung des Titels verzichtet.

Es wurde allerdings eine Kategorisierung der Leittechnik eingeführt, die von der Verfahrenstechnik vorgegeben wird und in Abschnitt 2.2 beschrieben wird. Sie schafft die Möglichkeit einer eindeutigen Abstufung der Anforderungen an die Sicherheitsleittechnik.

Dieser funktionale Ansatz zur Abstufung über die Kategorisierung wird die bisherigen hinsichtlich der funktionalen Bedeutung interpretationsfähigen Begriffe des Sicherheitssystems wie Zustandsbegrenzungen oder Schutzbegrenzungen ersetzen.

Zu „Grundlagen“

Zu „Grundlagen“ Absatz 1

Es wird nur noch auf die „Sicherheitsanforderungen an Kernkraftwerke“ vom 22. November 2012 und deren Interpretationen vom 29. November 2013 verwiesen. Die Sicherheitskriterien sowie die Störfallleitlinien und die RSK-Leitlinien werden behördlicherseits nicht mehr herangezogen. Die Änderung wurde am 19. März 2014 auf der 42. Sitzung des UA-PG abgestimmt.

Die Sicherheitsanforderungen und deren Interpretationen wurden am 3. März 2015 noch einmal revidiert.

Zu „Grundlagen“ Absatz 2 (neu)

Der Absatz ist neu eingefügt worden. Es wird der Zusammenhang zwischen der Aufgabenstellung an die Leittechnik, die sich aus den Anforderungen an die Systemtechnik ableitet, und den Anforderungen an die Systemtechnik, die sich aus den Sicherheitsebenen ableiten, hergestellt. Die Beziehung zwischen Sicherheitsebenen und Leittechnikauslegung sollte als Regelgrundlage benannt werden.

Zu „Grundlagen“ Absatz 3 (neue Nummerierung)

Zusätzlich zum Reaktorschutzsystem und den Überwachungseinrichtungen des Sicherheitssystems werden, entsprechend des Anwendungsbereiches dieser Regel, Schutz- und Zustandsbegrenzungen aufgenommen. Weiterhin wurde die Änderung der Bezüge entsprechend Absatz 1 der Grundlagen angepasst.

Zu „Grundlagen“ Absatz 4 (neu)

Der ursprüngliche Abschnitt 12 wurde als neuer Absatz 3 in den Grundlagen aufgenommen, um konsistent mit der KTA 3701 zu bleiben. Der Abschnitt 12 sollte laut Empfehlung des KTA ersatzlos gestrichen werden. Die Ergänzung in den Grundlagen erfolgte aber trotzdem, da die ZPI eine Kategorisierung der bei Änderungen vorzulegenden Unterlagen in

a) Betriebsunterlagen
b) Vorprüfunterlagen
c) Genehmigungsunterlagen

begründet. Ansonsten würden für den wichtigen Anwendungsbereich der KTA 3501 notwendige und bewährte Maßstäbe, die eine Änderung in Begutachtung, Vorprüfung I und II begründen und damit das (Vor-) Prüfverfahren zweckmäßig aufteilt, entfallen.

Dies kann zu einer Verkürzung der inhaltlichen Sachprüfung der Behörde führen, wodurch wesentliche Nachweise/Informationen zu den Anlagenteilen nicht mehr als Genehmigungs- oder Vorprüfunterlagen erhoben und damit evtl. auch nicht mehr im Aufsichtsverfahren geführt werden müssen.

Zu „Grundlagen“ Absatz 5 (neu)(neue Nummerierung)

Hinweis auf die Kategorisierung der leittechnischen Funktionen in Abschnitt 2.2

Zu „Grundlagen“ Absatz 6 (neue Nummerierung)

Redaktionelle Anpassung.

Zu „Grundlagen“ Absatz 9 (neue Nummerierung)

Der Verweis auf Regeln zum Nachweis der Beständigkeit von elektrischen Einrichtungen unter Störfallbedingungen wurde erweitert um die Regeln KTA 2101.3 „Brandschutz in Kernkraftwerken Teil 3: Brandschutz an maschinen- und elektrotechnischen Anlagen“ und KTA 2201.4 „Auslegung von Kernkraftwerken gegen seismische Einwirkungen; Teil 4: Anforderungen an Verfahren zum Nachweis der Erdbebensicherheit für maschinen- und elektrotechnische Anlagenteile“. Beide Regeln waren 1985 noch nicht gültig sind aber inzwischen verabschiedet.

Zu „Grundlagen“ Absatz 10 (neue Nummerierung)

Es wurde der Verweis auf die 2010 neu erschienene KTA 1403 „Alterungsmanagement in Kernkraftwerken“ ergänzt.

Zu „Grundlagen“ Absatz 11 (neue Nummerierung)

Der Absatz beschreibt den Zusammenhang zwischen konventionellem Regelwerk und KTA Regeln. Er soll verdeutlichen, dass es kernkraftwerkspezifisch Ausnahmen geben kann, die ebenfalls betrachtet werden sollten.

Der Absatz weist auf den Sachverhalt hin, dass wenn aus kernkraftwerkspezifischen Gründen von Gesetzen, Verordnungen, sonstigen öffentlich-rechtlichen Vorschriften und Unfallverhütungsvorschriften abgewichen werden muss, in jedem Einzelfall nach den in diesen Vorschriften niedergelegten Ausnahmeregelungen und Befreiungen zu verfahren ist.

Der UA-EL hat dazu am 11. September 2012 die verwendete Formulierung verabschiedet, die in alle Regeln aufgenommen wurde, die durch den UA-EL betreut werden.

Zu „1 Anwendungsbereich“

Der Anwendungsbereich wurde umformuliert und an die neu eingeführte Kategorisierung der leittechnischen Funktionen angepasst.

Der Anwendungsbereich wurde trotz der Verwendung des Begriffes Sicherheitsleittechnik nicht erweitert. Die Anforderungen konzentrieren sich hauptsächlich auf Einrichtungen mit Leittechnikfunktionen der Kategorie A und B. Anforderungen an Einrichtungen mit Leittechnikfunktionen der Kategorie C wurden nur insoweit behandelt, wie sie auch im Anwendungsbereich der KTA 3501 (1985-06) enthalten waren, wie etwa Gefahrenmeldeeinrichtungen für Gefahrenmeldungen der Klasse II. Anforderungen an weitere C-Funktions-Einrichtungen sollen in den entsprechenden Leittechnik-Kapiteln der betreffenden systemspezifischen KTA-Regeln, wie KTA 3902 für Hebezeuge, KTA 3601 für lüftungstechnische Anlagen, KTA 1505 für Strahlenmessgeräte, usw. festgelegt werden. Soweit Anforderungen an Einrichtungen mit Leittechnikfunktionen der Kategorie C gestellt wurden, wurden diese Einrichtungen explizit genannt (z. B. Gefahrenmeldeeinrichtungen der Klasse II). Auf eine umfassende Behandlung aller C-Funktionseinrichtungen wurde verzichtet, da diese den Rahmen der Regel sprengen würde.

Die Sicherheitsleittechnik umfasst alle leittechnischen Einrichtungen, die Funktionen der Kategorie A, B oder C ausführen. Diese Kategorisierung, die von der Verfahrenstechnik vorgegeben wird, schafft die Möglichkeit einer eindeutigen Abstufung der Anforderungen an die Sicherheitsleittechnik. Die hier gewählte Kategorisierung ist vergleichbar mit der Kategorisierung nach DIN EN 61226, hinterlässt aber weniger Interpretationsspielraum.

Zu „1 Anwendungsbereich“ Absatz 1

Der Anwendungsbereich wurde auf Errichtung oder Änderung beschränkt. Die Beschränkung würdigt die Altanlagen, die aufgrund ihrer Betriebsgenehmigung an den Stand von Wissenschaft und Technik zur Vorsorge gegen Schäden anpassen müssen.

Die Einschränkung des Anwendungsbereiches auf Errichtung und Änderung greift nach Auffassung einiger Mitarbeiter im KTA, unzulässig in das Aufsichtsverfahren ein und sollte deshalb nicht aufgenommen werden.

Der UA-EL diskutierte beide Positionen und beschloss am 2. September 2014 auf die Einschränkung zu verzichten. Er folgte damit der Argumentation, dass an dieser Stelle ausschließlich der Regelgegenstand festgelegt werden muss. Die Entscheidung ob und wann die Regel heranzuziehen ist, wird von der Behörde im jeweiligen Aufsichtsverfahren getroffen.

Zu „1 Anwendungsbereich“ Absatz 2 Hinweis

Die „Sicherheitsgefahrenmeldungen“ wurden mit dem Klammerausdruck „Klasse S“ ergänzt.

Zu „1 Anwendungsbereich“ Absatzes 3

Der Absatz wurde zusätzlich mit den nötigen Serviceeinrichtungen für A- und B-Funktions-Einrichtungen ergänzt. Diese Anpassung erfolgte insbesondere im Hinblick auf rechnerbasierte Systeme.

Zu „1 Anwendungsbereich“ Absatzes 4

Der Ausschluss der elektrischen Antriebe, der Leistungskabel und der Schaltanlagenabzweige einschließlich der Steuerstromkreise wurde noch einmal diskutiert, aber nicht inhaltlich geändert. Folgende Positionen wurden dabei vertreten:

- Die „Steuerstromkreise“ gehören zur Leittechnik und sollten deshalb nicht ausgeschlossen werden.
- Die Schnittstelle zwischen der 35er und der 37er Reihe wurde bisher durch die Koppelrelais gebildet. Eine Streichung würde bedeuten, dass Schutzrelais, Koppelrelais, Schaltanlagenhilfsspannungen, Steuerungen, die bislang Bestandteil der Komponente gewesen sind (Motoranlauf, Positionierung des Stellantriebs usw.) in den Anwendungsbereich der KTA 3501 fallen. Eine derartige Erweiterung des Anwendungsbereiches war im Auftrag des KTA nicht vorgesehen. Weiterhin wäre der sicherheitstechnische Gewinn dieser Änderung fraglich, da die KTA 3504 und die 37er Reihe bereits Anforderungen an diese Komponenten stellen.

Siehe auch Anmerkungen zur Definition „Leittechnische Einrichtungen“

Zu „2 Begriffe“

Zu „2.1 Definitionen“ Absatz 1 (neu)

Die Definition wurde aufgrund der neu eingeführten Kategorisierung eingefügt.

Zu „2.1 Definitionen“ Absatz 3 (neue Nummerierung) „Anregeebene“

Anpassung aufgrund der neu eingeführten Kategorisierung. Die Definition gilt für A-, B- und C-Funktions-Einrichtungen gleichermaßen.

Zu „2.1 Definitionen“ Absatz 9 (neue Nummerierung) „Antivalenzüberwachung“

Das Beispiel in Klammern hat nicht direkt mit Antivalenzüberwachung zu tun und wurde deshalb gestrichen.

Zu „2.1 Definitionen“ Absatz 10 (neue Nummerierung) „Ausfall“

Der Begriff wurde aus den SiAnf Anhang 1 übernommen.

Zu Fehlern werden auch latente Fehler gezählt, die sich nicht als Ausfall zeigen. Der Begriff „Fehler“ im Hinweis wurde deshalb durch „fehlerhaften Zustand“ ersetzt.

Zu „2.1 Definitionen“ Absatz 11 (neue Nummerierung) „Ausfall, systematischer“ Hinweis

Der Begriff wurde aus den SiAnf Anhang 1 übernommen und durch Hinweis 1 ergänzt, um auf besondere Aspekte in der Leittechnik aufmerksam zu machen. Die Ergänzung berücksichtigt, dass der systematische Ausfall das Versagen von mehreren Komponenten aufgrund der gleichen Ursache zu annähernd gleicher Zeit sei.

Im Zuge der Bearbeitung wurden die Begriffe „Ausfall“ und „Versagen“ diskutiert und festgestellt, dass mit einem „Ausfall“ gleichzeitig ein „Versagen“ auftreten kann, aber nicht muss. Zum Beispiel kann ein Aggregat, das nicht angefordert wird, ausgefallen sein, versagen wird es erst, wenn es angefordert wird und seine Funktion nicht mehr erbringt. Zur Verdeutlichung des Unterschiedes zwischen Ausfall und Versagen wurde gleichzeitig die Definition „Versagen“ aus den SiAnf Anhang 1 eingefügt.

Der Hinweis 2 stammt aus der KTA 3501 Fassung 1985

Der UA-PG hat auf seiner 35. Sitzung die Behandlung des Brandes als Ursache für einen systematischen Ausfall (Hinweis 2) diskutiert und hat dem AG KTA 3501 vorgeschlagen, den Brand als Beispiel für ein systematisches Versagen zu streichen. Er begründet dies damit, dass in der Kombination von Definition systematischer Ausfall und der Forderung eines Nachweises gemäß 4.4.1 (2) (alt) bei der Auslegung des Reaktorschutzsystems ein Brand gemeinsam mit einem anderen, davon unabhängigen Störfall zu unterstellen sei. Dies widerspräche der KTA 2101.1 in der ein redundanzübergreifender Brand durch bauliche Maßnahmen ausgeschlossen wird.

Das Arbeitsgremium kam zu dem Schluss, dass der Brand als Ursache für einen systematischen Ausfall nicht gestrichen werden sollte. Die angesprochene Fehlinterpretation wurde durch zwei Hinweise im Abschnitt 4.1.1 Grundsätzliche Anforderungen Absatz 2 abgefangen. Die bestehende Formulierung in der KTA 3501, welche Fälle bei den Ausfallkombinationen zu unterstellen sind und welche nicht wurden durch die ergänzten Hinweise konkretisiert.

Zu „2.1 Definitionen“ Absatz 13 (neue Nummerierung) „Bestimmungsgemäßer Betrieb“

Der Begriff wurde aus den SiAnf Anhang 1 übernommen, allerdings ohne die Nennung der jeweiligen Sicherheitsebenen, die bei den Instandhaltungsvorgängen nicht angegeben wurde. Der Bezug zu den Sicherheitsebenen erfolgt im Abschnitt Grundlagen, in denen auf die SiAnf verwiesen wird und kann an dieser Stelle entfallen.

Zu „2.1 Definitionen“ Absatz 14 (alt) „Betriebssystem“

Der Begriff ist doppeldeutig und wurde deshalb gestrichen. Er wird einerseits für Softwarebetriebssystem verwendet und andererseits für betriebliche Systeme, die in der ursprünglichen Definition gemeint waren. Auf die Verwendung dieses Begriffes im Regeltext im Sinne der ursprünglichen Definition wurde verzichtet.

Zu „2.1 Definitionen“ Absatz 16 (neu) „B-Funktions-Einrichtungen“

Die Definition wurde aufgrund der neu eingeführten Kategorisierung eingefügt.

Zu „2.1 Definitionen“ Absatz 17 „Dissimilare leittechnische Einrichtungen“ (neu)

Der Begriff „Dissimilare leittechnischen Einrichtungen“ wurde eingeführt, um bei Einsatz vergleichbarer Technologien durch Bewertung unterschiedlicher Aspekte die hinreichende Unähnlichkeit zweier Systeme auszudrücken.

Folgende Auffassung wurde dazu im Arbeitsgremium vertreten:

1. Dissimilarität ist der Oberbegriff
2. Dissimilarität sollte als Sonderform der Diversität beschrieben werden.

   Nach NUREG 6303 gibt es folgende Unterteilung zu Diversität:

   3.2.1. Design Diversity

   3.2.2. Equipment Diversity

   3.2.3. Functional Diversity

   3.2.4. Human Diversity

   3.2.5. Signal Diversity

   3.2.6. Software Diversity

   3.2.7. Combining Diversity Attributes

   Damit ist Diversität der Oberbegriff und Dissimilarität eine unter 3.2.7 zu subsummierende Variante von kombinierten Diversitätsattributen (hier: Geräte-, Software- und Personaldiversität). Dieses Verständnis von Diversität wird auch vom VDI/VDE Leitfaden 3528 unterstützt und sollte in KTA 3501 entsprechend der DIN IEC-Definition und im Zusammenhang mit den Begriffen Dissimilarität und Gerätediversität vorgegeben werden.

Der Begriff Dissimilarität wird im kerntechnischen Bereich international nicht genutzt.

Zu „2.1 Definitionen“ Absatz 18 „diversitäre leittechnische Einrichtungen“ (neu)

Der Begriff ersetzt die Gerätediversität, die gestrichen wurde. Der Begriff wurde aus den SiAnf Anhang 1 übernommen.

Zu „2.1 Definitionen“ Absatz 19 (neue Nummerierung) „Einzelantriebssteuerung“ Hinweis

Anpassung an neuen Terminus.

Zu „2.1 Definitionen“ Absatz 21 „Firmware“ (neu)

Die Definition von Firmware wurde für rechnerbasierte Systeme eingeführt. Der Begriff leitet sich davon ab, dass Firmware funktional fest mit der Hardware verbunden ist, was bedeutet, dass das eine ohne das andere nicht nutzbar ist. Sie nimmt eine Zwischenstellung zwischen Hardware (also den physikalischen Anteilen eines Gerätes) und der Anwendungssoftware (den ggf. austauschbaren Programmen eines Gerätes) ein.

Zu „2.1 Definitionen“ Absatz 22 (neue Nummerierung) „Folgeausfall“

Präzisierung.

Zu „2.1 Definitionen“ Absatz 23 (neue Nummerierung) „Funktionsgruppensteuerung“

Hinweis auf veralteten Begriff .

Zu „2.1 Definitionen“ Absatz 24 (neue Nummerierung) „Gefahrenmeldung der Klasse II“

Die Definition des Betriebssystems wurde gestrichen. demzufolge musste die Definition der Gefahrenmeldung der Klasse II neu formuliert werden. Redaktionelle Anpassung.

Zu „2.1 Definitionen“ Absatz 26-29 “Baugruppe/Gerät“ (neu)

Die Definition ermöglicht die Berücksichtigung technologiespezifischer Eigenschaften bei der Erstellung der Anforderungen. Es wird zwischen rechnerbasierten, programmierbaren sowie nicht programmierbaren Geräten unterschieden.

Zu „2.1 Definitionen“ Absatz 32 (neue Nummerierung) „Grenzsignalgeber“

Redaktionelle Anpassung.

Zu „2.1 Definitionen“ Absatz 34 „Inspektion“ (neu)

Der Begriff wurde aus den SiAnf Anhang 1 übernommen.

Zu „2.1 Definitionen“ Absatz 35 „Instandhaltung“

Der Begriff wurde aus den SiAnf Anhang 1 übernommen und redaktionell angepasst. Die WKP wurde in Klammern bei den „Inspektionen“ ergänzt und im 1. Satz gestrichen.

Zu „2.1 Definitionen“ Absatz 36 „Komponente“ (neu)

Dieser Begriff wurde aus der KTA Begriffe-Sammlung (2012-01) übertragen. Der Begriff wurde neu eingeführt, um den Unterschied zwischen den häufig synonym verwendeten Begriffen Gerät/ Baugruppe und Komponente klarzustellen. Der Begriff wurde nicht aus den SiAnf Anhang 1 übernommen, da diese spezielle Ergänzungen für die Verfahrenstechnik enthält, die in der Leittechnik zu Verwirrungen führen würden.

Zu „2.1 Definitionen“ Absatz 37 „Leittechnik“ (neu)

Der Begriff wurde in Anlehnung an SiAnf Anhang 1 zusätzlich aufgenommen Die vorgeschlagene Definition wurde allerdings überarbeitet. Der Aspekt, dass auch Einrichtungen zur Prozessführung durch einen Operator zur Leittechnik gezählt werden, ist in der Definition „Leittechnische Einrichtungen“ enthalten und wurde deshalb gestrichen.

Zu „2.1 Definitionen“ Absatz 38 „leittechnische Einrichtungen“ (neu)

Für die Erstellung der Definition wurde die DIN IEC 61513, die DIN IEC 60050-351 und das Modul 5 der Sicherheitskriterien für Kernkraftwerke Revision D (2009-04) herangezogen. Allerdings wurde die „Schnittstelle zwischen der Steuerebene und der Schaltanlage“ präzisiert durch „den den Einzelantrieben zugeordneten Teilen der Steuerung zur Auslösung von Schutzaktionen“ (S.a. neues Bild 2-1). Der Begriff wurde zur eindeutigen Festlegung des Anwendungsbereiches eingeführt.

Der Begriff wird in den SiAnf wurde nicht definiert.

Zu „2.1 Definitionen“ Absatz 39 „Leittechnik-Funktion“ (neu)

Die Definition stammt aus dem Modul 5 der Sicherheitskriterien für Kernkraftwerke Revision D (2009-04). Der Begriff „Leittechnik-Funktion“ wird von Verfahrenstechnikern verwendet, um die funktionalen Anforderungen an die Leittechnik zu strukturieren. Der Begriff bildet die Basis für die Kategorisierung in Abschnitt 2.2.

Zu „2.1 Definitionen“ Absatz 43 „Phasenmodell“ (neu)

Die Definition wurde eingeführt, um Anforderungen an den Softwareentwicklungsprozess stellen zu können.

Zu „2.1 Definitionen“ Absatz 45 (neue Nummerierung) „Reaktorschutz“

Der Begriff wurde aus den SiAnf Anhang 1 übernommen. Allerdings wurde der erste Satz gelöscht und am Ende des Absatzes folgender Satz eingefügt „Die Leittechnik-Funktionen des Reaktorschutzsystems sind typischerweise der Kategorie A zugeordnet.“ Das Reaktorschutzsystem sollte nicht über die Kategorie A definiert werden. Weiterhin wurden die Funktionsgruppensteuerungen im Hinweis gestrichen, da sie nicht mehr Stand der Technik sind und in dieser Regel nicht mehr behandelt werden. Der Hinweis aus der alten Definition wurde ansonsten beibehalten.

Zu „2.1 Definitionen“ Absatz 47 (neue Nummerierung) „Redundanz“

Der Begriff wurde aus den SiAnf Anhang 1 übernommen und präzisiert.

Zu „2.1 Definitionen“ Absatz 48 (neue Nummerierung) „Redundanzgruppe“

Präzisierung.

Zu „2.1 Definitionen“ Absatz 49 (neue Nummerierung) „Rückwirkungsfreiheit“ Hinweis (neu)

Es wurde ein Hinweis ergänzt, der eine „nicht unzulässige Beeinflussung“ erläutert.

Zu „2.1 Definitionen“ Absatz 50 (neue Nummerierung) „Schutzaktion“

Der Begriff wurde aus den SiAnf Anhang 1 übernommen, allerdings wurde der Halbsatz: „*die zur Beherrschung von Ereignissen erforderlich sind“* in *„die zur Beherrschung von Störfällen erforderlich sind“* geändert, da ansonsten der KTA-spezifische Anwendungsbereich verlassen wird. Einige Ereignisse werden nicht durch den Reaktorschutz beherrscht. (z.B. FLAB, deren Auswirkungen können nur gemindert werden.)

Zu „2.1 Definitionen“ Absatz 51(neue Nummerierung) „Schutzaktion, eindeutig sicherheitsgerichtete“

Präzisierung.

Zu „2.1 Definitionen“ Absatz 52 (neue Nummerierung) „Schutzaktion, nicht eindeutig sicherheitsgerichtete“

Präzisierung.

Zu „2.1 Definitionen“ Absatz 53 (neue Nummerierung) „Schutzbegrenzung“

Hinweis auf veralteten Begriff.

Zu „2.1 Definitionen“ Absatz 56 (neue Nummerierung) „Schutzüberbrückung“ Hinweis

Die Beispiele für Schutzüberbrückungen wurden reduziert auf die Anfahrüberbrückung.

Zu „2.1 Definitionen“ Absatz 60 (neue Nummerierung) „Sicherheitsabstand“

Der Begriff muss für diese Regel präziser gefasst werden, als in den SiAnf Anhang 1 vorgesehen. Der ursprüngliche Regeltext bildet dies adäquat ab und wurde deshalb beibehalten.

Zu „2.1 Definitionen“ Absatz 61 (neue Nummerierung) „Sicherheitseinrichtung, aktive“

Der Begriff wurde nicht wortgleich aus den SiAnf Anhang 1 übernommen. Die Präzisierung, dass es sich um eine „technische“ Einrichtung handeln muss, ist an dieser Stelle korrekt und sollte nicht verloren gehen.

Zu „2.1 Definitionen“ Absatz 62 (neue Nummerierung) „Sicherheitssystem“

Der Begriff wurde nicht wortgleich aus den SiAnf Anhang 1 übernommen. Mit der Definition aus den SiAnf würden alle Sicherungsanlagen dem Sicherheitssystem zugeordnet, die jedoch nicht in der Zielsetzung der KTA 3501 liegen. Die ursprüngliche KTA-Definition wurde deshalb beibehalten.

Zu „2.1 Definitionen“ Absatz 64 (neue Nummerierung) „Sicherheitsvariable“

Der Begriff nicht wortgleich aus den SiAnf Anhang 1 übernommen. Die Definition in den SiAnf Anhang 1 greift zu kurz (Die Sicherheitsvariable kann auch eine Rechengröße sein). Die ursprüngliche Definition präzisiert die Definition aus den SiAnf und steht nicht im Widerspruch zu ihr.

Zu „2.1 Definitionen“ Absatz 66 (neue Nummerierung) „Störfall“

Die neue Definition wurde aus den Sicherheitsanforderungen (SiAnf) übernommen.

Zu „2.1 Definitionen“ Absatz 55 (alt) „Störung“

Die Definition wurde gestrichen, da der Begriff in zwei unterschiedlichen Bedeutungen in der Regel verwendet wird:

1. wie in der ehemaligen Definition angegeben als Fehlverhalten eines Bauelements
2. Störung im Sinne der Zuordnung zu Ereignissen der Sicherheitsebene 2.

Die jeweilige Bedeutung ergibt sich aus dem Kontext. Auf eine Definition kann deshalb verzichtet werden. Weiterhin würde die alte Definition im Widerspruch zu den SiAnf stehen.

In den SiAnf wird Störung folgendermaßen definiert:

> *Ereignis* bzw. Ereignisablauf, dessen Eintreten während der Betriebsdauer der Anlage häufig zu erwarten ist, für den die Anlage ausgelegt ist oder für den bei der Tätigkeit vorsorglich *Maßnahme*n und *Einrichtung*en vorgesehen sind und nach dessen Eintreten der Betrieb der Anlage oder die Tätigkeit fortgeführt werden kann (*Sicherheitsebene* 2). Synonyme: *Anomaler Betrieb*, gestörter *Betriebszustand*.

Zu „2.1 Definitionen“ Absatz 67 „Validierung“ (neu)

Die Definition wurde eingeführt, um Anforderungen an den Softwareentwicklungsprozess stellen zu können. Für die Erstellung wurde die DIN EN 60880 herangezogen.

Der Begriff *Systemvalidierung* wurde durch *Validierung* ersetzt. Die Validierung wird in KTA 3501 in einem anderen Kontext verwendet und weicht deshalb von der Definition in den SiAnf Anhang 1 ab. (s. a. Phasenmodell, Verifikation). Die Definition wurde deshalb beibehalten und der Systembezug weggelassen.

Zu „2.1 Definitionen“ Absatz 68 „Verifikation“(neu)

Die Definition wurde eingeführt, um Anforderungen an den Softwareentwicklungsprozess stellen zu können. Für die Erstellung wurde die DIN EN 60880 herangezogen.

Der Begriff Verifikation wird in KTA 3501 in einem anderen Kontext verwendet und weicht deshalb von der Definition in den SiAnf Anhang 1 ab (s. a. Validierung). Die Definition wurde deshalb beibehalten.

Zu „2.1 Definitionen“ Absatz 70 „Versagen“ (neu)

Der Begriff wurde aus den SiAnf Anhang 1 übernommen.

Mit einem Ausfall kann gleichzeitig ein Versagen auftreten, muss aber nicht. Zum Beispiel kann ein Aggregat, das nicht angefordert wird, ausgefallen sein, versagen wird es erst, wenn es angefordert wird und seine Funktion nicht mehr erbringt. Zur Verdeutlichung des Unterschiedes zwischen Ausfall und Versagen wurde die Definition „Versagen“ aus den SiAnf Anhang 1 eingefügt.

Zu „2.1 Definitionen“ Absatz 75 (neue Nummerierung) „Zustandsbegrenzungen“ Hinweis

Hinweis auf veralteten Begriff .

Zu Bild 2-1

Bei der „logischen Verknüpfungsschaltung“ wurde der Plural verwendet. Weiterhin wurde die Position und der Gebrauch der „Einzelantriebssteuerung“ als missverständlich angesehen und entsprechend verschoben.

Zu „2.2 Kategorisierung der Funktionen der Sicherheitsleittechnik“

Die Einrichtungen der Sicherheitsleittechnik führen Leittechnik-Funktionen unterschiedlicher sicherheitstechnischer Bedeutung aus. Entsprechend ihrer sicherheitstechnischen Bedeutung sind die Leittechnik- Funktionen in unterschiedliche Kategorien einzuordnen, für die abgestufte Sicherheitsanforderungen gelten. In der folgenden Tabelle sind die Vorschriften aus den unterschiedlichen Regelwerken einander gegenüber gestellt und verglichen worden:

KTA 3501		**DIN IEC 61226**		**RSK - Leitlinien**		**Sicherheitsanforderungen Modul 5**	
Kat.		Kat.	Definition (Stand 2005-09)	Kat.	Definition	Kat.	Definition
A	Die Leittechnik-Funktionen der Kategorie A umfassen alle Funktionen, die erforderlich sind, um Störfälle zu beherrschen. Hinweis: Im Reaktorschutzsystem werden Leittechnik-Funktionen der Kategorie A ausgeführt, Klasse S Meldungen werden noch diskutiert.	A	In Kategorie A werden die Funktionen eingestuft, die eine grundsätzliche Rolle für die Erreichung und Beibehaltung der Sicherheit des Kernkraftwerks spielen, weil sie verhindern, dass Auslegungsereignisse zu unzulässigen Folgen führen.	1	Die Leittechnikfunktionen der Kategorie 1 umfassen alle Funktionen, die erforderlich sind, um nichttolerable Auswirkungen der Störfälle zu verhindern.	A	Die Leittechnikfunktionen der Kategorie A umfassen alle Funktionen, die erforderlich sind, um Ereignisse der Sicherheitsebene 3 zu beherrschen.
B	Die Leittechnik-Funktionen der Kategorie B umfassen alle Funktionen, die erforderlich sind, um die Ausweitung einer Störung zu einem Störfall zu verhindern. Hinweis: Z. B. „Schutzbegrenzungen“ (Zustandsbegrenzungen werden noch diskutiert)	B	In der Kategorie B werden Funktionen eingestuft, die für Erreichung und Beibehaltung der erforderlichen Sicherheit des Kernkraftwerks eine ergänzende Rolle zu den Funktionen der Kategorie A spielen (verhindern der Ausweitung einer Störung auf einen Störfall). Wenn eine Funktion der Kategorie B wirksam ist, kann die Notwendigkeit entfallen, eine Funktion der Kategorie A anzuregen.	2	Die Leittechnikfunktionen der Kategorie 2 umfassen alle Funktionen, die erforderlich sind, um die Ausweitung einer Störung auf einen Störfall zu verhindern. (*Bei Ausfall dieser Leittechnik-Funktionen sind nur geringe Schadensauswirkungen zu erwarten)	B	Die Leittechnikfunktionen der Kategorie B umfassen alle Funktionen, die erforderlich sind, um Ereignisse der Sicherheitsebene 2 zu beherrschen sowie das Eintreten von Ereignissen der Sicherheitsebene 3 zu vermeiden.
C	Die Leittechnik-Funktionen der Kategorie C umfassen alle übrigen Leittechnik-Funktionen von Systemen mit sicherheits-technischer Bedeutung. Hinweis: Leittechnik-Funktionen der hier zu berücksichtigenden Systeme sind z. B. Klasse 1 Meldungen des Reaktorschutzsystems.	C	In Kategorie C werden Funktionen eingestuft, die eine unterstützende oder indirekte Rolle bei der Erreichung und Erhaltung der erforderlichen Sicherheit des Kernkraftwerks spielen. Kategorie C umfasst Funktionen, die eine sicherheitstechnische Bedeutung haben, aber nicht in Kategorie A oder Kategorie B einzuordnen sind.	3	Die Leittechnikfunktionen der Kategorie 3 umfassen alle übrigen Funktionen mit sicherheitstechnische Bedeutung. (*Funktionen dieser Einrichtungen sind z.B. Teile der Störfall- und der Strahlenschutzinstrumentierung)	C	Die Leittechnikfunktionen der Kategorie C umfassen alle übrigen Funktionen mit sicherheitstechnischer Bedeutung.

Sicherheitsebenen	
Ebene	Definition
4 a/b/c	a: sehr seltene Ereignisse b: Ereignisse mit Mehrfachversagen von Sicherheitseinrichtungen c: Unfälle mit schweren Kernschäden
3	Störfälle
2	Anomaler Betrieb (bestimmungsgemäßer Betrieb)
1	Normalbetrieb (bestimmungsgemäßer Betrieb)

Nach Überprüfung der in der Tabelle angegebenen Kategorisierungsvorschriften, erfolgte eine erste Festlegung in Anlehnung an die RSK-Leitlinien.

Es hat sich weiterhin gezeigt, dass diese Definitionen nicht abdeckend hinsichtlich aller Anforderungen sind. Deshalb wurden zunächst zusätzlich Zustands- und Schutzbegrenzungen in die Kategorisierung einbezogen. Die Abschnitte 4.11 Schutzbegrenzungen und 7 Zustandsbegrenzungen konnten deshalb entfallen.

Die Kategorisierung wurde aber schließlich aus den Interpretationen der SiAnf I-3, Abschnitt 2 übernommen, die die RSK-Leitlinien ersetzen sollen. Die Sicherheitsebenen wurden inhaltlich übernommen und durch etablierte Begriffe ersetzt, die in den SiAnf definiert sind. Die ursprünglich formulierten Ausnahmen in Kategorie B sollten sich aus der geforderten Analyse in 3.1 (1) ergeben und wurden deshalb gestrichen.

Zu „3 Ermittlung der Aufgabenstellung“

Alter Titel „3 Ermittlung der Aufgabenstellung für das Reaktorschutzsystem“

Die Überschriften der Abschnitte 3, 4 und 5 wurden vereinfacht. Wie in der Definition von Reaktorschutz und Bild 2-1 erläutert ist die Sicherheitsleittechnik nur Teilmenge des Reaktorschutzes. Auf die Verwendung von Reaktorschutz wurde verzichtet, da der Reaktorschutz an dieser Stelle nicht eineindeutig ist.

Zu „3.1 Grundsätzliche Anforderungen“ Absatz 1 (neu)

Der alte Abschnitt wurde, dem Anwendungsbereich entsprechend, als neuer Absatz 1 überarbeitet. Die sporadische Beschreibung der geforderten Störfallanalyse wurde gestrichen (Satz 2) und der vorletzte Satz (Satz 3) wurde ergänzt, um klarzustellen welche Dokumente als Ergebnis der Analyse erwartet werden.

Die geforderte Analyse wurde auf Handmaßnahmen erweitert, um bei der Kategorisierung nach 2.2 nicht alle Handmaßnahmen zur langfristigen Störfallbeherrschung der Kategorie A zuzuordnen.

Zu „3.1 Grundsätzliche Anforderungen“ Absatz 2 (neu)

Der Absatz stammt aus „4.13 Ermittlung der Grenzwerte zur Auslösung von Schutzaktionen“ (alt) Absatz 1 und wurde als grundlegend eingestuft. Der neu eingefügte Absatz wurde redaktionell überarbeitet. Der Abschnitt 4.13 konnte entfallen, da auch der 2. Absatz verschoben wurde.

Zu „3.1 Grundsätzliche Anforderungen“ Absatz 3 (neu)

Die aus Absatz 3 des Abschnittes „4.1.8 Abstimmung zwischen den A-Funktions-Einrichtungen und den aktiven Sicherheitseinrichtungen“ (alt 4.9) stammenden Anforderung wurde als grundlegend eingestuft und deshalb an diese Stelle verschoben.

Zu „3.1 Grundsätzliche Anforderungen“ Absatz 4 (neu)

Der Absatz stammt aus „4.13 Ermittlung der Grenzwerte zur Auslösung von Schutzaktionen“ (alt) Absatz 2. Er wurde als grundlegend eingestuft und an diese Stelle verschoben. Der neu eingefügte Absatz wurde redaktionell überarbeitet. Der Abschnitt 4.13 konnte entfallen, da auch der 2. Absatz verschoben wurde.

Zu „3.2 Ereignisabläufe und ihre Auswirkungen“ Absatz 1

Es werden die in Betracht zu ziehenden Ereignisse behandelt, die ebenfalls im Anhang 2 der SiAnf angegeben werden. Deshalb wurden diese durch Verweise auf Anhang 2 der SiAnf ersetzt. Die Tabelle 5-3 des Anhanges 2 der SiAnf wurde ausgeschlossen, da sie die Ereignisliste für Ereignisse enthält, die die Brennelement-Lagerbeckenkühlung betreffen. Diese liegen nicht im Anwendungsbereich der KTA 3501.

Zu „3.2 Ereignisabläufe und ihre Auswirkungen“ Absatz 2

Resultierende redaktionelle Anpassung aus den Änderungen in Absatz 1.

Zu „3.3 Ausgangszustand der Anlage“

Der missverständliche letzte Satz des Abschnittes wurde umformuliert. Inhaltlich wurde am alten Regeltext nichts verändert

Der Satz 3 wurde so umformuliert, dass in der Analyse ein Einzelfehler in der Leittechnik Auswirkungen auf die verfahrenstechnische Anwendung haben kann und analysiert werden muss z. B. die Leistungsdichteverteilung (Begrenzung).

Zu „3.4 Erfassung der Störfälle“ Absatz 2 Hinweis (neu)

Die Anforderung in diesem Absatz wird in Absatz 1 von *4.1.4.2 Festlegung der Anregekriterien* wiederholt. Der Absatz 1 von 4.1.4.2 wurde deshalb gestrichen und der Hinweis an diese Stelle verschoben.

Zu „3.4 Erfassung der Störfälle“ Absatz 3 (neu)

Der Absatz wurde aus 4.1.4.2 (2) verschoben. Der Abschnitt 4.1.4.2 kann deshalb entfallen.

Zu „4 Auslegungsgrundlagen“

Alter Titel „4 Auslegungsgrundlagen für das Reaktorschutzsystem“

Der Abschnitt wurde aufgrund des umformulierten Anwendungsbereiches und gemäß der Kategorisierung nach 2.2 neu strukturiert. Der Abschnitt 4.1 (alt 4) stellt Anforderungen an A-Funktions-Einrichtungen ursprünglich Reaktorschutz. Der Abschnitt 4.2 wurde neu hinzugefügt und gilt speziell für B-Funktions-Einrichtungen. Die Abschnitte 4.3 Änderungen an der Sicherheitsleittechnik und Abschnitt 4.4 IT-Sicherheit sind neu hinzugefügt worden und gelten für A- und B-Funktions-Einrichtungen.

Ein weiterer Abschnitt für Auslegungsanforderungen an C-Funktions-Einrichtungen war zunächst geplant wurde dann aber aufgrund eines Beschlusses des UA-EL auf seiner 68.Sitzung fallen gelassen. Der UA-EL hielt eine Erweiterung auf alle Einrichtungen, die Leittechnikfunktionen der Kategorie C ausführen, wie zum Beispiel: Hebezeuge, Strahlungsinstrumentierung oder Kommunikationseinrichtungen für problematisch. Der ursprüngliche Anwendungsbereich der KTA 3501 durfte nach Beschluss des UA-EL nicht erweitert werden.

Die Überschriften der Abschnitte 3, 4 und 5 wurden vereinfacht. Wie in der Definition von Reaktorschutz und Bild 2-1 erläutert ist die Sicherheitsleittechnik nur Teilmenge des Reaktorschutzes. Auf die Verwendung von Reaktorschutz wurde verzichtet, da der Reaktorschutz an dieser Stelle nicht eineindeutig ist.

Zu „4.1 Auslegungsanforderungen an A-Funktions-Einrichtungen“

Basis für diesen Abschnitt war der Abschnitt „4 Auslegungsgrundlagen für das Reaktorschutzsystem“ der Fassung 1985-06. Der Abschnitt wurde auftragsgemäß mit Anforderungen an rechnerbasierte Leittechnik ergänzt.

Zu „4.1.1 Grundsätzliche Anforderungen“ Absatz 1+2+3

Der ursprüngliche Absatz 1 wurde aufgeteilt in Absatz 1 und 2.Die Absätze mussten angepasst werden, da in den SiAnf die Einwirkungen von innen (EVI) und Einwirkungen von außen (EVA) neu definiert wurden. Zivilisatorisch bedingte Einwirkungen, wie Flugzeugabsturz oder Explosionsdruckwelle werden in den SiAnf zu den Notstandsfällen gerechnet. Aus diesem Grund wurden die Einwirkungen von innen und außen, die im KTA anders definiert werden hinzugefügt. Es wird davon ausgegangen, dass EVI und EVA Störfälle verursachen, die dann den zu unterstellenden Störfall nach 4.1.3.1 abdecken. Im Absatz 3 wurde die Formulierung aus der Fassung 1985 beibehalten. Sollte ein versagensauslösendes Ereignis aus 4.1.2.1 oder 4.1.2.2 einen Störfall auslösen (abhängiger Störfall), so muss kein weiterer Störfall unterstellt werden. Es muss jedoch ein zusätzliches versagensauslösendes Ereignis entweder als Zufallsausfall oder als systematischer Ausfall unterstellt werden. An dieser Stelle wäre die Ergänzung wie in Absatz 1 nicht korrekt.

Zu „4.1.1 Grundsätzliche Anforderungen“ Absatz 2 (alt 4.1)

- Vertreter der RSK: Eine Überlagerung von auslösenden Ereignissen werde nur unterstellt, wenn ein kausaler Zusammenhang bestehe oder wenn das gleichzeitige Auftreten aufgrund der Wahrscheinlichkeit und des Schadensausmaßes in Betracht zu ziehen sei. Unabhängig davon werde die Trennung der Redundanzen gefordert, so dass bei anlageninternen Ereignissen nur eine Redundanz betroffen wäre. (s. a. Anhang 1)

- AG: In Abschnitt 4.1.1 werden grundsätzliche Auslegungsanforderungen an das Sicherheitssystem gestellt:

1. Das Sicherheitssystem müsse nichttolerierbare Auswirkungen von Störfällen und Einwirkungen von innen und außen verhindern.

2. Das Auftreten eines der benannten versagensauslösenden Ereignisse und deren Auswirkungen auf eine leittechnische Funktion dürfe nicht dazu führen, dass im Anforderungsfall (Störfall) das Sicherheitssystem versagt.

Die angesprochene Forderung nach räumlicher Trennung von Redundanzen sei nur eine Maßnahme aus einem Strauß von Maßnahmen, die sich aus diesen Auslegungsprinzipien ableiten. Die harte Forderung nach räumlicher Trennung von Redundanzen sei nicht immer nötig (z. B. LT0, Redundanzgruppen) bzw. nicht immer möglich (FSA-Station). Ein Brand an einer beliebigen Stelle sei Teil der Analyse und sollte beherrscht werden, die Störfallbeherrschung dürfe nicht eingeschränkt werden. Entweder werde der Brand zugelassen, da die Einrichtung eindeutig sicherheitsgerichtet auslöse, oder der Brand werde beherrscht durch Brandschutzmaßnahmen (z. B. Löschanlage), Redundanztrennung.

Zu „4.1.1 Grundsätzliche Anforderungen“ Absatz 3 (alt 4.1) Hinweis 2 und 3

Hier erfolgt eine Abgrenzung des „Auslegungsbrandes“ gegenüber dem „auslegungsüberschreitenden Brand“ (redundanzübergreifenden Brandes). Der UA-PG wies darauf hin, dass es in der KTA 2201.1 und KTA 3501 missverständliche Formulierungen gäbe, die beispielsweise durch die Streichung des Hinweises in der Begriffsdefinition von „systematischer Ausfall“ in der KTA 3501 bereinigt werden könnten. Der im UA-PG angesprochene Widerspruch zur KTA 2101.1 bestand darin, dass bei den anzunehmenden Ausfallkombinationen der unabhängige redundanzübergreifende Brand als systematischer Ausfall betrachtet werden muss.

Die vom UA-PG vorgeschlagene Streichung des Hinweises löst, nach Ansicht des Arbeitsgremiums, die Mehrdeutigkeiten nicht auf. Die bestehende Formulierung in der KTA 3501, welche Fälle bei den Ausfallkombinationen zu unterstellen sind und welche nicht wurden durch die ergänzten Hinweise konkretisiert.

zu „4.1.2 Versagensauslösende Ereignisse (alt 4.2)

zu „4.1.2.1 Versagensauslösende Ereignisse innerhalb der A-Funktions-Einrichtungen (alt 4.2.1)

Alter Titel „4.2.1 Versagensauslösende Ereignisse innerhalb des Reaktorschutzsystems“

Die beispielhaft genannten, in Betracht zu ziehenden versagensauslösenden Ereignisse wurden, um die Belange der rechnerbasierten Leittechnik sowie der elektromagnetischen Beeinflussung EMB ergänzt.

zu „4.1.2.2 Versagensauslösende Ereignisse innerhalb der Reaktoranlage“ (alt 4.2.2) Hinweis

Im Hinweis wurde die elektromagnetischen Beeinflussung EMB als Beispiel für versagensauslösende Ereignisse innerhalb der Reaktoranlage ergänzt. Die explizite Nennung erfolgt aufgrund der rechnerbasierten Leittechnik. Weiterhin wurde der Verweis auf die „Interpretationen der Sicherheitskriterien (Einzelfehlerkonzept)“ ersetzt durch einen Verweis auf die SiAnf Anhang 4.

zu „4.1.2.3 Auslegung gegen versagensauslösende Ereignisse außerhalb der Reaktoranlage“ (alt 4.3)

Die Netzstörungen wurden aufgrund des Erfahrungsrückflusses aus dem Forsmark-Ereignis neu aufgenommen. Der Begriff „Erdbeben“ wurde präzisiert in „induzierte Erschütterungen“. Der Brand wurde neu aufgenommen, da er auch außerhalb der Reaktoranlage Auswirkungen auf die Sicherheitsleittechnik haben kann. Weiterhin wurde ein Verweis auf den Abschnitt 2.4 „Schutzkonzept gegen Einwirkungen von innen und außen sowie gegen Notstandsfälle“ der SiAnf aufgenommen.

zu „4.1.3 Ausfallkombinationen“ (alt 4.4)

zu „4.1.3.1 Grundannahmen“ Absatz 2 (alt 4.4.1) Hinweis

Der Hinweis, dass der Zufallsausfall auch durch versagensauslösende Ergebnisse verursacht werden kann, wurde ergänzt.

zu „4.1.3.1 Grundannahmen“ Absatz 3 (alt 4.4.1)

Der Absatz wurde an die Formulierung aus den Interpretationen der SiAnf I-3, 3.2 (12) angepasst.

zu „4.1.3.1 Grundannahmen“ neuer Absatz 4 (alt 4.4.1)

Berücksichtigung selbstüberwachender Maßnahmen bei der Ausfallkombination.

Die Anforderung öffnet eventuell für alle Architekturen den Abzählreim (soll eigentlich nur für 2 von 2 Struktur (AA, BB) gelten), deshalb wurde ein Hinweis darauf ergänzt.

Die Fehlerüberwachung soll sicherstellen, dass die Unverfügbarkeit aufgrund von Ausfällen so gering wird, dass der systematische Ausfall zusammen mit dem Zufallsausfall nicht mehr gleichzeitig unterstellt werden muss. Kurze Instandsetzungszeiten können nur bei Zufallsausfällen erreicht werden. Bei „unbekannten“ systematischen Ausfällen kann keine Aussage über die Instandsetzungszeit getroffen werden. Der Absatz wurde mehrheitlich angenommen.

Gradic stimmt gegen die Aufnahme des neuen Absatzes und begründet dies folgendermaßen:

1.) Die gemäß Bild 4-1 anzuwendende Ausfallkombination „S & I“ werde nicht beherrscht (Wenn (S) nach Absatz (6) ausgeschlossen wäre, wäre Absatz (4) überflüssig.).

2.) Die Voraussetzung a) sei sehr unspezifisch, da der Grad der Fehlerselbsterkennung nicht nur von der Anzahl der „erkennbaren Fehler“ abhänge.
In jedem Fall sei die Fehlerselbsterkennung bei einer Struktur mit 2 Redundanzen in Gerätetechnik A und 2 Redundanzen in dissimilarer Gerätetechnik B im Vergleich zu einem homogenen 4-fach redundanten System im Verarbeitungsteil deutlich eingeschränkt. Durch das unterschiedliche zeitliche Verhalten der verschiedenen Systeme sei eine Gleichlaufüberwachung errechneter Größen bei Transienten nicht möglich. Damit sei aber der extrem hohe Fehlerselbsterkennungsgrad nicht erreichbar. Die Ausfallwahrscheinlichkeit des Gesamtsystems (und damit der Funktion) nehme deutlich zu, denn die Wahrscheinlichkeit weiterer Ausfälle nehme mit der Zustandsdauer unerkannter Ausfälle zu.
Hier werde also eine deutliche Steigerung der Unverfügbarkeit des Sicherheitssystems in Kauf genommen (2 vollständig unabhängige und 4-fach redundante Systeme seien damit nicht notwendig), um einer „deterministischen“ Auslegung zu genügen, die jedoch auf unrealistischen Postulaten (Dissimilarität schließe den „Systematischen Fehler“ aus) beruhe.

3.) Die Beseitigung eines systematischen Fehlers könne nicht durch Instandsetzung (erst recht nicht mit kurzen Instandsetzungszeiten) behoben werden. Denn die Beseitigung eines „Systematischen Fehlers“ setzte immer eine Änderung (in einem Sicherheitssystem mit atomrechtlichem Änderungsverfahren) voraus.

zu „4.1.3.1 Grundannahmen“ Absatz 5 (alt 4.4.1 Absatz 4)

Der Instandsetzungsfall wurde durch den Instandhaltungsfall korrigiert.

zu „4.1.3.1 Grundannahmen“ Absatz 6 (alt 4.4.1 Absatz 5) Hinweis

Die Formulierung wurde aus den SiAnf 3.7 (4) übernommen. Die „Sicherheitsebene 3“ wurde, wie in Abschnitt *2.2 Kategorisierung,* durch den etablierten Begriff „Störfall“ ersetzt.

Der Hinweis unter dem Absatz 6 wurde unter Absatz 7 verschoben, da Absatz 7 sich auf Absatz 6 bezieht und beide eng miteinander verknüpft sind.

Gradic stimmt gegen die Einschränkung auf festverdrahtete Systeme im Hinweis und begründet dies folgendermaßen:

Es werde indirekt die Forderung nach diversitärer oder dissimilarer Technik bei Einsatz rechnerbasierter Leittechnik verstärkt. Dies sei jedoch wie nachfolgend dargelegt nicht begründet.

1.) Der Nachweis das Gerätesysteme dissimilar zueinander sind, sei weder vollständig möglich noch sinnvoll quantifizierbar. Einerseits sei der analytische Nachweis, dass gleiche Schaltungsteile in verschiedenen hochintegrierten Bauelementen oder gleiche Softwareteile in der Systemsoftware nicht vorhanden sind, praktisch nicht möglich. Andererseits sei es gerade bei hochintegrierter Elektronik wahrscheinlich, dass z.B. durch Mitarbeiterwechsel oder Kauf von Patenten gleiche Hardwareschaltungen oder Softwarealgorithmen in verschiedenen Komponenten vorhanden sind. Dissimilare (oder diversitäre) Technik könne deshalb den CCF nicht deterministisch ausschließen.(Darüber hinaus zeige die Erfahrung, dass unabhängige Entwicklungsteams gleiche Fehler gemacht haben)

2.) Wirksame Maßnahmen gegen einen CCF (common cause failure = Ausfall mit gemeinsamer Ursache) zu treffen, sei deshalb schwierig, weil apriori nicht klar sei, wie der CCF aussieht. Sowohl in hochintegrierten Bauelementen oder komplexer Systemsoftware, aber auch in den festverdrahteten Leittechniksystemen mit über 100 Schränken und aufwendiger Verkabelung seien Fehler nicht ausgeschlossen. Dabei könne es sich jedoch nicht um triviale Fehler handeln, denn diese würden die allgemeine Funktionsweise dieser Systeme unmöglich machen oder bei den durchzuführenden Prüfungen der Grundfunktionen aufgedeckt werden. Vielmehr könne es sich nur um sehr spezifische Fehler handeln, die ausschließlich bei ganz bestimmten Signalkombinationen an den Eingängen der Bauelemente in Verbindung mit bestimmten Speicherstellungen (z.B. Register im Steuerwerk oder Rechenwerk eines Prozessors) Auswirkungen haben können. Damit würden die Forderungen zur Beherrschung von CCF bei komplexen Leittechniksystemen erkennbar. Es müsse verhindert werden, dass zueinander redundante Leittechnik (egal ob dissimilar, oder diversitär oder homogen) an den Verarbeitungseingängen die gleichen Bitkombinationen anliegen haben. Dies könne dadurch erreicht werden, dass Rechner keine gleiche (absolute) Uhrzeit führen dürfen und keine andere Art der Synchronisierung zwischen den redundanten Rechnern erfolgt und jede Redundanz ihre eigene analoge Signalerfassung hat. Die Rechner müssen möglichst unabhängig voneinander laufen (wie dies im internationalen Regelwerk gefordert werde). Ihre Kopplung erfolge ausschließlich über die Kraftwerksanlage. Unter diesen Bedingungen seien bitgleiche Signalzustände in den redundanten Verarbeitungseinheiten ausgeschlossen. Darüber hinaus seien weitere rechnerspezifische Forderungen zu erfüllen, wie z.B. keine Verarbeitung externer Interrupts, die durch den Kraftwerksanlagenzustand ausgelöst werden können. Durch diese Maßnahmen werde das Triggern von Ereignissen, die zum gleichzeitigen Wirksam werden von möglicherweise vorhandenen nicht trivialen Fehlern führen könnten, ausgeschlossen. Diese Maßnahmen seien in jedem Fall notwendig, auch bei Einsatz dissimilarer Gerätetechnik. Insofern sei der Einsatz dissimilarer Gerätetechnik allein nicht hinreichend.

3.) Wenn die unter 2.) genannten Forderungen an ein rechnerbasiertes Sicherheitsleittechniksystem erfüllt sind, sei Dissimilarität (oder Diversität) nicht mehr notwendig.

4.) Die Komplexität eines Leittechniksystems sei nicht nur von der Komplexität einzelner Baugruppen abhängig, sondern auch von der Art der Zusammenschaltung (also der Struktur) und dem Automatisierungsgrad. Die meisten Baugruppen rechnerbasierter Leittechnik seien komplexer als die verdrahtungsprogrammierter Leittechnik. Sie hätten jedoch den Vorteil als Standardkomponenten während und nach der Herstellung standardisiert und anwendungsunabhängig intensiv geprüft zu werden. Die Baugruppenvielfalt und die Anzahl benötigter Baugruppen sei geringer. Die Struktur der zum Gesamtsystem zusammengeschalteten Baugruppen sei einfacher. Die größere Komplexität sei auf der Gesamtsystemebene nicht mehr gegeben. Die CCF-Problematik bei der erfolgreich eingesetzten „Verdrahtungsprogrammierten binären und analogen Leittechnik“ sei ebenfalls vorhanden. Hierbei werde die projektierte Funktionalität (dies sei ebenfalls Software, die falsch sein könne) durch Verdrahtung der funktionsbezogenen Baugruppen in Baugruppenträgern, Schränken und durch Verkabelung zwischen den Schränken erreicht. Es wären für deutsche Reaktorschutzsysteme über hundert Schränke notwendig, die über eine Millionen Rangierpunkte und Kabelanschlusspunkte aufweisen. Dabei sei ein Stromversorgungs- und Schirmungskonzept konsequent umzusetzen, ansonsten wäre die redundanzüberschreitende elektromagnetische Verträglichkeit nicht gewährleistet. So ein System sei ebenfalls nicht vollständig prüfbar. Vollständig geprüft würde heißen, es müssten alle Eingangssignalkombinationen unter Berücksichtigung der im System vorhandenen Speicher vorgegeben werden, um die sich einstellenden Ausgangssignalkombinationen mit den erwarteten Ausgangssignalkombinationen zu vergleichen. Tatsächlich würden mit Sachverstand und Erfahrung „überlappende“ Prüfungen ausgewählt. Dabei werde jedoch unterstellt, dass die Geräte und Bauelemente innerhalb ihrer Toleranzgrenzen spezifikationsgerecht funktionieren. Es werde aber nicht geprüft, ob die realen Impedanzen und die realen Bauteiltoleranzen des zusammen geschalteten Systems in allen Signalkombinationen funktionieren. Es sei auch hierbei zu unterstellen, dass „nicht triviale“ Fehler vorhanden wären, die sich aufgrund des hohen Redundanzgrades, der Unabhängigkeit der Redundanzen, der konservativen Auslegung und der daraus resultierenden Systemrobustheit nicht zutage treten und sich auch zukünftig höchstens als Einzelfehler auswirken würden.

5.) Die Auswirkungen von Einzelfehlern auf das Gesamtsystemverhalten seien bei dissimilarer Technik schwieriger vorhersagbar. Damit nehme die Gefahr von Fehldiagnosen oder Fehlinterpretationen zu. Das notwendige Wissen zur Statusbeurteilung des Gesamtsystems nehme deutlich zu. Die Forderung nach dissimilaren Instandhaltungsteams stehe dem diametral entgegen. Die Gefahr von Fehlhandlungen durch unergonomische, weil unterschiedliche Bedienoberflächen für die Instandhaltung nehme zu. Die Auswertung der weltweiten Erfahrungsrückflüsse aus Kernkraftwerken unter den Aspekten „Ereignisse mit gravierenden Folgen“ oder „Ereignisse mit CCF-Potenzial“ zeige als wichtigste Ursachen:

   1. Fehlerhafte Anforderungsspezifikation (auch Fukushima-Daiichi).
   2. Fehlerhafte leittechnische Umsetzung der verfahrenstechnischen Anforderungen.
   3. Menschliche Fehlhandlungen bei der Bedienung der Anlage in besonderen Situationen. Dies gelte insbesondere bei den ausländischen Anlagen, deren Bedienphilosophie eine höhere Priorität der

menschlichen Bedienung gegenüber dem Reaktorschutzsystem einräume und bei denen der Automatisierungsgrad des Reaktorschutzsystems deutlich kleiner sei als bei deutschen Anlagen.

4. Menschliche Fehlhandlungen bei der Instandhaltung aufgrund nicht verstandener technischer Zusammenhänge

Diese Ursachen würden durch den Einsatz dissimilarer oder diversitärer Gerätetechnik im Verarbeitungsteil der Sicherheitsleittechnik nicht beseitigt, sondern tendenziell eher verstärkt. Darüber hinaus sei kein einziger Fall bekannt, bei dem ein gerätetechnisch bedingter CCF in einem deutschen Kernkraftwerk tatsächlich zum gleichzeitigen Ausfall von zueinander redundanten Funktionen geführt hätte. Alle gerätetechnisch bedingten Fehler hätten sich immer als Einzelfehler ausgewirkt (z.B. Whisker).

6.) Die Fehlerselbsterkennung sei eine wichtige Eigenschaft der Sicherheitsleittechnik. Die Zuverlässigkeitskenngrößen „Verfügbarkeit“, „Mittlere Zeit zwischen Ausfällen“ und „Ausfallzeit“ der Sicherheitsleittechnik würden sich überproportional verschlechtern, wenn der Grad der Fehlerselbsterkennung abnehme. Dies ließe sich z.B. mit Zuverlässigkeitsberechnungen mit Hilfe von Markow-Ketten zeigen. Zur Fehlerselbsterkennung würden verschiedene Mechanismen wie dynamische Arbeitsweise, Speichertests, Spannungs- und Stromüberwachungen, etc. verwendet. Damit ließen sich Fehlerselbsterkennungsgrade von maximal 80% bis 90% aller Fehler erreichen. Wenn jedoch ein Fehlerselbsterkennungsgrad von >90% angestrebt werde (wie dies bei den derzeitigen Reaktorschutzsystemen in Deutschland der Fall sei), sei dies nur durch Vergleich von zueinander redundanten Messsignalen und errechneten Größen möglich. (Dies diene nicht zur Synchronisation, sondern zur Fehlererkennung.) Dissimilare Systeme hätten jedoch grundsätzlich ein so unterschiedliches zeitliches Verhalten bei Anlagentransienten, dass diese Vergleichermeldungen entweder bei Anlagentransienten unterdrückt werden müssten, oder ständig ansprechen würden. Die „Gleichlaufüberwachung“, um einen extrem hohen Fehlerselbsterkennungsgrad zu erreichen, sei praktisch nur bei homogenen, zueinander redundanten Systemen möglich.

Dissimilarität als das deterministische Mittel gegen das gleichzeitige Versagen von redundanten, rechnerbasierten Einrichtungen im Verarbeitungsteil des Reaktorschutzsystems anzusehen, sei nicht begründet sondern ein Postulat, das empirisch nicht bestätigt werden könne.

zu „4.1.3.1 Grundannahmen“ neuer Absatz 7 (alt 4.4.1)

Der Absatz wurde aus dem 2.Absatz der Interpretationen der SiAnf, I-3, 3.2 (11) abgeleitet. Die Bedingung für die Anwendung dieses Absatzes wurde allgemeiner gefasst und bezieht sich jetzt nicht mehr nur auf rechnerbasierte oder programmierbare leittechnische Einrichtungen.

zu „4.1.3.1 Grundannahmen“ neuer Absatz 7 (alt 4.4.1) Hinweis

Zur Abstufung von festverdrahteten und rechnerbasierten Einrichtungen wurde der Hinweis aus Absatz 6 hierher verschoben. Unter Absatz 6 werden die Bedingungen für die Nachweisführung eines Ausschlusses von systematischem Versagen formuliert und unter Absatz 7 die Bedingungen falls dieser nicht gelingen sollte. Der letzte Satz des Hinweises:

Die Minderung der Auswirkungen kann zusätzliche Maßnahmen außerhalb der A-Funktions-Einrichtungen erfordern.

wurde gestrichen, da, durch die Umformulierung, der Bezug zu den „Auswirkungen systematischer Ausfälle“ nicht mehr vorhanden ist.

Die im Hinweis aufgezählten Maßnahmen zur Minderung der Eintrittswahrscheinlichkeit gelten nur für festverdrahtete Systeme. Dies wurde im Hinweis ebenfalls ergänzt.

zu „4.1.3.1 Grundannahmen“ neuer Absatz 8 (alt 4.4.1)

Fehlervermeidende und fehlerbeherrschende Maßnahmen werden speziell für rechnerbasierte Systeme auftragsgemäß ergänzt.

Dissimilare leittechnische Einrichtungen wurden im Abschnitt Begriffe als Teilmenge von diversitären leittechnischen Einrichtungen definiert. Sie werden im Rahmen dieser Regel im gleichen Sinne zur Vorsorge gegen systematische Fehler/Ausfälle eingesetzt. Die Formulierung wurde deshalb im Hinweis bei der beispielhaften Aufzählung fehlerbeherrschender Maßnahmen vereinheitlicht.

Beim Einsatz von dissimilarer Leittechnik zur Beherrschung systematischer Fehler, die im Hinweis unter b) bei fehlerbeherrschenden Maßnahmen angegeben werden gibt es folgende abweichende Meinung:

Gradic: Siehe Begründung für Absatz 6 des Abschnittes 4.1.3.1.

zu „4.1.4 Anregung von Schutzaktionen“ (alt 4.5)

zu „4.1.4.2 Festlegung der Anregekriterien“ (alt 4.5.2)

Der Abschnitt wurde unter *3.4 Erfassung der Störfälle* integriert und an dieser Stelle gestrichen. Der Absatz 2 wurde in *3.4 Erfassung der Störfälle* als neuer Wickel (3) eingefügt und Absatz 1 wurde gestrichen, da er eine Wiederholung zu 3.4 Absatz 2 darstellt.

Die Fehlerselbsterkennung wurde neben einer Verkürzung der Prüfzyklen und dem Einsatz unterschiedlicher Messgeräte vorgesehen, die als Ersatzmaßnahme herangezogen werden können, sofern die Anregekriterien nicht aus verschiedenartigen Prozessvariablen ableitbar sind.

Der Hinweis weist noch einmal auf den Stellenwert der Fehlerselbsterkennung hin.

zu „4.1.4.2 Automatisierungsgrad“ neuer Absatz 2 (alt 4.5.3)

Die Möglichkeit von Handmaßnahmen unabhängig von automatisierten eindeutig sicherheitsgerichteten Schutzaktionen wurde neu aufgenommen. Diese Anforderung ergänzt die Anforderung aus Absatz 1 und zielt implizit auf rechnerbasierte Systeme, da bei Ausfall des rechnerbasierten Systems die notwendige Handmaßnahme immer noch möglich sein muss.

Folgende Aspekte wurden dabei diskutiert:

1.) Es handelt sich hierbei nicht um eine A- oder B-Funktion. Die Anforderung wird aber in den „Sicherheitsanforderungen für Kernkraftwerke“ 3.7 (5) abgebildet und könnte deshalb entfallen.

2.) mit dieser Formulierung können Unwägbarkeiten abgedeckt werden. Die Anforderung gehört zwar nicht zur Störfallbeherrschung, aber zur Auslegung.

3.) Der Absatz könnte im Widerspruch zum Absatz 3 des Abschnittes 5.1.7.3 Vorrangsteuerung stehen und sollte deshalb gestrichen werden. Weiterhin würde der Aufbau eines zweiten Leittechniksystems parallel zur Automatik-RESA kontraproduktiv wirken. Das Hand-RESA-Signal könnte unbemerkt vom Reaktorschutz auslösen.

zu „4.1.4.3 Protokollierung“ (alt 4.5.4)

Die Streichung des Beispiels öffnet die Möglichkeit der Nutzung neuer, besserer technischer Möglichkeiten (siehe auch KTA 3904 (2007-11)). Weiterhin wurde die geforderte Dokumentation präzisiert. (übersichtlich und in der richtigen Reihenfolge)

zu „4.1.5 Redundanz und Unabhängigkeit“ (alt 4.6) Absatz 2

Klarstellung.

zu „4.1.5 Redundanz und Unabhängigkeit“ (alt 4.6) Absatz 4 (neu)

Diese Anforderung wurde speziell für rechnerbasierte Einrichtungen eingeführt, um dem Aspekt der IT-Sicherheit Rechnung zu tragen.

zu „4.1.6 Trennung der A-Funktions-Einrichtungen von anderen Systemen“ Absätze 1, 2 und 5 (alt 4.7)

alter Titel „4.7 Trennung des Reaktorschutzsystems von anderen Systemen“

Durch die Streichung der Definition des Betriebssystems waren an dieser Stelle redaktionelle Anpassungen nötig. Unter Absatz 1 wurde weiterhin ein Hinweis ergänzt, der klarstellt, dass trotz der Erlaubnis A-Funktions-Einrichtungen auch für andere Aufgaben einzusetzen, davon möglichst wenig Gebrauch gemacht werden soll.

zu „4.1.6 Trennung der A-Funktions-Einrichtungen von anderen Systemen“ Absatz 3

Der Absatz wurde durch Interpretation der SiAnf, I-3, 3.8 (4) ergänzt. Die in den SiAnf verwendeten Begriffe „Datenverarbeitungs- oder Datenübertragungseinrichtungen“ wurde allerdings durch „leittechnischen Einrichtungen“ ersetzt, um keine neue Begrifflichkeiten einzuführen.

zu „4.1.6 Trennung der A-Funktions-Einrichtungen von anderen Systemen“ Absatz 6

Die Anforderung steht im ersten Satz. Der zweite Satz wurde gelöscht, da dieser eher einschränkenden Charakter hat und nicht alle anlagenspezifischen Gegebenheiten (z. B. Polarität, 600-V-Ebene) abdeckt. Der erste Satz wurde zusätzlich präzisiert (systemfremde Überspannungen).

zu „4.1.7 Instandhaltung“ Absatz 1 Hinweis (alt 4.8)

Der Hinweis enthält klare Anweisungen und wurde deshalb als neuer Absatz 2 eingeführt.

zu „4.1.7 Instandhaltung“ Absatz 2+3 (neu) (alt 4.8)

alter Titel „4.8 Betrieb des Reaktorschutzsystems bei Instandhaltungsarbeiten“

Der Absatz 2 war ursprünglich ein Hinweis unter dem Absatz 1. Da er klare Anweisungen und Bedingungen angibt, wurde er als Regeltext aufgenommen.

Der Absatz 3 wurde insbesondere für den Austausch von rechnerbasierten Geräten eingeführt.

zu „4.1.7 Instandhaltung“ Absatz 4 (neue Nummerierung) (alt 4.8)

alter Titel „4.8 Betrieb des Reaktorschutzsystems bei Instandhaltungsarbeiten“

Redaktionelle Anpassung, die durch die Streichung des zweideutigen Begriffes „Betriebssystem“ erforderlich war. Das Beispiel mit der Hauptkühlmittelpumpe wurde entfernt. Die Anforderung wurde klarer formuliert.

Bei enger Auslegung wäre mit der gegebenen Formulierung die Anlage abzufahren, wenn beispielsweise ein Defekt in der Verdrahtung oder auch ein zufällig erkannter Ausführungsfehler in der Verdrahtung behoben werden müsste. Deshalb wurde die unbedingt einzuhaltenden Forderung (muss) in eine bedingt einzuhaltende Forderung (soll) umgewandelt.

zu „4.1.7 Instandhaltung“ Absatz 5 (neue Nummerierung) (alt 4.8)

alter Titel „4.8 Betrieb des Reaktorschutzsystems bei Instandhaltungsarbeiten“

Der Absatz wurde durch SiAnf Anhang 4, 4 (10) mit wenigen redaktionellen Änderungen ersetzt.

zu „4.1.7 Instandhaltung“ Absatz 6 (neue Nummerierung) (alt 4.8)

alter Titel „4.8 Betrieb des Reaktorschutzsystems bei Instandhaltungsarbeiten“

Die schnelle und richtige Ausfallortung zählt zur Instandsetzung dazu und wurde deshalb gestrichen.

zu „4.1.7 Instandhaltung“ Absatz 8 (neue Nummerierung) (alt 4.8)

Der Absatz wurde gestrafft. Der Nebensatz des ersten Satzes beschreibt einen Sachverhalt der in KTA 3503 und KTA 3505 bereits geregelt ist.

zu „4.1.7 Instandhaltung“ Absatz 9 (neue Nummerierung) (alt 4.8)

Der Absatz wurde aus den Interpretationen, I-3, 6(3) mit redaktionellen Änderungen ergänzt.

zu „4.1.8 Abstimmung zwischen den A-Funktions-Einrichtungen und den aktiven Sicherheitseinrichtungen“ Absatz 2 (alt 4.9)

alter Titel „4.9 Abstimmung zwischen dem Reaktorschutzsystem und den aktiven Sicherheitseinrichtungen“

Der Hinweis wurde in den Regeltext aufgenommen, da es sich um eine Erlaubnis handelt. Die Ergänzung „..durch Aufteilung in sicherheitstechnisch wichtige Systeme…“ wurde gestrichen, da durch die „vorgegebene Redundanz“ alles abgedeckt wird.

zu „4.1.8 Abstimmung zwischen den A-Funktions-Einrichtungen und den aktiven Sicherheitseinrichtungen“ Absatz 3 (alt 4.9)

alter Titel „4.9 Abstimmung zwischen dem Reaktorschutzsystem und den aktiven Sicherheitseinrichtungen“

Der Absatz wurde in den Abschnitt 3 Aufgabenstellung für die Sicherheitsleittechnik Unterabschnitt Grundsätzliches Absatz 4 verschoben. Diese Anforderung passt besser in die Aufgabenstellung und nicht in die Auslegung.

zu „4.1.9 Überwachung auf Funktionsbereitschaft und Prüfbarkeit“ (alt 4.10)

zu „4.1.9.1 Überwachung auf Funktionsbereitschaft“ Absatz 2 (alt 4.10.1)

Der Absatz wurde durch die Interpretationen I-3, 3.2(5) mit redaktionellen Änderungen ersetzt. Der Satz „Die Prüfzyklen sind auf Grundlage von Zuverlässigkeitsbetrachtungen festzulegen.“ wurde nicht übernommen. Die Durchführung der WKP wird in KTA 3506 ausführlich beschrieben. Der Satz greift an dieser Stelle zu kurz.

Im Hinweis wurden zyklische Speichertests und die Überwachung der Datenübertragung als weitere Mittel zur Selbstüberwachung ergänzt. Diese Prüfungen werden insbesondere bei rechnerbasierten Systemen eingesetzt.

zu „4.1.9.1 Überwachung auf Funktionsbereitschaft“ Absatz 3 (alt 4.10.1)

Die Anforderung wurde dahingehend präzisiert, dass anhand der Meldung, der Ort des Ausfalls soweit angezeigt wird, dass eine Instandsetzung erfolgen kann. Weiterhin wurde im Hinweis die Systemfehlermeldung in die beispielhafte Aufzählung der Mittel zur Lokalisierung des Ausfalls aufgenommen. Die Systemfehlermeldung wurde speziell für die rechnerbasierten Systeme ergänzt.

zu „4.1.9.2 Prüfbarkeit der A-Funktions-Einrichtungen“ Absatz 1 (alt 4.10.2)

alter Titel „4.10.2 Prüfbarkeit des Reaktorschutzsystems“

Die beschriebenen Prüfungen, die ohne unzulässige Minderung der Sicherheit der Anlage während des bestimmungsgemäßen Betriebs durchgeführt werden können müssen, werden präzisiert. Der Hinweis auf die Zulässigkeit von administrativen Maßnahmen wurde gestrichen und so umformuliert, dass er die Anforderung ergänzt. Die neue Formulierung macht deutlich, dass administrative Maßnahmen zwar zulässig sind, aber der Vorzug den technischen Maßnahmen zu geben ist.

zu „4.1.9.2 Prüfbarkeit der A-Funktions-Einrichtungen“ Absatz 2 (alt 4.10.2)

alter Titel „4.10.2 Prüfbarkeit des Reaktorschutzsystems“

Das „Schutzuntersystem“ wurde im Abschnitt Begriffe definiert und ersetzt deshalb das „Untersystem“.

Im bisherigen Regeltext wurde eine lückenlose Prüfung gefordert. Eine lückenlose Prüfung ist nicht möglich und wurde deshalb aus der Forderung gestrichen. Weiterhin wurde ein Hinweis eingefügt, der erläutert, dass bei der Bewertung von Abweichungen von bei Auslegung zugrunde gelegten Toleranzwerten auch von der verfahrenstechnischen Toleranz Kredit genommen werden sollte.

zu „4.1.9.2 Prüfbarkeit der A-Funktions-Einrichtungen“ Absatz 3 (alt 4.10.2)

alter Titel „4.10.2 Prüfbarkeit des Reaktorschutzsystems“

Das „Schutzuntersystem“ wurde im Abschnitt Begriffe definiert und ersetzt deshalb das „Untersystem“.

In diesem Absatz wurde die Anforderung, dass die Prüfung ohne Eingriff in die Verdrahtung durchgeführt werden kann, näher beschrieben, wie diese realisiert werden kann. Diese Erläuterung wurde hauptsächlich für die Prüfung programmierbarer oder rechnerbasierter Systeme ergänzt.

Bei programmierbaren oder rechnerbasierten Systemen sind in der Regel Selbsttestroutinen mit vergleichsweise hoher Testabdeckung etabliert. Von diesen kann Kredit genommen werden und der Prüfumfang entsprechend festgelegt werden. Ein Verweis auf die KTA 3506 bezüglich der Selbstüberwachung wurde ergänzt.

zu „4.1.9.2 Prüfbarkeit der A-Funktions-Einrichtungen“ Absatz 3 Hinweis (alt 4.10.2)

alter Titel „4.10.2 Prüfbarkeit des Reaktorschutzsystems“

Der Hinweis konnte als Anforderung interpretiert werden und wurde deshalb umformuliert.

zu „4.1.9.2 Prüfbarkeit der A-Funktions-Einrichtungen“ Absatz 4 (alt 4.10.2)

alter Titel „4.10.2 Prüfbarkeit des Reaktorschutzsystems“

Die beispielhafte Nennung der Prüftafeln wurde ergänzt durch Servicestationen, die bei rechnerbasierte Einrichtungen zur Anwendung kommen.

Der Hinweis auf die Messumformer wurde als Beispiel für eine begründete Ausnahme eingefügt.

zu „4.1.9.2 Prüfbarkeit der A-Funktions-Einrichtungen“ neuer Absatz 5 (alt 4.10.2)

Der Absatz stammt aus den Interpretationen, I-3, 5(3) und wird neu eingefügt.

zu „4.1.9.2 Prüfbarkeit der A-Funktions-Einrichtungen“ Absatz 6 (alt 4.10.2)

alter Titel „4.10.2 Prüfbarkeit des Reaktorschutzsystems“

Die Bedingungen für Prüfungen mit automatischen Prüfeinrichtungen wurden an den Stand der Technik angepasst. Die ursprünglichen Anforderungen an die Protokollierung wurden gestrichen, da diese trivial und in den entsprechenden Abschnitten der KTA 3506 oder KTA 3507 ausreichend beschrieben sind.

Die gestrichenen Bedingungen wurden zum einen ersetzt durch die Bedingung, dass ein Nachweises zur Eignung und Qualität vorliegt und zum anderen durch die Bedingung, dass die Prüfeinrichtung in der Konfigurations- Identifikations- Dokumentation (KID) des Prüflings spezifiziert ist. Beide Anforderungen werden vor allem beim Einsatz von programmierbaren oder rechnerbasierten Prüfeinrichtungen erforderlich.

zu „4.1.10 Handeingriffe“ Hinweis (neu) (alt 4.14)

Es wurde ein einführender Hinweis zur Präzisierung ergänzt, der die rechnerbasierte Leittechnik betrifft.

zu „4.1.10 Handeingriffe“ Absatz 1 (neu) +Hinweis (neu) (alt 4.14)

Der Absatz wurde ergänzt, um Anpassungen an A-Funktions-Einrichtungen zu berücksichtigen, die nicht durch Fehler innerhalb dieser Einrichtungen begründet bzw. keiner Instandsetzung bedürfen.

zu „4.1.10 Handeingriffe“ Absatz 2 (neue Nummerierung) Aufzählung b) (alt 4.14)

Redaktionelle Anpassung, die durch die Streichung des zweideutigen Begriffes „Betriebssystem“ erforderlich war.

Der Absatz wurde so umformuliert, dass sowohl Maßnahmen zum Vorbeugen gegen Fehler als auch Maßnahmen zur Begrenzung der Folgen von Fehlern durch Handeingriffe gefordert werden.

In der Aufzählung im Hinweis wurde q) durch „ergonomische Gestaltung“ ergänzt. Ergonomie ist ein wesentliches Hilfsmittel zur Vermeidung von menschlichen Fehlern.

zu „4.1.10 Handeingriffe“ Absatz 4 (neue Nummerierung) (alt 4.14)

Die allgemeingültige Formulierung „Maßnahmen zur Erschwerung von Handeingriffen…“ wurde präzisiert durch „Maßnahmen zur Erschwerung von Handeingriffen durch Unbefugte…“.

zu „4.1.10 Handeingriffe“ Absatz 5 (neu) (alt 4.14)

Diese Anforderung wurde speziell für rechnerbasierte Einrichtungen eingeführt, um dem Aspekt der IT-Sicherheit Rechnung zu tragen.

zu „4.2 Auslegungsanforderungen an B-Funktions-Einrichtungen“ (neu)

Dieser Abschnitt wurde neu erstellt aufgrund der Kategorisierung nach 2.2. Basis für diesen Abschnitt bildete der überarbeitete Abschnitt 4.1 „Auslegungsanforderungen an A-Funktions-Einrichtungen“. Die Anforderungen wurden an den Stellen modifiziert an denen eine Abstufung der Anforderungen an B-Funktions-Einrichtungen erforderlich war.

Zu „4.3 Änderungen an der Sicherheitsleittechnik“ (neu)

Anforderungen bei Änderungen wurden bislang nur implizit behandelt. In diesem Abschnitt wurden sie zur besseren Übersichtlichkeit zusammengefasst.

Zu „4.4 IT-Sicherheit“ (neu)

Der Abschnitt wurde speziell für rechnerbasierte Geräte neu aufgenommen und wurde zunächst mit den zur Verfügung stehenden Angaben aus der SEWD-Richtlinie IT diskutiert und abgeglichen. Die relevanten Passagen sollten übernommen und redaktionell angepasst werden.

Um unbeabsichtigte Widersprüche zu vermeiden, wurde nur der Verweis auf die SEWD-Richtlinie IT aufgenommen.

zu „4.11 Schutzbegrenzungen“ (ursprüngliche Nummerierung)

Der interpretationsfähige Begriff wurde nicht mehr verwendet. Deshalb wurden die Anforderungen an die Schutzbegrenzungen mit den Anforderungen an Einrichtungen mit Leittechnikfunktionen der neu eingeführten Kategorisierung nach 2.2 verglichen und entsprechend zugeordnet. Der Abschnitt konnte aus diesem Grund entfallen.

zu „4.12 Funktionsgruppensteuerung des Reaktorschutzsystems“ (ursprüngliche Nummerierung)

Die Funktionsgruppensteuerung ist veraltet und wurde deshalb gestrichen. Sollten sie trotzdem noch eingesetzt werden, so werden die Anforderungen vollständig in den Anforderungen an Einrichtungen mit Leittechnikfunktionen der neu eingeführten Kategorisierung nach 2.2 abgebildet

zu „4.13 Ermittlung der Grenzwerte zur Auslösung von Schutzaktionen“ (ursprüngliche Nummerierung)

Der Abschnitt konnte entfallen, da die beiden Absätze nach 3.1 (3) und (5) verschoben wurden.

zu „5 Aufbau und Ausführung der Sicherheitsleittechnik“

alter Titel „5 Aufbau von Reaktorschutzsystemen“

Der Abschnitt wurde aufgrund des umformulierten Anwendungsbereiches und gemäß der Kategorisierung nach 2.2 neu strukturiert. Der Abschnitt 5.1 (alt 5) stellt Anforderungen an A-Funktions-Einrichtungen ursprünglich Reaktorschutz. Dieser Abschnitt wurde überarbeitet und durch den neu erstellten Unterabschnitt 5.1.2 Anforderungen an die Qualifizierung von Software ergänzt.

Der Abschnitt 5.2 wurde neu hinzugefügt und gilt speziell für B-Funktions-Einrichtungen.

Ein weiterer Abschnitt für Anforderungen an C-Funktions-Einrichtungen war zunächst geplant wurde dann aber aufgrund eines Beschlusses des UA-EL auf seiner 68. Sitzung fallen gelassen. Der UA-EL hielt eine Erweiterung auf alle Einrichtungen, die Leittechnikfunktionen der Kategorie C ausführen, wie zum Beispiel: Hebezeuge, Strahlungsinstrumentierung oder Kommunikationseinrichtungen für problematisch, da Überschneidungen mit anderen KTA-Regeln entstünden. Der ursprüngliche Anwendungsbereich der KTA 3501 durfte nach Beschluss des UA-EL nicht erweitert werden. C-Funktions-Einrichtungen sollen nur insoweit behandelt werden, wie sie auch bereits bisher im Regelungsumfang der KTA 3501 enthalten waren, wie etwa Gefahrenmeldeeinrichtungen für Gefahrenmeldungen der Klasse II. Anforderungen an weitere C-Funktions-Einrichtungen sollen in den entsprechenden Leittechnik-Kapiteln der betreffenden komponentenspezifischen KTA-Regeln festgelegt werden.

Die Überschriften der Abschnitte 3, 4 und 5 wurden vereinfacht. Wie in der Definition von Reaktorschutz und Bild 2-1 erläutert ist die Sicherheitsleittechnik nur Teilmenge des Reaktorschutzes. Auf die Verwendung von Reaktorschutz wurde verzichtet, da der Reaktorschutz an dieser Stelle nicht eineindeutig ist.

zu „5.1 Aufbau und Ausführung von A-Funktions-Einrichtungen“

Angabe der Struktur des Abschnittes.

zu „5.1.1 Gerätequalität“ (alt 5.1)

zu „5.1.1.1 Eignungsnachweis für betriebsbewährte Geräte“ Absatz 3 (alt 5.1.1)

Die Möglichkeit Nachweise in Abstimmung mit dem Sachverständigen (nach § 20 AtG) zu erbringen besteht grundsätzlich immer und muss nicht in einer KTA-Regel geregelt werden. Die Erlaubnis, dass analytische Nachweise von bestimmten Geräteeigenschaften in Abstimmung mit dem Sachverständigen (nach § 20 AtG) erfolgen können wurde deshalb gestrichen.

zu „5.1.1.1 Eignungsnachweis für betriebsbewährte Geräte“ Absatz 4 (alt 5.1.1)

Der Absatz wurde neu eingeführt, um die speziellen Bedingungen anzugeben, unter denen die Betriebsbewährung als Eignungsnachweis bei programmierbaren Geräten gelten dürfen. Für rechnerbasierte Geräte wurde diese Möglichkeit ohne zusätzliche Nachweise ausgeschlossen. Folgende Aspekte wurden dabei diskutiert:

1. Eine Trennung der Betriebsbewährung von Geräten in Softwarebetriebsbewährung und Hardwarebetriebsbewährung ist nicht möglich, da bei rechnerbasierten Geräten die Hardware ohne Software nicht funktionsfähig ist. Betriebsbewährung kann nur für das gesamte Gerät erlangt werden und sollte hier auch zugelassen werden, vorausgesetzt, dass keine Änderungen am Gerät vorgenommen wurden.
2. Ein Eignungsnachweis durch Betriebsbewährung für programmierbare und rechnerbasierte Geräte ist aus folgenden Gründen nicht möglich:
    a) Bei programmierbaren und rechnerbasierten Geräten sind Software-Updates zu erwarten. Diese führen automatisch zur Beendigung einer begonnenen Betriebsbewährung.
    b) Die Geräte können in einem unterschiedlichen Kontext mit unterschiedlicher Konfiguration des Geräts betrieben werden. Dies erlaubt nur in identischen Kontext mit identischer Konfiguration einen Beitrag zur Betriebsbewährung.
    c) Nicht alle Softwarezustände werden während der Betriebsdauer des Geräts angesprochen. Somit ist durch zufällige Ereignisse / Einflüsse mit dem Eintritt vorher noch nie eingetretener Softwarezustände zu rechnen.
3. In den KTA-Regeln 3503 und 3505 ist bereits heute festgeschrieben, dass für softwarebasierte Geräte eine theoretische Prüfung der Software-Unterlagen zu erfolgen hat. Von daher bildet diese Anforderung keine zusätzliche Einschränkung. Der ergänzte Hinweis auf diese Regeln verdeutlicht dies in ausreichendem Maße.

zu „5.1.1.2 Eignungsnachweis für neu entwickelte oder modifizierte Geräte“ Absatz 1 und 2 (alt 5.1.2)

Die Festlegung soll die Grundqualität der Komponenten sichern, die mehr und mehr im Ausland gefertigt werden. Das Arbeitsgremium beschließt, die Stufe B nach DIN EN 61192-1 (Fertigungsklasse 2 nach IPC A610D) als Mindestanforderung aufzunehmen. Dabei wird vor Allem auf die in dieser Fertigungsklasse übliche Serienfertigung und die damit verbundene Betriebserfahrung verwiesen. Die Produktion von kleinen Stückzahlen in der Stufe C nach DIN EN 61192-1 (Fertigungsklasse 3 nach IPC A610D) wurde vom Arbeitsgremium als Nachteil bewertet. Weiterhin wurde angeführt, dass die Umgebungsbedingungen nicht immer besonders harsch sind (z.B. Betrieb in klimatisierten Räumen) und viele Baugruppen redundant im System verwendet werden. Der Einzelausfall wird mit der Anwendung des Redundanzprinzips beherrscht. Die Anforderungen wurden in zwei neuen Absätzen formuliert.

zu „5.1.1.3 Anforderungen an die Auslegung neu entwickelter oder modifizierter Geräte“ Absatz 5 (alt 5.1.3) Hinweis

Die beispielhafte Aufzählung der „Einstellzeit“ wurde durch den prägnanteren Ausdruck „Zeitverhalten“ ersetzt. Die Einstellzeit ist implizit im Zeitverhalten enthalten.

zu „5.1.1.4 Zuverlässigkeit und Qualitätsprüfung“ Absatz 3 Hinweis (alt 5.1.4)

Da es sich bei Firmware in Geräten um spezielle Software handelt wurde an dieser Stelle ein Verweis auf den Abschnitt 5.1.2 Anforderungen an die Qualifizierung von Software ergänzt, der zusätzliche Anforderungen stellt.

zu „5.1.2 Anforderungen an die Qualifizierung von Software“ (neu)

Dieser Abschnitt wurde auftragsgemäß neu erstellt. Basis für diesen Abschnitt bildete der Abschnitt „7.6 Software der Sicherheitsleittechnik“ der RSK-Leitlinien. Weiterhin wurde das Modul 5 der „Sicherheitskriterien für Kernkraftwerke“ Revision D, Abschnitt „7.3.2 Software für Leittechnik-Funktionen der Kategorie A“ berücksichtigt.

zu „5.1.3 Systemeigenschaften und Aufbau“ (neu)

Der Abschnitt ist neu erstellt worden und beschreibt Anforderungen zur Realisierung von fehlervermeidenden und fehlerbeherrschenden Maßnahmen bezüglich eines systematischen Fehlers. Dazu wurden die VDE/VDI 3527 und die DIN EN 62340 herangezogen.

zu „5.1.4 Umgebungseinflüsse“ (alt 5.2)

zu „5.1.4.1 Beanspruchungen bei bestimmungsgemäßem Betrieb“ Absatz 1 (alt 5.2.1)

Für die Einhaltung des Verbotes, dass die Funktion nicht unzulässig beeinträchtigt werden darf, wurde ein Nachweis gefordert. Bei den zu betrachtenden Einflüssen wurde die elektromagnetische Beeinflussung und Verträglichkeit ergänzt, als Anpassung an den Stand der Technik.

zu „5.1.4.1 Beanspruchungen bei bestimmungsgemäßem Betrieb“ Absatz 2 (alt 5.2.1)

Redaktionelle Änderung.

zu „5.1.4.2 Beanspruchungen bei Leckratenprüfungen des Reaktorsicherheitsbehälters“

Der Prüfumfang einer WKP reicht unter Umständen an dieser Stelle nicht aus und wurde deshalb gestrichen.

zu „5.1.5.2 Kabel“ Absatz 2 (alt 5.3.2)

Richtigstellung der Aufzählung.

zu „5.1.5.2 Kabel“ (alt 5.3.2) Absatz 5

Redaktionelle Anpassung.

zu „5.1.5.3 Wirkdruckleitungen“ Absatz 4 (neu)

Über diese Anforderung sollen technische Vorkehrungen in den Fokus gerückt werden, die benötigt werden, um eine einwandfreie Funktion des Messumformers (unverfälschtes Messsignal) zu gewährleisten. Die Anforderung ist vergleichbar zur Forderung nach Prüfbarkeit der leittechnischen Einrichtungen sowie für die Durchführung von Instandsetzungen anzusehen.

zu „5.1.6.3 Justier- und Einstellvorrichtungen“ (alt 5.4.3)

Dieser Abschnitt wurde auftragsgemäß um Anforderungen an programmierbare und rechnerbasierte Systeme ergänzt. Zur Erstellung wurden unter anderem die DIN IEC 61513 und die DIN EN 60880 herangezogen.

zu „5.1.6.4 Zugänglichkeit“ (alt 5.4.4) Absatz 2

alter Titel „5.4.4 Instandhaltung“

Die Anforderungen dieses Abschnittes beziehen sich nicht direkt auf Instandhaltung, sondern auf Ergonomie, deshalb wurde eine treffendere Überschrift gewählt.

Die Begründung dafür, dass man leicht auswechselbare Geräte einbauen soll, wurde auf „…Erleichterung von Instandhaltungsmaßnahmen…“ verkürzt. Die Beschleunigung von Instandhaltungsmaßnahmen ist implizit in der Erleichterung enthalten und wurde deshalb gestrichen.

Der Hinweis wurde redaktionell überarbeitet.

zu „5.1.7 Aufbau von Schutzuntersystemen“ (alt 5.5)

Der Abschnitt wurde entsprechend Bild 2-1 (Aufteilung in Ebenen) neu strukturiert. Der Abschnitt teilt sich zunächst in 3 Unterabschnitte Anregeebene, Logikebene und Steuerebene. Der Unterabschnitt Steuerebene wurde neu eingefügt. Ihm wurden die Einzelantriebssteuerung und die Vorrangsteuerung zugeordnet.

zu „5.1.7.1 Anregeebene“ (neu) (alt 5.5

Die Teilüberschrift *5.1.7.1.1 Messsignalvergleich* ist irreführend und wurde deshalb gestrichen. Die Anforderung gilt allgemein für die Anregeebene und wurde entsprechend angepasst.

zu „5.1.7.1.1 Analoge Anregekanäle“ (alt 5.5.1.2 + 5.5.1.3)

Die Aufteilung in analoge und digitale Anregekanäle wurde fallengelassen. Gemeint ist an dieser Stelle ein analoger Anregekanal in analoger oder digitaler Gerätetechnik. Dieser Sachverhalt wurde in einem Hinweis ergänzt.

zu „5.1.7.1.3 Grenzsignalgeber und Vergleicher“ (alt 5.5.1.4) neuer Absatz 6

Auftragsgemäß wurde eine Anforderung für rechnerbasierte Geräte ergänzt.

Zu „5.1.7.2 Logikebene“ (alt 5.5.2)

Der missverständliche Begriff „Schaltkanal“ wurde durch „Signalpfad“ ersetzt. Weiterhin wurde der Absatz 3 aus Abschnitt *5.1.7.3.2 Vorrangsteuerung (alt 5.5.3)* an diese Stelle verschoben, da er dort thematisch besser passt (Anforderung an die Logikebene).

Zu „5.1.7.2.1 Verriegelungen“ (neu)

Der Abschnitt „Verriegelungen“ (alt 5.5.5) wurde der Logikebene zugeordnet.

Der Hinweis unter Absatz 2 wurde gestrichen. Dieser Hinweis bietet an dieser Stelle keinen Mehrwert und verwirrt eher.

zu „5.1.7.3 Steuerebene“ (neu)

Der Abschnitt *5.1.7.3 Steuerebene* wurde entsprechend Bild 2-1 (Aufteilung in Ebenen) neu eingeführt. Die Abschnitte „Einzelantriebsteuerung“ und „Vorrangsteuerung“ wurden ihm zugeordnet.

Zu „5.1.7.3.1 Einzelantriebssteuerungen“ (alt 5.5.4)

Die Absätze 2 – 5 enthalten Anforderungen an die Koppelglieder, die der Vorrangsteuerung zugeordnet werden. Die Absätze wurden deshalb in den Abschnitt *5.1.7.3.2 Vorrangsteuerung* verschoben. „strangweise“, „viersträngig“ usw. wurden durch die einheitlich verwendeten Begriffe „redundant“, „redundanzbezogen“ usw. ersetzt.

Zu „5.1.7.3.2 Vorrangsteuerung“ (alt 5.5.3)

Die „betrieblichen Steuersignale“ wurden redaktionell überarbeitet, so dass die Formulierung mit denen aus der Ersetzung des „Betriebssystems“ übereinstimmen. Weiterhin wurde der Absatz 1 des Abschnittes 5.1.7.3.2 zur Klarstellung redaktionell überarbeitet. Im Absatz 2 desselben Abschnittes wurde „Strang“ durch den einheitlich verwendeten Begriff „Redundanz“ ersetzt. Der Absatz 3 wurde in den Abschnitt *5.1.7.2 Logikebene* verschoben, da die Anforderung für die Logikebene gilt. Die Absätze 4-6 stammen aus dem Abschnitt Einzelantriebssteuerungen. Die Anforderungen an die Koppelglieder wurden der Vorrangsteuerung zugeordnet. Die Neuordnung wurde erforderlich durch die Korrektur von Bild 2-1.

zu „5.2 Aufbau und Ausführung von B-Funktions-Einrichtungen“ (neuer Abschnitt)

Dieser Abschnitt wurde neu erstellt aufgrund der Kategorisierung nach 2.2. Basis für diesen Abschnitt bildete der überarbeitete Abschnitt „5.1 Aufbau und Ausführung von A-Funktions-Einrichtungen“. Die Anforderungen wurden an den Stellen modifiziert an denen eine Abstufung der Anforderungen an B-Funktions-Einrichtungen erforderlich war.

Zu „6 Aggregateschutz“

Zu „6 Aggregateschutz“ Absatz 1

Der erste Satz des Absatzes 1 wurde redaktionell so angepasst, dass der Aggregateschutz näher beschrieben wird. Die Aufgabe des Aggregateschutz wird dadurch deutlicher hervorgehoben.

Zu „6 Aggregateschutz“ Absatz 2+3 (neu)

Die beiden Absätze wurden aus den Interpretationen der SiAnf, I-3, 3.21 (13) Absätze 3 und 4 übernommen. Sie ersetzen teilweise den alten Absatz 2.

Zu „6 Aggregateschutz“ Absatz 4 (neue Nummerierung) (alt 2)

Der in den neu eingeführten Absätzen 2+3 fehlende Aspekt aus dem alten Absatz 2 wurde in Absatz 4 aufgenommen und redaktionell angepasst.

Zu „6 Aggregateschutz“ Absatz 5 (neue Nummerierung) (alt 3)

Redaktionelle Überarbeitung.

Zu „7 Zustandsbegrenzung“ (alt)

Der interpretationsfähige Begriff wurde nicht mehr verwendet. Deshalb wurden die Anforderungen an die Zustandsbegrenzungen mit den Anforderungen an Einrichtungen mit Leittechnikfunktionen der neu eingeführten Kategorisierung nach 2.2 verglichen und entsprechend zugeordnet. Der Abschnitt konnte aus diesem Grund entfallen.

Zu „7 Lüftungstechnische Anlagen zur Raumkühlung von A-Funktions-Einrichtungen“ (neue Nummerierung) (alt 8)

alter Titel „8 Lüftungstechnische Anlagen zur Kühlung des Reaktorschutzsystems“

Zur Klarstellung wurde der Absatz 2 und der Hinweis redaktionell überarbeitet.

Zu „8 Elektrische Energieversorgung“ (neue Nummerierung) (alt 9)

Zu „8 Elektrische Energieversorgung“ Absatz 1-3

Redaktionelle Überarbeitung.

Zu „8 Elektrische Energieversorgung“ (alt 9) Absatz 4

Der Absatz wurde aus den Interpretationen der SiAnf, I-3 3.10 (3) übernommen.

Zu „8 Elektrische Energieversorgung“ (alt 9) Absatz 5

Der ursprüngliche Absatz 5 wurde durch einen Verweis auf die KTA 3703 ersetzt, da die Anforderungen an die Batteriekapazität des Notstromsystems in der KTA 3703 zentral geregelt sind.

Zu „9 Gefahrenmeldeeinrichtungen“ (neue Nummerierung) (alt 10)

Zu „9.1 Allgemeines“

Es wurde ein neuer Absatz eingefügt, der allgemeine Anforderungen an die Eignung der Geräte stellt.

Zu „9.2 Gefahrenmeldeeinrichtungen der Klasse S“ (alt 10.2)

Zu „9.2.2 Auslegung“ Absatz 1 (neu)

Es wurden Anforderungen an die Gerätequalität ergänzt, die bislang nicht explizit erwähnt wurden.

Zu „9.2.3 Software für Gefahrenmeldeeinrichtungen der Klasse S“ (neu)

An dieser Stelle wurde ein neuer Abschnitt mit einem Verweis auf die entsprechenden Softwareabschnitte der A- und B-Funktions-Einrichtungen eingefügt.

Zu „9.3 Gefahrenmeldeeinrichtungen der Klasse I“ (alt 10.3)

zu „9.3.2 Auslegung“ Absatz 4 (alt 10.3.2)

Der Absatz wurde allgemeiner formuliert, damit die Anforderung auch für Bildschirmwarten gelten kann.

zu „9.3.3 Software für Gefahrenmeldeeinrichtungen der Klasse I“ (neu) +Hinweis

Die Gefahrenmeldeeinrichtungen der Klasse I wurden den C-Funktions-Einrichtungen zugeordnet. Dieser neue Abschnitt legt an dieser Stelle nur eine Qualifizierung nach anerkannten Methoden fest und schlägt im Hinweis vor, die DIN EN 62138 Kategorie C heranzuziehen

zu „10 Prüfungen“ (alt 11)

zu „10.1 Prüfungen an A- und B-Funktions-Einrichtungen und an Gefahrenmeldeeinrichtungen der Klasse S“ (alt 11.1)

zu „10.1.1 Prüfung der Eignung der Gerätetypen“ (alt 11.1.1)

zu „10.1.1.1 Ergänzende Typprüfungen für betriebsbewährte Geräte“ Absatz 2 (alt 11.1.1.1)

und

zu „10.1.1.2 Typprüfungen für neu entwickelte oder modifizierte Geräte“ (alt 11.1.1.2) Absatz 2

Neben einer Ersetzung der Formulierung bezüglich des „Sachverständigen (nach § 20 AtG)“ durch die im Abschnitt 3.2 g) des Merkblattes (2011-11) vorgeschlagene Formulierung, wurde die Durchführung der praktischen Prüfung durch den Werksachverständigen in eine Erlaubnis umgewandelt. Als gleichwertig zur Prüfung mit dem Werksachverständigen wurde eine Prüfung durch ein geeignetes Prüflabor oder eine geeignete Prüfstelle angegeben. Als geeignetes Prüflabor wird je nach vorzunehmender Prüfung ein akkreditiertes oder zertifiziertes Prüflabor verstanden.

Durch den angestiegenen Prüfumfang und den dazu nötigen Prüfhilfsmitteln z. B. bei den EMV-Prüfungen werden die Prüfungen häufig in externen Prüflaboren durchgeführt. Die eingeführte Erlaubnis berücksichtigt diese Entwicklung.

zu „10.1.2 Werksprüfungen“ (alt 11.1.2)

Die Beschränkung auf das Sicherheitssystem wurde aufgrund der neu eingeführten Kategorisierung fallen gelassen.

zu „11 Konfigurations-und Identifikations-Dokumentation“ (neu)

Mit der Formulierung dieses Abschnittes erfolgte eine Anpassung an den Stand von Wissenschaft und Technik, die sich aus der Einführung der rechnerbasierte Leittechnik ergab. Die Anforderungen an die Konfigurations-Identifikations-Dokumentation (KID) werden in KTA 3506 gestellt, auf die an dieser Stelle verwiesen wird.

Diskussionen bei der Überarbeitung der 35er Reihe des KTA-Regelwerks zeigten, dass sowohl die bestehende Dokumentation als auch das Identifikationsmanagement der „konventionellen“ Sicherheitsleittechnik den Anforderungen von KTA 3506 genügen.

zu „12 Zusammenstellung der im atomrechtlichen Genehmigungs- und Aufsichtsverfahren für das Reaktorschutzsystem zur Prüfung erforderlichen Informationen“ (alt)

Dieser Abschnitt wurde an dieser Stelle auftragsgemäß gestrichen. Der Abschnitt wurde aber sinngemäß in Absatz 3 der Grundlagen eingefügt, um konsistent zur 3701 zu bleiben.

zu „Anhang A Bestimmungen, auf die in dieser Regel verwiesen wird“

Die Verweise wurden aktualisiert.