Institut für
Sicherheitstechnologie
(ISTec) GmbH

Aufstellung von Kriterien und Kenngrößen zur deterministischen Prüfung der Eignung von Redesign-Baugruppen für den Einsatz in der Sicherheitsleittechnik von KKW

Typprüfung von Redesign-Komponenten mit komplexen Baugruppen
Machbarkeitsstudie Komplexitätsmessung für Redesign-Komponenten

Lindner, A.
März, J.
Miedl, H.
Schnürer, G.

ISTec - A - 2158
Rev. 1
Dezember 2014

Dieser Bericht ist im Auftrag der GRS unter der Auftragsnummer 469022 erstellt worden. Der Eigentümer behält sich alle Rechte vor.

Revisionsblatt

Rev.	Änderungen	Autor	Datum
00	Erstfassung		
01	Redaktionelle Überarbeitung nach Kommentaren des AG	Lindner	11.12.2014

Kurzfassung

Im vorliegenden Bericht werden Anforderungen an die Prüfung von und Bewertungskriterien für den Einsatz von Redesign-Komponenten für die Sicherheitsleittechnik von Kernkraftwerken beschrieben. Der Schwerpunkt liegt dabei auf Prüfverfahren für komplexe digitale rechnerbasierte Komponenten.

Es zeigte sich, dass sich Anforderungen bezüglich der Fertigung von Redesign-Baugruppen aus IPC 610 ableiten lassen. Anforderungen für FPGA-basierte Redesign-Baugruppen sind für HDL-programmierte Schaltkreise in der IEC 62566 zu finden. Von den zusätzlich betrachteten Testverfahren hat der Burn-in-Test das Potenzial, die Typprüfung nach KTA 3503 zu ergänzen. Testverfahren zur stark beschleunigten Alterung durch extreme Temperaturwechsel und Vibrationsbelastung erscheinen nicht zielführend, da das Belastungsprofil für Kernkraftwerke untypisch ist und Berechnungsergebnisse aufgrund der inhomogenen Zusammensetzung der Leittechnikbaugruppen zu ungenau sind, um belastbare Ergebnisse zu liefern. Ergänzend zu den direkten kerntechnischen Qualifizierungsverfahren wurde die Vorgehensweise nach der VDI-Richtlinie 3528 in die Betrachtung einbezogen.

Im zweiten Teil des Berichts wurde untersucht, inwiefern und mit welchen Methoden sich die Komplexitätsmessung, die für Software entwickelt wurde, auf Redesign-Baugruppen anwenden lässt. Dabei wurde sichtbar, dass konventionelle, festverdrahtete Redesign-Baugruppen und Redesign-Baugruppen in Dickschicht-Hybridtechnik als einzelne Baugruppe nicht sinnvoll bezüglich ihrer Komplexität bewertet werden können. Komplexere rechnerbasierte Baugruppen sind weitgehend mit der Methode der Komplexitätsmessung analysierbar. Die dabei zu erzielenden Resultate sind denen der Komplexitätsmessung der Software gleichwertig.

Abstract

The report describes requirements for tests and assessment criteria for application of re-design modules used in safety I&C of nuclear power plants. The main focus was put on test procedures for complex digital software-based modules.

It was revealed that requirements regarding manufacturing can be derived from IPC 610. Requirements for FPGA-based re-design modules are included in IEC 62566 for HDL programmed circuits. Additional test procedures have been taken into account. The Burn-in-Test seems to be suited to complement type testing corresponding to KTA 3503. Test procedures based on accelerated aging by extreme temperature changing and strong vibration seem not to be constructive, because the load profile is not typical for nuclear power plants and the theoretical results are to inaccurate due to heterogeneous constitution of complex modules. Additional to the direct nuclear qualification procedures the approach based on VDI-Guideline 3528 was taken into account.

The second part of the report provides the results to what extend and with which methods complexity measurement, developed for software, can be applied to re-design modules. It was revealed that conventional hardwired re-design modules and re-design modules based on thick-film hybrid technology can not been reasonably evaluated regarding their complexity by this method. More complex computer-based modules can be widely evaluated with the complexity measurement method. The results obtained are equivalent to the results obtained for software.

INHALTSVERZEICHNIS

VERZEICHNIS DER BILDER

VERZEICHNIS DER TABELLEN

1 EINLEITUNG

Gegenstand des Projekts "Aufstellung von Kriterien und Kenngrößen zur deterministischen Prüfung der Eignung von Redesign-Komponenten für den Einsatz in der Sicherheitsleittechnik von Kernkraftwerken" der GRS 3611R01355 ist es, Anforderungen und Bewertungskriterien für den Einsatz von Redesign-Komponenten, insbesondere Komponenten in der Sicherheitsleittechnik von Kernkraftwerken, zu entwickeln.

In diesem Rahmen trägt ISTec mit zwei Arbeitspaketen zum GRS-Projekt bei. Das Arbeitspaket 4, Anforderungen an die Typprüfung beim Redesign, befasst sich mit spezifischen Vorgehensweisen, die bei der Typprüfung von Redesign-Komponenten mit komplexen insbesondere digitalen rechnerbasierten Bauteilen anzuwenden sind. Es sollen Typprüf-Anforderungen für Redesign-Komponenten abgeleitet und zusammengestellt werden.

Im Arbeitspaket 5, Machbarkeitsstudie für eine Komplexitätsmessung von elektronischen Komponenten, wird die Machbarkeit einer Ausdehnung der beim ISTec bislang angewandten Komplexitätsmessung auf Redesign-Komponenten mit komplexen programmierbaren Bauelementen untersucht.

Bei ISTec ist Expertise zur Komplexitätsmessung von Software digitaler Sicherheitsleittechnik vorhanden. Dieses Konzept ist für unterschiedliche digitale Leittechniksysteme anwendbar. Das Messverfahren und seine praktische Realisierbarkeit wurden durch die Anwendung auf ein Test-System nachgewiesen /MAE 10/. Die beschriebene Auswertung der Ergebnisse belegt die unmittelbare Bedeutung der Komplexitätsmessung für die Qualifizierung digitaler Leittechniksysteme. Die Anpassung der Komplexitätsmessung auf Redesign-Komponenten eröffnet die Möglichkeit der gleichzeitigen Bewertung der zugehörigen Hard- und Software und kann damit einen wesentlichen Beitrag zur Qualifizierung von Redesign-Komponenten mit komplexen programmierbaren Bauelementen leisten.

Ziel im Rahmen dieses Arbeitspakets ist die Beantwortung der Frage, ob bzw. unter welchen Bedingungen eine Anpassung der Komplexitätsmessung auf Redesign-Komponenten machbar ist.

Grundlage der im Projekt "Aufstellung von Kriterien und Kenngrößen zur deterministischen Prüfung der Eignung von Redesign-Komponenten für den Einsatz in der Sicherheitsleittechnik von Kernkraftwerken" vom ISTec durchzuführenden Arbeiten ist die im ISTec vorhandene, langjährige Erfahrung in der Typprüfung rechnerbasierter Sicherheitsleittechnik und der Entwicklung und Anwendung von Methoden und Werkzeugen zur Analyse und zum Sicherheitsnachweis von Software /MAI 95/, /MAE 95/.

Da die in der Leittechnik eingesetzten Bauteile, Geräte und Systeme ständig weiterentwickelt werden, kommen immer komplexere und durch höhere Integrationsdichten gekennzeichnete Bauteile zum Einsatz. Aufgrund der geringen Stückzahlen von zu fertigenden Komponenten im Bereich der Kerntechnik sind komplexe und flexibel einsetzbare elektronische Komponenten, die auch in anderen Bereich Einsatz finden können, geradezu für solche Einsatzfälle prädestiniert. Diese Technologie kann nicht als pure Hardware betrachtet werden, da die Entwicklung der Funktionalität EDV-basiert erfolgt und sehr große Ähnlichkeit mit der Softwareentwicklung aufweist (z.B. Verwendung von Hardwarebeschreibungssprachen (HDL)).

In den letzten Jahren haben sich kleinere Firmen etabliert, die komplexe elektronische Komponenten auch in kleinen Stückzahlen als Sonderfertigung anbieten. Damit wird ein Weg

eröffnet, bestehende Sicherheitsleittechnik unter Verwendung moderner Elektronik aber unter Beibehaltung genehmigter Systemstrukturen aufrechtzuerhalten. Dies wirft spezifische Fragen des Nachweises der Eignung dieser Komponenten auf, für die in der Typprüfung nach KTA (3503, 3505) neue Akzeptanzkriterien festgelegt werden müssen.

Hervorzuheben bezüglich der Entwicklung von Methoden und Werkzeugen für die Qualifizierung rechnerbasierter Leittechniksysteme ist die in jüngster Zeit entwickelte und bereits prototypisch implementierte Methode zur Komplexitätsmessung von Software digitaler Sicherheitsleittechnik /MAE 10/. Die Komplexitätsmessung bezieht sich auf die spezifische Struktur generischer, digitaler Leittechnik-Systeme, welche mittels Code-Generatoren auf der Grundlage einer graphischen Spezifikation der Funktionalität erzeugt werden. Das Messverfahren ermöglicht, das Komplexitätsspektrum der implementierten, leittechnischen Funktionen digitaler Leittechnik-Systeme darzustellen und Rückschlüsse hinsichtlich Art, Größe und Verteilung der Komplexität innerhalb des Systems zu ziehen.

Eine Grundlage für die ISTec-Arbeiten war die Teilnahme an „HARMONICS“ („Harmonised Assessment of Reliability of Modern Nuclear I&C Software“), einem FP-7 Projekt der EU.

Es ist das Ziel von HARMONICS, der Kerntechnik fundierte und auf dem neuesten Stand von Wissenschaft und Technik beruhende Methoden für die Qualifizierung der Software computerbasierter Sicherheitssysteme bereitzustellen.

2 PRÜFUNG VON REDESIGN-BAUGRUPPEN MIT KOMPLEXEN PROGRAMMIERBAREN BAUELEMENTEN

2.1 Allgemeines

Gegenwärtig wird besonders von der deutschen nuklearen Industrie der Einsatz von Redesign Baugruppen auch auf Basis von programmierbaren Bauelementen angestrebt, da hier die Möglichkeit besteht, bestehende festverdrahtete Sicherheits-Leittechnik mit programmierbaren Technologien auszutauschen, ohne das übergeordnete Sicherheitsleittechnikkonzept zu modifizieren. Ein solches Vorgehen verringert dann den Bewertungs- und Qualifizierungsaufwand, sofern diese hardwareprogrammierbaren Technologien nach etablierten Typ- und Eignungsprüfungsmethoden qualifiziert sind. Ein Redesign bestehender, zumeist sogenannter festverdrahteter Analogbaugruppen der Sicherheitsleittechnik, ist dann funktions- und in der Regel auch Pin kompatibel zur originären Baugruppe, wobei die hardwareprogrammierbare Komponente auf der redesignten Baugruppe auf z.B. FPGA oder ASIC Anwendungen basieren kann.

Die hohen Qualifizierungsanforderungen in Deutschland erfordern im Rahmen der Typprüfung eine konsequente und formale Bewertungsprozedur für sämtliche Komponenten und Systeme im Sicherheitsbereich von Kernkraftwerken insbesondere mit Blick auf Zuverlässigkeit und Funktionssicherheit. Grundlage des nachstehend vorgestellten, der Typprüfung zugrundeliegenden Qualifizierungsansatzes ist deshalb die Fragestellung, auf welche Weise Applikationen mit programmierbaren Bauelementen zu qualifizieren sind damit ein analog zur bestehenden Sicherheitsleittechnik hoher Qualifizierungslevel erzielt wird um Leittechnikfunktionen auszuführen. Da jedoch Anwendungen von programmierbaren Bauelementen gegenwärtig in Deutschland noch einen innovativen Charakter haben, sind, vorzugsweise basierend auf international etablierten Qualifizierungs-Anforderungen, entsprechende Qualifizierungs- und Bewertungs-Anforderungen auch für Deutschland zu entwickeln. Diese Qualifizierungs-Anforderungen sollen dann einerseits bestehende nationale und internationale nukleare Regelwerke und Standards (z.B. in Bezug auf generische Qualifizierungsprozeduren) sowie anwendungs-spezifische Aspekte (wie z.B. die Bewertung von Entwicklungs- und Qualifizierungs-Tools) berücksichtigen. Andererseits sind aber auch besondere deutsche, bereits fest etablierte und bewährte Bewertungs- und Qualifizierungs-Anforderungen, wie diese z.B. in KTA 3503 (Typprüfung von elektrischen Baugruppen der Sicherheitsleittechnik) enthalten sind, zu erfüllen.

Zu diesen bereits fest etablierten und bewährten Bewertungs- und Qualifizierungs-Anforderungen zählen vornehmlich hardware- und systemspezifische Anforderungen, wie Robustheit (u.a. gegen EMB) und ein mindestens determinierbarer funktioneller Status (z.B. sicherheitsgerichtetes Ausfallverhalten) sogar im Falle des Auftretens von Systemfehlern. Darüber hinaus wird die Determinierung und Quantifizierung von Zuverlässigkeitskenndaten mit bereits etablierten Methoden, wie z.B. einer Schwachstellenanalyse, erfolgen.

Sämtliche der nachstehend vorgestellten Sicherheitsanforderungen sind in voller Übereinstimmung mit deutschen sowie internationalen Regeln und Standards zur Sicherheitsleittechnik in KKW. Jedoch wurden wegen der weitgefächerten Erfahrungen auf dem Gebiet der Qualifizierung von FPGA-Anwendungen im Sicherheitsbereich von Kernkraftwerken neben kerntechnischen Regelwerksanforderungen auch nichtnukleare Regelwerksanforderungen

berücksichtigt, sofern diese zielführend und im Einklang mit nuklearen Regelwerksanforderungen sind. Allerdings ist es im Hinblick auf die FPGA-Spezifika unerlässlich, bestehende, in der Regel softwarespezifische Qualifizierungsanforderungen in FPGA-spezifische Qualifizierungsanforderungen, unter Beibehaltung der eigentlichen Anforderungen, umzusetzen.

Losgelöst hiervon ist eine weitere wesentliche Qualifizierungs-Voraussetzung, dass der vorgestellte Qualifizierungsansatz ausschließlich nur für den Synchronbetrieb (zyklische Betriebsweise) und zudem mit sogenannten „On-Chip Testfacilities“ effektiv umsetzbar ist.

Die Forderung einer synchronen Betriebsweise rechtfertigt sich aus den bereits für einen synchronen rechnerbasierten Betrieb entwickelten Qualifizierungsanforderungen, die an die Belange von „Baugruppen mit programmierbaren Bauelementen“ angepasst werden. Außerdem zeigt sich bei einem nichtsynchronen Betrieb von „Baugruppen mit programmierbaren Bauelementen“ der Effekt eines sogenannten „Wettlaufverhaltens“. Dies bedeutet die Zeitspanne zwischen Signaleingang, Signalverarbeitung und Ausgang ist insbesondere bei mehreren parallelen Signaleingängen nicht mehr determinierbar. Demgegenüber ist ein determinierbares Verhalten, wie es bei einer synchronen Betriebsweise vorliegt, Voraussetzung für eine kerntechnische Typprüfung.

Analog hierzu ist es Voraussetzung für eine kerntechnische Typprüfung die Korrektheit (Unversehrtheit) der auf dem Chip implementierten bzw. projektierten Verbindungen (z.B. Routen von vorkonfigurierten Schaltkreisen), Software, Schnittstellen und nicht zuletzt implementierten leittechnischen Funktion einschließlich der Hardware zu verifizieren.

Eine Übersicht internationaler nuklearer Regeln zur Qualifizierung von sicherheitskritischer Software und programmierbaren Systemen ist in Tabelle 2.1 zusammengestellt.

Tabelle 2.1: Internationale nukleare Regeln zur Qualifizierung von sicherheitskritischer Software und programmierbaren Systemen

Nr.	Titel
IEC 60671	Nuclear power plants - Instrumentation and control systems important to safety - Surveillance testing
IEC 60780	Nuclear Power Plants - Electrical equipment of the safety system - Qualification
IEC 60880	Nuclear Power Plants - Instrumentation and control important for safety - Software aspects for computer-based systems performing category A functions
IEC 60987	Nuclear Power Plants – Instrumentation and control systems important to safety – Hardware design requirements for computer based systems
IEC 60987	Nuclear Power Plants – Instrumentation and control systems important to safety – Hardware design requirements for computer based systems Amendment 1

Nr.	Titel
IEC 61226	Nuclear Power Plants – Instrumentation and control systems important to safety – Classification of instrumentation and control functions
IEC 61513	Nuclear Power Plants – Instrumentation and control for systems important to safety – General requirements for systems
IEC 62340	Nuclear Power Plants - Instrumentation and control systems important to safety - Requirements for coping with common cause failure (CCF)
IEC 62566	Nuclear power plants – Instrumentation and control important to safety – Development of HDL-programmed integrated circuits for systems performing category A functions
ISO 9001	Quality management systems – Requirements
IAEA NS-G-1.3	Instrumentation and Control Systems Important to Safety in Nuclear Power Plants

Da sich die Schwierigkeiten bei der Beschaffung von Ersatzteilen und -baugruppen für sicherheitsrelevante Leittechnik für Kernkraftwerke schon vor einigen Jahren abzeichneten, hat der VDI Facharbeitskreis 7.11 „Leittechnik in Kernkraftwerken“ die VDI-Richtlinie 3528 „Anforderungen an Serienprodukte und Kriterien für deren Einsatz in der Sicherheitsleittechnik in Kernkraftwerken“ /VDI 11/ erarbeitet. Auf diese Richtlinie wird deshalb in diesem Bericht eingegangen.

2.2 Typprüfung nach KTA 3503

Die kerntechnische Regel KTA 3503 befindet sich seit Juni 2011 in Revision. Dies bedeutet, das ein von der KTA eingesetztes Arbeitsgremium auftragsgemäß diese Regel unter anderem auch an die typprüfspezifischen Belange von Redesign-Baugruppen mit komplexen programmierbaren Bauelementen anpasst, zumal in der Vorläuferversion vom November 2005 diese Technologie explizit keine Erwähnung fand.

Im Detail werden aktuell in KTA 3503 in Anlehnung an DIN IEC 61226 Typprüfanforderungen an „Baugruppen mit programmierbaren Bauelementen“, die Sicherheits-Funktionen der Kategorie (Funktionskategorie) A und B ausführen, berücksichtigt. Grundsätzlich gelten für Baugruppen mit programmierbaren Bauelementen der Funktionskategorie A und B hinsichtlich Prüfumfang und Tiefe gleichwertige und darüber hinaus vergleichbare Anforderungen wie bei rechnerbasierten Baugruppen. Zudem sind die bereits existierenden softwarespezifischen Anforderungen in der Regel sinngemäß auf Baugruppen mit programmierbaren Bauelementen übertragbar, da auch diese nur mit softwarebasierten Design-, Konfigurierungs-, und Prüftools implementiert werden.

Demzufolge ist in KTA 3503 unter Abschnitt 3, Prüfverfahren vereinbart:

„(3) Bei rechnerbasierten oder programmierbaren Baugruppen ist eine Prüfung der Software und deren Qualitätsmerkmale im Rahmen der theoretischen Prüfungen nach 4.2. und die Prüfung der Funktion im Rahmen der praktischen Prüfungen durchzuführen..“

In den Folgeabschnitten von KTA 3503 wird dann in der Regel nur noch erläuternd auf die typprüfspezifischen Belange von Baugruppen mit programmierbaren Bauelementen eingegangen.

2.3 Zusammenstellung von Anforderungen an die Prüfung komplexer programmierbarer Baugruppen

2.3.1 Abnahmekriterien von elektronischen Baugruppen nach IPC 610

Die weltweitverbreitete und international anerkannte IPC-Richtlinie IPC-A-610 legt die Abnahmekriterien für den Entstehungsprozess von elektronischen Baugruppen fest. Der Name IPC geht auf das in 1957 gegründete “Institute for Printed Circuits“ zurück. Im April 2010 wurde die aktuelle Revision E der Richtlinie IPC-A-610 vom amerikanischen Fachverband „Association Connecting Electronics Industries“ (IPC) veröffentlicht.

Nach den vorliegenden Erkenntnissen ist das IPC weltweit die einzige Institution, die eine breite Palette dieser Dokumente durchgehend für den gesamten Prozess der Entwicklung und Herstellung von Leiterplatten sowie kompletten elektronischen Baugruppen anbietet. Das IPC ist zudem bemüht, den Übergang zu neuen Baugruppentechniken in der Praxis möglichst frühzeitig mit entsprechenden Normen und Richtlinien zu unterstützen.

Aus diesem Grund soll anschließend die Intension und der Aufbau der IPC Richtlinien erläutert werden.

Grundsätzlich ist sicherzustellen, dass das Bauteil oder die Baugruppe wie beabsichtigt funktioniert. Aus diesem Grund muss die Umgebung, in der sie später betrieben werden soll, zum Zeitpunkt der Entwicklung und vor Beginn des Leiterplatten-Designs bekannt sein. Hierzu zählen Betriebsbedingungen für das Gerät, wie z.B. Umgebungstemperatur, von Bauelementen erzeugte Wärme, Ventilation, Erschütterung und Vibration.

Um hierbei die Kommunikation zwischen Entwicklung und Fertigung zu erleichtern, wurden drei abgestufte Qualitätsklassen entwickelt, die die wachsenden Anforderungen hinsichtlich technologischem Anspruch, funktionaler Leistungsfähigkeit und Häufigkeit bzw. Aufwand an Wartung oder Beanspruchungsprüfung wiederspiegeln. Nachstehende Tabelle gibt eine Übersicht dieser „Klassen“.

Tabelle 2.2: Qualitätsklassen nach IPC 610

Klasse	Anforderung	Anwendungsbeispiele
Klasse 1: Gewöhnliche Elektronikprodukte (General Electronic Products)	Die Hauptforderung an die Produkte dieser Klasse ist, dass die fertige Baugruppe funktioniert.	Konsumer Elektronik wie z.B. Hifi, TV, Video etc.
Klasse 2: Zweckbestimmte Elektronikprodukte (Dedicated Service Electronic Products)	Hierunter fallen Produkte, für die kontinuierliche Leistung und verlängerte Lebensdauer gefordert sind und für die unterbrechungsfreier Betrieb erwünscht, aber nicht kritisch ist. Die typische Anwendungsumgebung bewirkt keinen Ausfall.	Allgemeine Industrieelektronik wie z.B. SPS, Gebäudeleittechnik, z.T. Automotive (auch TXS, ISKAMATIC, TXP …….)
Klasse 3: Hochleistungselektronik (High Performance Products)	Hierunter fallen Produkte, für die kontinuierliche Hochleistung oder Leistung auf Abruf kritisch ist, bei denen ein Funktionsausfall nicht toleriert wird, die Endanwendungsumgebung besonders extrem sein kann, und das Gerät jederzeit funktionsfähig sein muss, z.B. in lebenserhaltenden oder anderen kritischen Systemen.	Hochleistungselektronik wie z.B. Luftfahrttechnik, Medizinprodukte, Bahntechnik, z.T. Automotive

Diese drei Klassen dienen dem Ziel gemeinsamer Qualitätsrichtlinien für Kunden und Lieferanten, wobei der Kunde die Klasse vorgibt. Hierbei fokussieren diese Klassen auf die Abnahmerichtlinien IPC-A-600-G für Leiterplatten, IPC-A610-D für Baugruppen und IPC-A610-E, welche Anforderungen an die Abnahme- und Sichtprüfung sowie weiterer anzuwendender Spezifikationen und IPC-Dokumente enthält. Sämtliche IPC Anforderungen verstehen sich als Mindestforderungen. Diese Mindestanforderungen nehmen Bezug auf ein breites Spektrum an IPC-Richtlinien von der Entwicklung über Leiterplattenherstellung bis hin zum Endprodukt. Eine Übersicht dieser IPC Fertigungsrichtlinien ist nachstehend zusammengestellt.

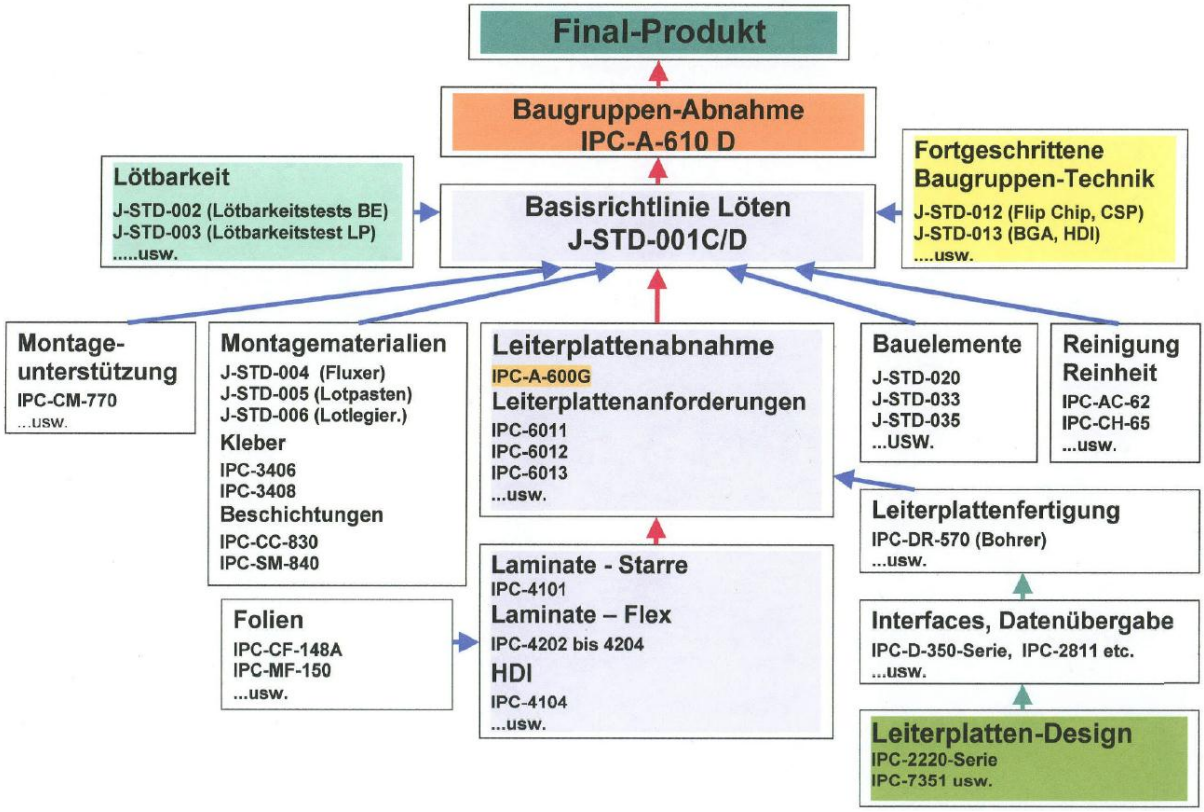

Bild 2.1: IPC-Fertigungsrichtlinien /GRÖ 06/

Neben der eigentlichen Fertigung werden die IPC Richtlinien bereits auch auf den Entwicklungsprozess von Elektronik angewandt. Nachstehende Übersicht zeigt die einzelnen Phasen eines Entwicklungsprozesses, der den IPC Richtlinien zugrunde liegt.

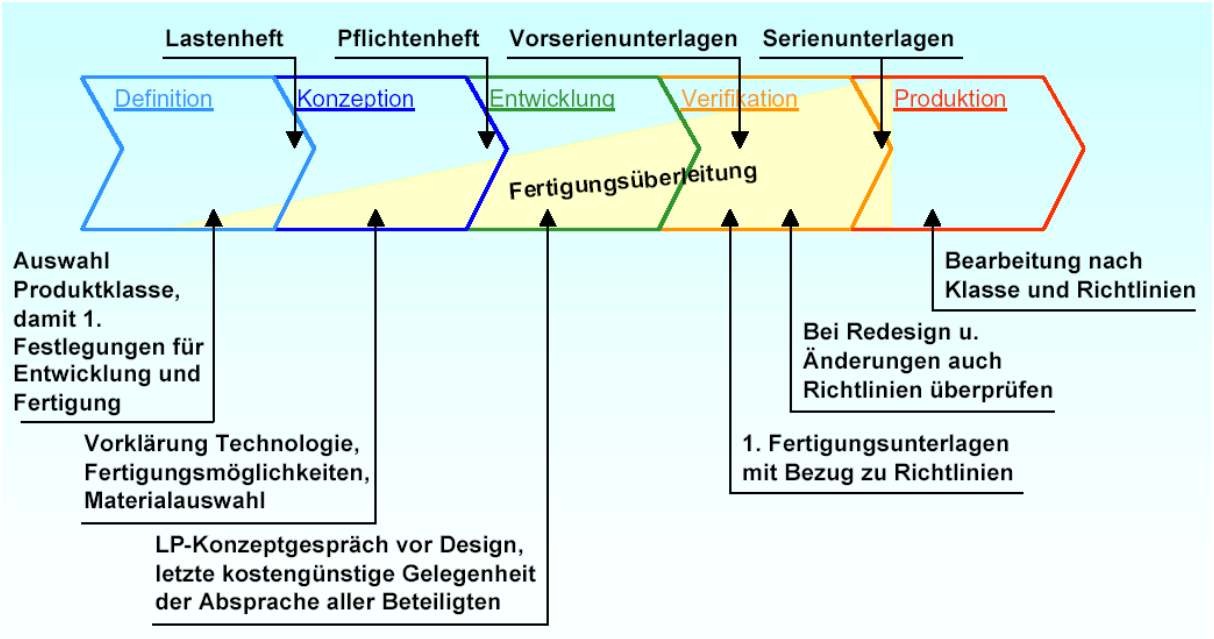

Bild 2.2: Entwicklungsprozess von Elektronik der den IPC Richtlinien zugrunde liegt /GRÖ 06/

Somit wird unter konsequenter Berücksichtigung der IPC Fertigungs- und Entwicklungsrichtlinien sichergestellt, dass die angestrebte Qualitätsklasse erzielt wird.

Infolge der internationalen Akzeptanz der IPC Richtlinien existieren auch verschiedene IEC (DIN/EN) Regeln, die einen unmittelbaren Bezug zu IPC haben. Nachstehende tabellarische Zusammenstellung zeigt hierfür Beispiele.

Tabelle 2.3: Beispiele von IEC Regeln, die einem unmittelbaren Bezug zu IPC Richtlinien haben.

IPC Dokument	Titel	Norm
IPC-D-350	Digital PWB Format	IEC 61182-1
IPC- SM-840	Solder Mask	IEC 249-3-3
IPC-D-356	Bare Board Electrical Test	IEC 61182-7
IPC-TM-650	Test Methods Manual	IEC 61189-1,-2, -3
IPC- 2141	Impedance Control	IEC 61188-1-2
IPC-7351…	Land Pattern Requirements	IEC 61188-5-1…
IPC-RB-276	Rigid Printed Boards	IEC 61326-4
J-STD-001A	Soldering Requirements	IEC 61191-1 to -4
IPC-A-610	Acceptability of Solder Joints	IEC 61192-1 to -4
J-STD-004	Flux Requirements	IEC 61190-1-1
J-STD-005	Solder Paste Requirements	IEC 61190-1-2
J-STD-006	Solid Solder Materials	IEC 61190-1-3

Die Diskussion innerhalb einschlägiger deutscher Expertengremien zeigte, dass im Sicherheitssystem deutscher Kernkraftwerke elektronische Geräte und Komponenten mindestens die Anforderungen der Klasse 2 erfüllen sollen, sofern einsatzumgebungsbedingt keine höheren Anforderungen, wie z.B. bei Störfallumgebungsbedingungen, zu erfüllen sind. Weiter wurde innerhalb dieser Gremien festgestellt, dass z.B. die Regeln IEC 61192-1 bis -4 zwar einen direkten Bezug zu IPC-A- 610 haben, inhaltlich jedoch durchaus Unterschiede aufweisen. So werden z.B. bei dem Anwendungsbereich zu den drei Qualitätsklassen abweichende Einsatzfelder genannt, die durchaus Anlass für Diskussionen waren. Es wurde hier deshalb vereinbart, in jedem Fall die Original-Anforderung aus der jeweiligen IPC Richtlinie zu berücksichtigen.

2.3.2 Anforderungen an die Prüfung von FPGA-basierten Baugruppen

Gemäß dem internationalen Regelwerk müssen Komponenten bzw. Systeme mit sicherheitstechnischer Bedeutung einem Sicherheitslebenszyklus folgend entwickelt werden. Dies gilt gleichermaßen für die Entwicklung von Field Programmable Gate Arrays (FPGAs). Bild 2.3 skizziert einen Sicherheitslebenszyklus für FPGA-Entwicklungen in Anlehnung an das V-Modell.

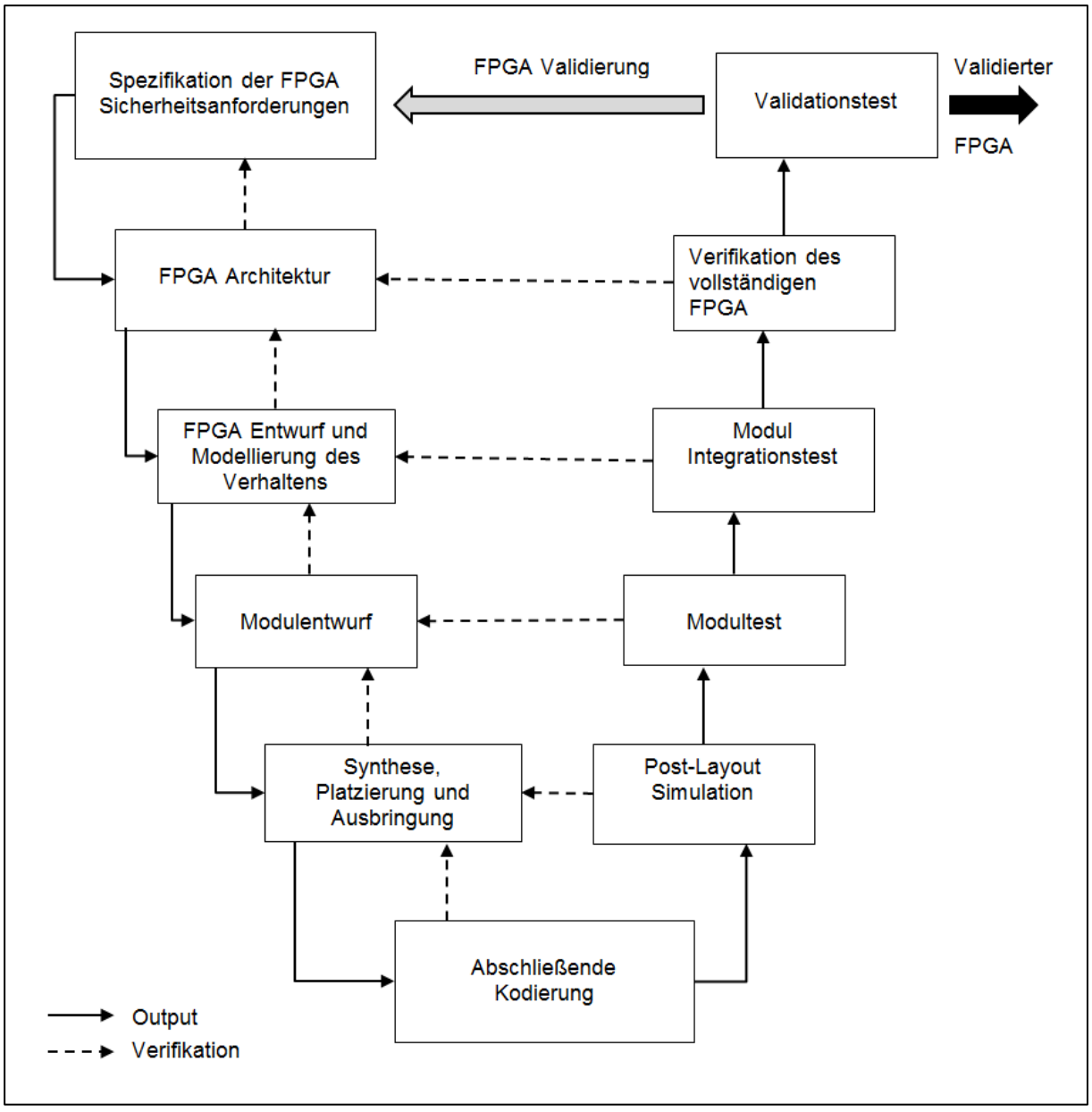

Bild 2.3: FPGA Sicherheitslebenszyklus

FPGAs beinhalten logische Funktionsblöcke und programmierbare Verbindungsleitungen mit steuerbaren Schaltern zwischen diesen Funktionsblöcken. FPGAs sind als Feld oder Matrix gefertigt, woraus sich der Name dieses Bausteins ableitet.

In den folgenden Abschnitten werden Empfehlungen und Anforderungen zu Struktur und Inhalt der Entwicklungsdokumentation deklariert, die für die Qualifikation von FPGA Anwen-

dungen für Sicherheitsfunktionen in der Kerntechnik erforderlich sind. Die Empfehlungen und Anforderungen wurden zusammengestellt unter Beachtung der internationalen Normen DIN EN 61508 und DIN EN 62566 einschließlich deren Entwurfsdokumente[1]. Zur Gliederung der Empfehlungen und Anforderungen für die Entwicklungsdokumentation wird der Sicherheitslebenszyklus exemplarisch in folgende vier Phasen unterteilt:

- Anforderungsphase
- Entwurfsphase
- Implementierungsphase
- Verifikations- und Validationsphase (V&V Phase)

Die Phasen des Sicherheitslebenszyklus sind nicht bindend. Das internationale Regelwerk schreibt weder die Anzahl noch den Umfang der einzelnen Phasen vor. Es ist jedoch gefordert ein Phasenmodell zu etablieren, entlang dessen FPGAs mit Hilfe von rechnergestützten Werkzeugen entwickelt werden. Ein typischer FPGA Design Flow wird in Bild 2.4 dargestellt.

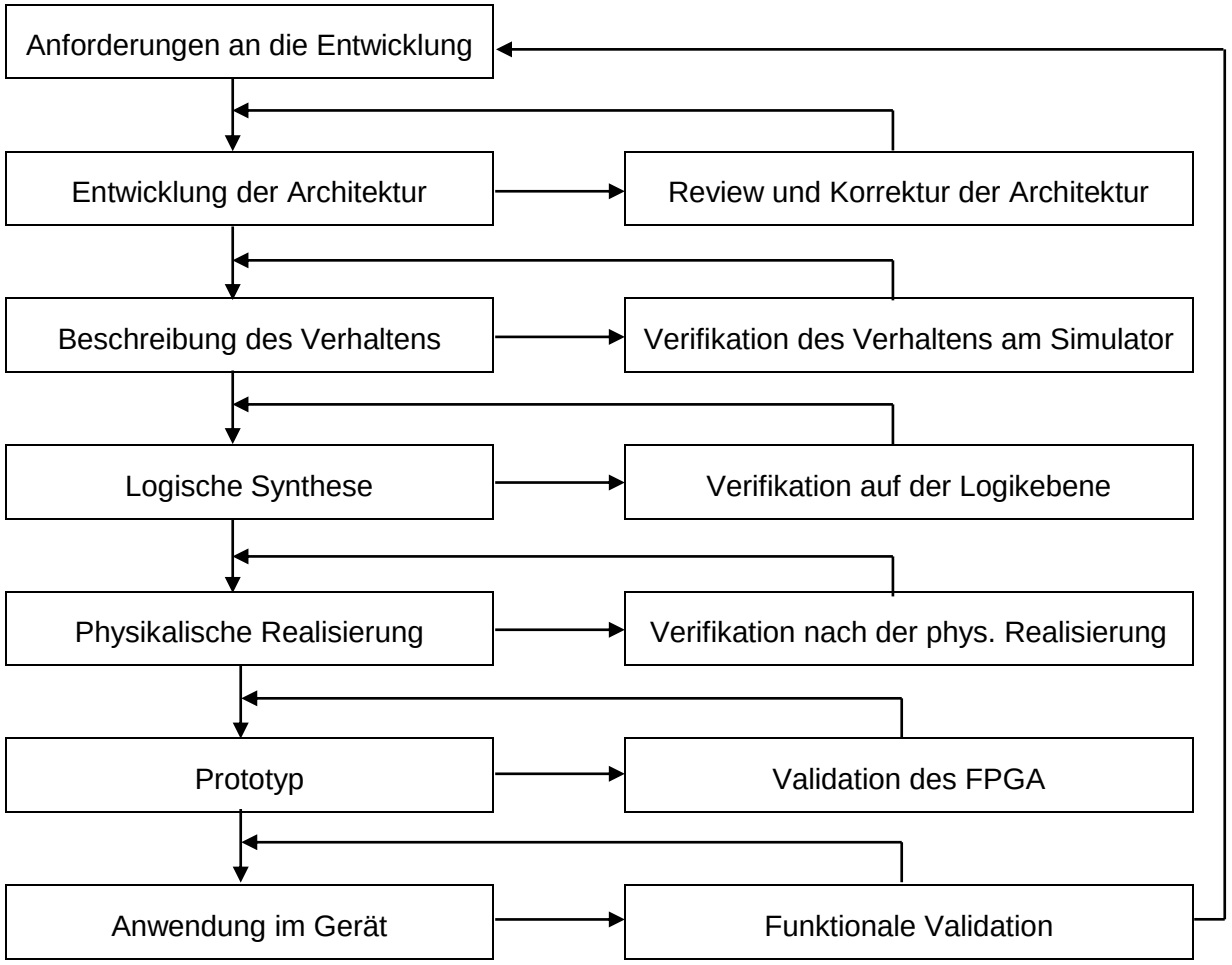

Bild 2.4: Typischer FPGA Design Flow

[1] Die IEC 62566 wurde im Laufe ihrer Entwicklung auf HDL-programmierbare Bausteine eingeschränkt. Dabei wurden Aspekte aus der Norm herausgenommen, die in diesem Bericht mit ausgewertet wurden.

Die Phasenergebnisse des FPGA Design Flow sollen mit formalen Methoden (kritische Reviews, Überprüfungen, Analyse bzw. eine Kombination dieser Methoden) verifiziert werden. Die Einrichtung und Führung eines nach Phasen aufgebauten Design Flow stellt sicher, dass die FPGAs entsprechend den Vorgaben an Design, Herstellung, Test, Instandhaltung und Qualitätssicherung entwickelt werden. Dies wird durch die Dokumentation der Phasenergebnisse untermauert.

2.3.2.1 Anforderungsphase

Die Dokumentation der Anforderungsphase bildet die Grundlage zur Entwicklung von Komponenten bzw. Systemen mit sicherheitstechnischer Bedeutung. Diese Zweckbestimmung wird in der internationalen Norm DIN EN 60880 für Softwaresysteme konstatiert. Dies gilt aber ebenso für die Entwicklung von FPGA-basierten Komponenten bzw. Systemen. Darüber hinaus sollten Genehmigungsaspekte (für die anlagenspezifische Anwendung) beachtet werden, da die Dokumentation der Anforderungsphase gegebenenfalls der Behörde vorzulegen ist.

Die Anforderungen sollen in vollständiger und eindeutiger Weise spezifiziert werden, um diese nachweisbar erfüllen zu können. Das Dokument soll knapp und akkurat beschreiben, was und warum zu fordern ist, und nicht wie es zu realisieren ist. Die Anforderungen sollen in Übereinstimmung mit dem internationalen Regelwerk formuliert werden, d.h. „soll“ für obligatorische Anforderungen, „sollte“ für empfohlene Anforderungen und „darf“ für optionale Anforderungen. Die in der Dokumentation der Anforderungsphase getroffenen Festlegungen werden in der nachfolgenden Phase des Sicherheitslebenszyklus (Entwurfsphase) weitergeführt und verfeinert. Sie dienen auch als Basis für die Validationsaktivitäten der V&V Phase.

Im Folgenden sind exemplarisch Struktur und Inhalt einer Anforderungsspezifikation skizziert. Die spezifischen Anforderungen sollten hierbei nicht als obligatorisch, sondern als Merkposten gesehen werden. Die spezifischen Anforderungen hängen von der mit FPGAs zu lösenden Aufgabenstellung ab. Die aufgelisteten Objekte können selbstverständlich kombiniert werden oder auch entfallen.

Allgemeine Beschreibung

- Motivation
- Ziele
- Mögliche Alternativen
- Einschränkungen (Sicherheitskategorie)

Spezifische Anforderungen

- Überblick
- Rolle der Komponente im Gesamtsystem
- Parameter
- Technische Daten
- Komponentenstruktur
- Beschreibung der Komponentenfunktionen

- Datenmodell
- Betriebsarten
- Dynamisches Verhalten
- Leistungsverhalten
- Initialisierung, Rücksetzen
- Schnittstellen zu anderen Komponenten
- Kommunikationsdiagramm
- Benutzerschnittstellen
- Datenblatt (FPGA Baugruppe)
- Selbstüberwachung
- Fehlerverhalten, Störverhalten
- DV-technische Sicherheitsaspekte
- Installation
- Softwarepakete
- Wartung, Diagnose

Qualitätssicherung

- Regelwerke und Normen
- Qualitätscharakteristika
- Qualitätsmaßnahmen
- Teststrategie, Testprozeduren und Akzeptanzkriterien
- Datensicherung
- Konfigurationsmanagement

Definitionen, Abkürzungen

Quellenangabe

2.3.2.2 Entwurfsphase

Die Hauptaufgabe der Entwurfsphase liegt in der Überführung der FPGA-Anforderungen aus der Anforderungsspezifikation in eine Beschreibung der Struktur, Elemente, Schnittstellen und Daten, wie sie für die Implementierung benötigt wird. Die Überführungsschritte sollten nach einem Top-Down-Vorgehen erfolgen. Die Entwurfsspezifikation definiert die Aufgaben, die das FPGA bereitstellen muss und wie die funktionalen und nicht-funktionalen Anforderungen zu erfüllen sind. Das Dokument sollte hinreichend detailliert sein und geeignete Abbildungen und Diagramme beinhalten.

Im Folgenden sind exemplarisch Struktur und Inhalt einer Entwurfsspezifikation skizziert. Die Entwurfsinhalte sollten hierbei nicht als obligatorisch, sondern als Merkposten gesehen wer-

den. Die Entwurfsinhalte hängen von der mit FPGAs zu lösenden Aufgabenstellung ab. Die aufgelisteten Objekte können selbstverständlich kombiniert werden oder auch entfallen.

Allgemeine Beschreibung

- Allgemeine technische Bedingungen
- Technische Lösung
- Mögliche Alternativen
- Einschränkungen

Entwurfsinhalte

- Überblick
- Aufgabenbereich der Komponente im Gesamtsystem
- Parameter
- Architektur
- Verhalten
- Technische Daten
- Beschreibung der Komponentenfunktionen (Rückverfolgbarkeit zu funktionalen Anforderungen)
- Komponentenstruktur (Verteilung der logischen Funktionen)
- Datenmodell
- Betriebsarten
- Dynamisches Verhalten
- Leistungsverhalten
- Selbstüberwachung
- Fehlerverhalten, Störverhalten, Fehlermeldungen
- Initialisierung, Rücksetzen
- Schnittstellen zu anderen Komponenten
- Kommunikationsdiagramm
- Datenaustausch
- Benutzerschnittstellen
- Datenblatt (FPGA Baugruppe)
- DV-technische Sicherheitsaspekte
- Installation
- Softwarepakete (vorgefertigte Software)
- Wartung, Diagnose

Design FMEA

Qualitätssicherung

- Qualitätsmaßnahmen
- Teststrategie, Testprozeduren und Akzeptanzkriterien
- Konfigurationsmanagement

Definitionen, Abkürzungen

Quellenangabe

2.3.2.3 Implementierungsphase

Die Ergebnisse der Entwurfsphase (Entwurfsspezifikation) werden innerhalb der Implementierungsphase weiter verfeinert. Die Implementierungsspezifikation sollte die Quelltexte wiederspiegeln, die als Grundlage für die Realisierung der FPGA-Anwendung dienen. Gemäß den internationalen Normen DIN EN 61508 und DIN EN 60880 sollte die Implementierungsspezifikation in klarer und verständlicher Form verfasst werden. Somit wird das Dokument verständlich für qualifizierte Ingenieure, die nicht im Entwicklungsprozess involviert sind.

Im Folgenden sind exemplarisch Struktur und Inhalt einer Implementierungsspezifikation skizziert. Die Quelltextbestandteile sollten hierbei nicht als obligatorisch, sondern als Merkposten gesehen werden. Die Quelltextbestandteile hängen von der mit FPGAs zu lösenden Aufgabenstellung ab. Die aufgelisteten Objekte können selbstverständlich kombiniert werden oder auch entfallen.

Allgemeine Beschreibung

- Allgemeine Anforderungen
- Technische Lösung
- Hardwarebeschreibungssprache
- Entwicklungsumgebung (Werkzeuge)
- Programmierrichtlinien (Einschränkungen)

RTL Quelltext mit Kommentaren bezüglich

- Problembeschreibung
- Beschreibung der Komponentenfunktionen (Rückverfolgbarkeit zu funktionalen Anforderungen)
- Schnittstellen
- Datenstrukturen
- Algorithmen
- Ablaufdiagramme
- Fehlervermeidende Maßnahmen
- Vorgefertigte Komponenten
- Testangelegenheiten

- Implementierungseinschränkungen
- Netzlisten
- Berichtsdateien

Qualitätssicherung

- Qualitätsmaßnahmen

Definitionen, Abkürzungen

Quellenangabe

2.3.2.4 Verifikations- und Validationsphase (V&V Phase)

Die Aktivitäten der V&V Phase können in zwei Bereiche unterteilt werden, den in der Regel statischen Verifikationsaktivitäten und den in der Regel dynamischen Validationsaktivitäten. Die V&V Aktivitäten, die als Teil des FPGA-Entwicklungsprozesses ausgeführt werden, liegen normalerweise in der Verantwortung des Lieferanten und werden von Personal durchgeführt, welches unabhängig von denen der FPGA-Produktion ist. Zusätzliche V&V Aktivitäten können erforderlich sein, um den Nachweis zu führen, dass das Produkt seinen Qualitätsvorgaben entspricht. Diese zusätzlichen V&V Aktivitäten können als Teil einer unabhängigen Bewertung („third party assessment“) erfolgen und betreffen sowohl das FPGA Produkt als auch seinen Entwicklungsprozess.

Die Ergebnisse jeder Phase des Sicherheitslebenszyklus müssen verifiziert werden. Falls dies als Teil des Entwicklungsprozesses ausgeführt wird, sollte die Verifikation einer Phase vor dem Beginn der nächsten Phase durchgeführt werden. Die Nachweistiefe hängt von der Bedeutung des FPGA für die Systemsicherheit und der Konsequenz des Systemausfalls ab. Somit unterliegen FPGAs des Sicherheitssystems einem strengeren Verifikationsprogramm als FPGAs der sicherheitsrelevanten Systeme. Die Verifikation soll den Design Flow begleiten, um Auslegungsfehler frühzeitig erkennen und korrigieren zu können.

Simulation und Testen soll vollzogen werden, um das FPGA und seine Software in Übereinstimmung mit den funktionalen und nichtfunktionalen Anforderungen aus der Anforderungsphase zu validieren. Die Werkzeuge, die während der Entwicklung Verwendung finden, sollen verifiziert und bewertet werden. Die Verifikation und Bewertung des Werkzeugs soll entsprechend den Zuverlässigkeitsanforderungen, der Art und dem Potenzial Fehler einzutragen erfolgen.

Die Tests sollen sich an den Betriebsbedingungen, für die die FPGAs ausgelegt sind, orientieren. Hierbei sind Aspekte, wie Spannungsversorgung, Umgebungsbedingungen, usw. zu berücksichtigen.

Im Folgenden sind exemplarisch Struktur und Inhalt einer V&V Dokumentation skizziert. Die einzelnen Themen sollten hierbei nicht als obligatorisch, sondern als Merkposten gesehen werden. Die Themen hängen von der mit FPGAs zu lösenden Aufgabenstellung ab. Die aufgelisteten Objekte können selbstverständlich kombiniert werden oder auch entfallen. Üblicherweise sind die Dokumente der V&V Phase unterteilt in Unterlagen, welche die Vorbereitung der V&V Aktivitäten und welche die Ergebnisse der V&V Aktivitäten betreffen.

Allgemeine Beschreibung (V&V Plan)

- V&V Ziele
- V&V Gegenstände
- Einschränkungen

Verifikationsprozess

- Verifikationsumgebung
- Verifikationsstrategie, Verifikationsansatz
- Überdeckungskriterien der Verifikation
- Verantwortlichkeiten
- Hilfsmittel zur Verifikation (Werkzeuge)
- Zeitplan
- Endekriterium der Verifikation (bestanden, nichtbestanden)

Verifikationsspezifikation (Szenarien, Testplan)

- Beschreibung der Eingaben und Ausgaben
- Detaillierte Verifikationsprozedur (Komponenten- und Systemverifikation)
- Nichtfunktionale Anforderungen (Leistung, Robustheit, Zuverlässigkeit, usw.)
- Definition der Verifikationsszenarien
- Akzeptanzkriterien

Verifikationsprozedur

- Spezielle Anforderungen
- Verifikationslog
- Einrichtung der Verifikationsumgebung
- Verifikationskonfiguration
- Verifikationsausführung

Verifikationsbericht

- Identifikation des Verifikationsszenarios
- Verifikationsumgebung
- Verifikationsergebnis
- Schlussfolgerungen, Empfehlungen

Validationsprozess

- Validationsumgebung
- Validationsstrategie, Validationsansatz
- Überdeckungskriterien der Validation
- Verantwortlichkeiten

- Hilfsmittel zur Validation (Werkzeuge)
- Zeitplan
- Endekriterium der Validation (bestanden, nichtbestanden)

Validationsspezifikation (Szenarien, Testplan)

- Beschreibung der Eingaben und Ausgaben
- Detaillierte Validationsprozedur (Komponenten- und Systemvalidation)

Validationsentwurf und -spezifikation

- Beschreibung der Eingaben und Ausgaben
- Detaillierte Validationsprozedur (Komponenten- und Systemvalidation)
- Validationsfalldefinition
- Akzeptanzkriterien

Validationsprozedur

- Spezielle Anforderungen
- Validationslog
- Einrichtung der Validationsumgebung
- Validationskonfiguration
- Validationsausführung
- Handhabung von Vorfällen bei der Validation
- Beenden der Validation

Validationsbericht

- Identifikation des Validationsgegenstands
- Validationsumgebung
- Validationslog
- Vorfälle bei der Validation
- Validationsergebnis
- Schlussfolgerungen, Empfehlungen

Definitionen, Abkürzungen

Quellenangabe

Neben den Empfehlungen und Anforderungen zu Struktur und Inhalt der Entwicklungsdokumentation sind weitere Aspekte bei der Prüfung von FPGA zu berücksichtigen. Für FPGA-Anwendungen gelten – wie für rechnerbasierte Komponenten bzw. Systeme – allgemeine Anforderungen, deren Einhaltung entsprechend zu prüfen ist.

FPGAs sollen so aufgebaut sein, dass leittechnische Elemente mit geringerer Sicherheitskategorie keinen Einfluss (innerhalb eines Toleranzbereichs) auf leittechnische Elemente mit höherer Sicherheitskategorie haben. Die leittechnische Funktion soll auch im Fall von Abwei-

chungen im Eingabesignalbereich ausgeführt werden. Im Idealfall sollen die FPGAs eine separate elektrische Versorgung aufweisen und der Informationsaustausch soll mittels galvanischer Trennelemente erfolgen. FPGAs, die Funktionsmodule verschiedener Sicherheitskategorien beinhalten, sollten das gleiche Maß an Verifikation und Validation erfahren wie für die höchste Sicherheitskategorie.

Zusätzlich zu den technischen Aspekten müssen für die Entwicklungsdokumente eine eindeutige Identifikation und ein System zur Versionshaltung eingerichtet werden. Hierzu kann beispielsweise ein entsprechendes Deckblatt generiert werden. Für die Handhabung aller Gegenstände des Entwicklungsprozesses soll ein Konfigurationsmanagement eingerichtet und eingesetzt werden. Das Konfigurationsmanagement soll den Vorgaben des Konfigurationsmanagementplans oder des Qualitätssicherungsplans entsprechen.

Das Konfigurationsmanagement ermöglicht es, alle Gegenstände des Entwicklungsprozesses zu identifizieren und Buch zu führen hinsichtlich des Grades der Erfüllung der physikalischen und funktionalen Anforderungen. Zu jeder Phase des Sicherheitslebenszyklus kann auf die realen Daten zugegriffen werden. Der Zugriff muss mit Schutzmechanismen geregelt sein, um beispielsweise unbeabsichtigte Änderungen auszuschließen. Mit der Auswahl der Konfigurationselemente soll zu Beginn des Sicherheitslebenszyklus begonnen werden. Die Konfigurationselemente müssen eindeutig und klar identifizierbar sein. Der Konfigurationsmanagementprozess muss gemäß den Phasen des Sicherheitslebenszyklus geplant, und Verantwortlichkeiten und Befugnisse für dessen Realisierung müssen zugewiesen werden.

Das Konfigurationsmanagement beim Hersteller des FPGA muss dokumentiert sein und soll den verwendeten Konfigurationsmanagementprozess identifizieren. Die Eignung des Hersteller-Konfigurationsmanagementprozesses ist mit Audits zu bestätigen.

Modifikationen an Konfigurationselementen erfordern ein nachvollziehbares Änderungsverfahren. Das Änderungsverfahren sollte den Änderungsprozess und die zu erstellenden Änderungsdokumente festlegen. Der aktuelle Zustand der revidierten Dokumente ist zu kennzeichnen. Hierbei sind auch unterstützende Dokumente in Betracht ziehen. Der Grund der Änderung ist anzugeben und die möglichen Konsequenzen der Änderung sind abzuschätzen. Zudem ist detailliert zu beschreiben, wie die Modifikation vorbereitet, ausgeführt und verifiziert werden soll.

Zur Realisierung von FPGA-Anwendungen werden in der Regel rechnergestützte Werkzeuge eingesetzt, an die bestimmte Anforderungen gerichtet sind. Die Werkzeuge sollen in allen Phasen des Sicherheitslebenszyklus eingesetzt werden, wo diese der Qualität oder Zuverlässigkeit zuträglich sind. Die Werkzeuge sollen in Abhängigkeit ihrer Bedeutung für die Sicherheit qualifiziert bzw. zertifiziert sein. Die Werkzeug-Ausgaben sind entsprechend zu verifizieren. Alle eingesetzten Werkzeuge sind mit vollständiger Kennzeichnung und Parametrierung vom Konfigurationsmanagement zu erfassen. Es soll dokumentiert werden, wie die Werkzeuge den FPGA Design Flow unterstützen und wie sie einzusetzen sind. Die Werkzeuge sollen hinreichend zuverlässig sein, um die Gesamtzuverlässigkeit der FPGA Anwendung nicht zu beeinträchtigen.

2.3.2.5 Qualität und Sicherheit

Sicherheit ist eng mit Qualität verknüpft. Qualität wird mit der Konformität zu Anforderungen definiert, die sich aus der technischen Spezifikation der Aufgabe und den zugehörigen Nor-

men ergeben. Mit den qualitätssichernden Maßnahmen soll erreicht werden, dass das FPGA die nötige Qualität aufweist, um auslegungsgemäß seine Funktion zu erfüllen.

In Abhängigkeit der Betriebsbedingungen (Normalbetrieb, Störung oder Notfall) und der auszuführenden Funktionen (aktiv oder passiv) sind den FPGAs Qualitätscharakteristika zuzuweisen. Die Qualitätscharakteristika bestimmen die Stabilität und Widerstandsfähigkeit gegenüber Grenzwerten, die aus externen Einflussfaktoren resultieren, unter Berücksichtigung von Qualitätsmargen. Die Einhaltung der Qualitätscharakteristika wird mit Kontrollen und Audits beim Hersteller durch unabhängige Experten verifiziert.

2.4 Zusammenstellung von Prüfverfahren für komplexe programmierbare Baugruppen

2.4.1 Prüfungen beim Fertiger

Beim Fertiger durchzuführende Prüfungen sind in der IPC 610 für verschiedenen Qualitätsklassen beschrieben (siehe dazu Abschnitt 2.2.1). Darüber hinaus enthält das Amendment 1 zur DIN EN 60987 spezifische Anforderungen an den Fertigungsprozess. Diese beinhalten jedoch keine technischen Qualifizierungsverfahren und Tests.

2.4.2 Burn-in-Tests

Ein Burn-in-Test ist ein Test für die Simulation des Dauerbetriebes von Bauteilen, Komponenten, Leiterplatten und Geräten. Bei diesem Test geht es darum, im Vorfeld Komponenten zu finden, die im Dauerbetrieb ausfallen würden. Daher werden die zu testenden Komponenten unter hoher Belastung in einer Klimakammer über längere Zeiträume getestet. In den Klimakammern wirken die spezifizierten maximalen Temperatur- und Relativfeuchte-Werte für einen Zeitraum von z.B. 1000 Stunden auf den Prüfling ein. Normalerweise brennen in einem solchen Burn-in-Test fehlerhafte Bauteile durch, die in den vorherigen Funktions- und Röntgentests nicht als fehlerhaft erkannt werden konnten. Der Burn-in-Test unterscheidet sich vom 1000 Stunden Test gemäß KTA 3503 durch die hohe funktionale Belastung der Komponente.

Burn-in-Tests erfordern keine Beeinflussung der Testobjekte von außen sondern spezielle Testsoftware, die die Komponenten einer Baugruppe oder eines Gerätes einer hohen Last aussetzt. Zur Unterstützung der Testwirksamkeit kann die Umgebungstemperatur und die Versorgungsspannung erhöht werden. Dazu benötigte Testsysteme sind kommerziell am Markt verfügbar (z.B. Burn-In-Testsystem Serie EBI der ET Instrumente GmbH, Hockenheim).

Für Standard-PCs sind kommerzielle Programme für Burn-in-Tests am Markt verfügbar (z.B. BurnIn-Test™ von PassMark® Software /PAS 12/). Für spezielle leittechnische Baugruppen ist Spezialsoftware erforderlich, die baugruppen- bzw. gerätespezifisch entwickelt werden muss.

Burn-in-Tests werden für Baugruppen mit hochintegrierten Bauelementen (CPUs, FPGAs) als sinnvolle Ergänzung zur KTA-Typprüfung gesehen.

2.4.3 Highly Accelerated Life Test (HALT)

Ein Highly Accelerated Life Test (hoch beschleunigter Lebenszyklus-Test, abgekürzt HALT) ist ein Testlauf mit dem Ziel, elektronische Baugruppen einer beschleunigten Alterung zu unterwerfen, um Schwachstellen und Designfehler aufdecken zu können. Die Alterung erfolgt dabei durch Temperatur und Vibration /WP 01/.

Der HALT Test wurde ursprünglich zum Testen von elektronischen Geräten, welche in der Raumfahrt eingesetzt werden, entwickelt. Das Ziel war das Gerät einer Kombination von Schock, Vibration und großen Temperaturschwankungen zu unterwerfen.

Der Test wird typischerweise bis zur Zerstörung des Prüflings durchgeführt.

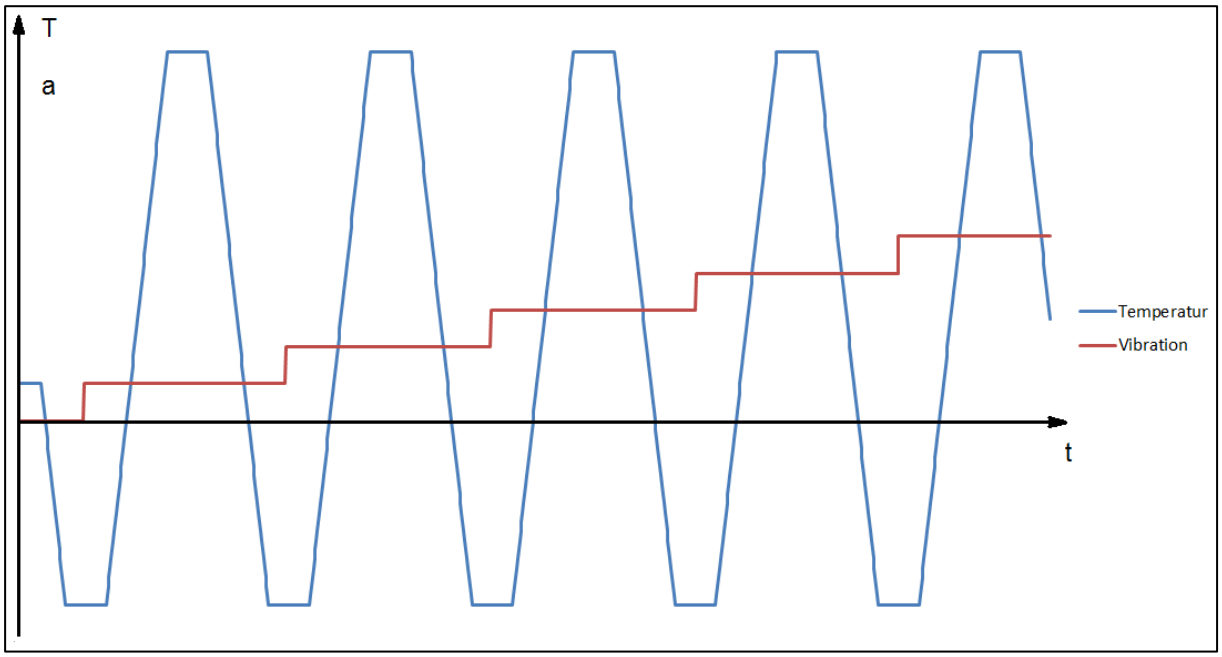

Bild 2.5: Typischer Ablauf eines HALT

Tabelle 2.4: Beispielhafte Werte für den HALT:

	Frequenzspektrum	Beschleunigung
Vibration	20 Hz – 10.000 Hz	bis 50 g
	Temperaturbereich	Temperaturgradient
Temperatur	-100 °C bis +200 °C	bis ΔT_{max}: 80 K/min

Vorgehensweisen zum HALT sind in verschiedenen Standards beschrieben. Dazu zählen:

- JEDEC Standard No.22-110B: Highly Accelerated Temperature and Humidity Stress Test
- JEDEC Standard No.22-118: Accelerated Moisture Resistance - Unbiased HAST

- IEC Publication 60068-2-66 (1994-6): Damp Heat Steady State
- IEC Publication 60749 Amendment 1: Damp Heat, Steady State Highly Accelerated
- EIAJ ED-4701 Method B-123: Unsaturated Vapor Pressure Test

Der HALT orientiert sich in seinem Belastungsspektrum an den Erfordernissen der Luft- und Raumfahrt. Diese unterscheiden sich grundlegend von den Belastungen für die Leittechnik in Kernkraftwerken, z.B. in Anforderungen zur Störfallfestigkeit. Für Baugruppen, die Störfallbedingungen unterliegen, gibt es in der Kerntechnik spezielle Störfallfestigkeitsprüfungen. Er wird deshalb kein Bedarf für einen HALT für leittechnische Baugruppen für Kernkraftwerke gesehen.

2.4.4 Highly Accelerated Stress Screening

Das Highly Accelerated Stress Screening (kurz HASS) ist eine Belastungsschnellprüfung mit dem Ziel, vorzugsweise elektronische Baugruppen während der Produktion intensiv zu testen, um initiale Fehler, die zu Frühausfällen führen aufdecken zu können. Dazu werden einzelne oder alle gefertigten Teile einem kurzen, intensiven Test mit Temperaturwechseln und Vibration unterworfen. Die Prüfschärfe wird so gewählt, dass Gut-Teile nicht zerstört, schadhafte Teile aber zuverlässig detektiert und ausgesondert werden können.

Das Highly Accelerated Stress Screening weist Parallelen zum Highly Accelerated Life Test auf. Es wird deshalb auch hier kein Bedarf für diesen Test für leittechnische Baugruppen für Kernkraftwerke gesehen.

2.4.5 Highly Accelerated Stress Test

Der Highly Accelerated Stress Test (HAST) wurde Ende der 1960iger Jahre entwickelt. Er basiert auf der Belastung des Prüflings mit erhöhter Temperatur und Feuchte. Daraus wird nach der folgenden Beziehung ein Alterungsfaktor AF bestimmt:

$$AF = e^{c*({RH_1}^n - {RH_0}^n)} * e^{\frac{E_a}{k}*\left(\frac{1}{T_0}-\frac{1}{T_1}\right)}$$

RH - relative Feuchte [%]

T - Temperatur [K]

c - empirische Konstante

n - empirische Konstante (gewöhnlich gilt 1 < n < 5)

E_a - Aktivierungsenergie

k - Boltzmannkonstante

Diese Methode weist Ähnlichkeiten zu Voralterungstests im Rahmen der Störfallfestigkeitsprüfungen auf. Ein wesentlicher Parameter für den Alterungsfaktor AF ist die materialabhängige Aktivierungsenergie E_a. Sie ist für komplexe Baugruppen, die Bauelemente aus unterschiedlichsten Materialien mit unterschiedlichen Aktivierungsenergien beinhalten, nur bedingt anwendbar, da die Ergebnisse für die funktionsbestimmenden Bauteile zu ungenau sind.

2.5 Einsatz industrieller Serienprodukte in der Sicherheitsleittechnik von KKW - Vorgehen nach VDI 3528

Die Richtlinie 3528 „Anforderungen an Serienprodukte und Kriterien für deren Einsatz in der Sicherheitsleittechnik in Kernkraftwerken“ /VDI 11/ wurde vom Fachausschuss 7.11 „Leittechnik in Kernkraftwerken“ der VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA) erarbeitet. Im Fachausschuss sind Experten verschiedener Interessensgruppen vertreten, wie beispielsweise Hersteller von Kraftwerkstechnik, Betreiber von Kernkraftwerken und verschiedene Gutachter.

Die VDI/VDE Richtlinie 3528 gibt Empfehlungen zu den grundsätzlichen Anforderungen, die Serienprodukte erfüllen müssen und definiert Kriterien, um diese für Funktionen der Sicherheitsleittechnik im KKW einsetzen zu können. Dies kann beispielsweise durch die Feststellung der Eignung bei Vorliegen adäquater Prüfzeugnisse aus anderen technischen Bereichen erfolgen, wobei noch zusätzliche Prüfungen zur Ergänzung der Qualifikation erforderlich sein können. Ebenso können Architekturen von Produkten zum Einsatz kommen, die z.B. durch höhere Redundanzgrade einen höheren Grad der Fehlertoleranz aufweisen. Ziel ist es, leittechnische Systeme unter Verwendung industrieller Serienprodukte, die nach konventionellem Regelwerk qualifiziert sind, zu realisieren, die als System Zuverlässigkeitswerte aufweisen, die äquivalent zu denen von Systemen sind, die nach kerntechnischen Normen gefertigt und geprüft wurden.

Die VDI/VDE Richtlinie 3528 ist in mehrere Teile gegliedert. Das Hauptblatt gibt Empfehlungen zu den übergeordneten Anforderungen und Kriterien an Serienprodukte, um diese für sicherheitstechnische Funktionen der Kategorien A, B und C einsetzen zu können. In den Folgeblättern werden die Anforderungen und Kriterien für einzelne Produktgruppen abhängig von der beabsichtigten sicherheitstechnischen Funktion und Bedeutung im Anlagenkontext, dem typischen Produktaufbau und den Einsatzrandbedingungen konkretisiert. Es werden Wege beschrieben, wie die einsatzspezifischen Anforderungen herausgearbeitet und geeignete Produkte und Strukturen ausgewählt werden können (evtl. sind ergänzende Qualifizierungen erforderlich). Die Ergebnisse und Lösungen werden in Checklisten dokumentiert. Zum Zeitpunkt der Berichtserstellung sind Folgeblätter für die Produktgruppen Messumformer, Sensoren und Schutzgeräte der Elektrotechnik in Bearbeitung, die in ihrer Schutzfunktion mit Funktionen der Sicherheitsleittechnik zusammenwirken.

Die Empfehlungen der VDI/VDE Richtlinie 3528 beziehen sich auf die Errichtung oder Änderung von elektro- und leittechnischen Einrichtungen in KKWs, deren Funktionen in die Kategorien 1, 2 und 3 der RSK-LL oder die Kategorien A, B und C der DIN IEC 61226 eingestuft sind. Die Empfehlungen dieser Richtlinie sollen als Ergänzung zu den Richtlinien zur Systemauslegung wie RSK-LL, KTA 3501, DIN IEC 61513, DIN IEC 60880, DIN IEC 62138 angewendet werden. Die Empfehlungen betreffen alle Komponenten, die zur Erfüllung der leittechnischen Funktionen erforderlich sind, angefangen beim Sensor und Messumformer über die Verarbeitungseinheiten bis zu den Schalt- und Schutzgeräten und die leittechnischen Komponenten von Antrieben (z. B. zur Rückmeldung). Die Empfehlungen dieser Richtlinie berücksichtigen damit sowohl die Errichtung oder den Austausch eines gesamten Leittechniksystems als auch den Ersatz von einzelnen peripheren Komponenten durch einen anderen Typ.

Um die Auslegungsziele leittechnischer Systeme unter Verwendung von Serienprodukten mit unterschiedlichen Qualifizierungstiefen zu erreichen, werden drei konzeptionelle Design-Varianten so definiert, dass durch unterschiedliche Schwerpunkte bei der leittechnischen Systemkonfiguration die gleiche Zuverlässigkeit für Funktionen einer bestimmten Sicherheitskategorie realisiert werden kann. Die erste Designvariante umfasst die Serienprodukte, für die keine Typprüfung oder Vergleichbares vorliegt. Designvariante zwei erfasst die industriell typgeprüften Serienprodukte und Designvariante drei die kerntechnisch typgeprüften Serienprodukte.

2.5.1 Designvariante 1

Bei dieser Variante dürfen lediglich Serienprodukte zum Einsatz kommen, die aus technischer Sicht für den Aufbau von hochzuverlässigen Systemen geeignet sind. Weiterhin sollen für diese Serienprodukte vom Hersteller aufgrund von hohen Stückzahlen und vielfältigen Anwendungen belastbare Angaben zur Betriebserfahrung dargelegt werden. Nachweise einer vom Hersteller unabhängigen Prüforganisation sind hierzu nicht zwingend.

Die Verwendung von Serienprodukten der Designvariante eins kann durch zusätzliche Maßnahmen bezüglich Fehlertoleranz, Funktionsverteilung und Funktionsparallelität auf Systemebene legitimiert werden. Damit kann auch bei einer konservativ angenommenen erhöhten Fehlerrate der Einzelgeräte die erforderliche Funktionszuverlässigkeit des Gesamtsystems erreicht werden. Für den Nachweis der Erhaltung der Produktqualität wird ein Qualitätspass etabliert, mit dem begleitend zum Einsatz die Betriebserfahrungen und die Änderungen der Gerätetechnik mitverfolgt und beurteilt werden.

Auf der Basis der genannten Maßnahmen und Nachweise sowie weiteren Angaben des Herstellers zu den wesentlichen Produkteigenschaften muss die Erfüllung der sicherheitstechnisch relevanten Anforderungen des Einsatzes durch eine vom Hersteller unabhängige Organisation bestätigt werden. Die Durchführung von zusätzlich erforderlichen Tests und Analysen sowie die resultierenden Ergebnisse müssen dokumentiert werden. In der Regel handelt es sich hier um einsatzfallbezogene Nachweise.

Die Designvariante eins ist nur für die Realisierung von Funktionen der Kategorie B oder C nach DIN IEC 61226 zulässig. Es müssen Voraussetzungen erfüllt sein, die im Rahmen einer detaillierten Analyse spezifisch für den Einsatzfall geklärt bzw. nachgewiesen werden müssen. So ist unter anderem nachzuweisen, dass die Serienprodukte mit ausreichenden Selbstüberwachungsmechanismen und mit der Fähigkeit, fehlertolerante Redundanzstrukturen zu bilden sowie mit einem gerichteten Ausfallverhalten ausgestattet sind. Die Serienprodukte müssen über ausreichende Möglichkeiten zur Protokollierung von Fehlerzuständen und zu Instandhaltungsmaßnahmen verfügen. Außerdem muss der Hersteller für Erfahrungsrückfluss bereit sein und ausreichend Ersatzteile müssen vorgehalten werden.

Zur Vermeidung des Eintragens von Fehlern während des Betriebs mit redundanzübergreifenden Auswirkungen ist ein spezifisches Instandhaltungsmanagement erforderlich. Hierbei ist sicherzustellen, dass beim Einsatz von Baugruppen mit neuen Versionsständen die potenziellen Auswirkungen begrenzt bleiben. Da die Prüfbarkeit der Kompatibilität zwischen alten und neuen Versionsständen bei integrierten Systemen begrenzt ist, dürfen neue Versionsstände von Baugruppen, die durch Hardware- oder Softwareänderungen bedingt sind, zunächst in nur einem von mehreren unabhängigen redundanten Teilsystemen eingebaut

werden und dürfen erst nach einer Bewährungsphase in weiteren Teilsystemen eingesetzt werden.

Für Funktionen der Kategorie B gilt zudem, dass nur solche Leittechnikfunktionen realisiert werden, die immer sicherheitsgerichtet sind und die bei aktivem Versagen zu keiner Anforderung von Funktionen der Kategorie A führen.

2.5.2 Designvariante 2

Produkte der Designvariante zwei sind speziell für industrielle Sicherheitsanwendungen entwickelt worden und mit für den Anwendungsfall geeigneten Zuverlässigkeitseigenschaften ausgestattet. Es wurde eine Typprüfung oder Baumusterprüfung dokumentiert und durch ein akkreditiertes Prüfinstitut bestätigt (z. B. gemäß DIN EN 61508). Auf dieser Basis kann die erforderliche Funktionszuverlässigkeit des Leittechniksystems durch angemessene Maßnahmen zur Fehlertoleranz, Unabhängigkeit, Funktionsverteilung und Funktionsparallelität erreicht werden.

Zusätzliche Nachweise sind erforderlich, falls sich dies aus der Eignungsüberprüfung im Vergleich zu den Anforderungen aus dem vorgesehenen Einsatzfall ergibt. Diese zusätzlichen Nachweise können durch den Hersteller erbracht werden. Die Durchführung der hierzu erforderlichen Tests und Analysen sowie die resultierenden Ergebnisse müssen dokumentiert werden.

Bei der Eignungsprüfung muss die Qualifizierungsgrundlage (z. B. SIL nach DIN EN 61508) entsprechend der sicherheitstechnischen Aufgabenstellung festgelegt werden. Typgeprüfte oder baumustergeprüfte Serienprodukte werden nach Änderungen einer umfassenden Prüfung durch ein Prüfinstitut unterzogen, um ihren Status entsprechend den Anforderungen für Designvariante 2 zu behalten.

2.5.3 Designvariante 3

Produkte der Designvariante drei sind speziell für den Einsatz im Sicherheitssystem in Kernkraftwerken typgeprüft worden. Die Grundlage für diese Typprüfung bilden die kerntechnischen Regeln des KTA, der DIN EN und der DIN IEC. Der Einsatz eines für das Sicherheitssystem typgeprüften Produktes gestattet aufgrund der nachgewiesenen Eigenschaften eine höhere Konzentration von Funktionen in dem leittechnischen Geräte im Vergleich zu Geräten, die nach den Designvarianten 1 oder 2 ausgelegt sind.

Zusätzliche Nachweise sind nur erforderlich, falls sich dies aus der Eignungsüberprüfung im Vergleich zu den Anforderungen aus dem vorgesehenen Einsatzfall ergibt. Die Durchführung der hierzu erforderlichen Tests und Analysen sowie die resultierenden Ergebnisse müssen dokumentiert werden. In der Regel werden diese zusätzlichen Nachweise als Erweiterung der zertifizierten Typprüfung behandelt.

Die VDI/VDE Richtlinie 3528 skizziert verschiedene Qualifizierungsverfahren, um den Auslegungsanforderungen der Funktionen der Kategorie A, B oder C gerecht zu werden. Für Funktionen der Kategorie A ist der Einsatz von Serienprodukten der Designvariante eins ausgeschlossen. Für Funktionen der Kategorien B und C sind im Allgemeinen alle drei Designvarianten möglich und somit auch Serienprodukte einsetzbar.

Bei der Systemauslegung sind in jedem Fall Maßnahmen zur Beherrschung von zufälligen Fehlern, Folgefehlern und systematischen Fehlern, auch unter Berücksichtigung des Instandhaltungsfalls, zu berücksichtigen. Bei Funktionen der Kategorie A muss in jedem Fall die Beherrschung des systematischen Fehlers ein besonderer Schwerpunkt sein. Einen wesentlichen Stellenwert für die Funktionen der Kategorien A und B hat die Überprüfung der Eignung für den spezifischen Einsatzfall. Dazu müssen die in der Typprüfung nachgewiesenen Eigenschaften und Maßnahmen an den Anforderungen des kerntechnischen Regelwerks gespiegelt und die angemessene Erfüllung dieser Anforderungen bestätigt werden.

Das folgende Bild veranschaulicht das Qualifizierungsverfahren von Produkten für Funktionen der Kategorie B.

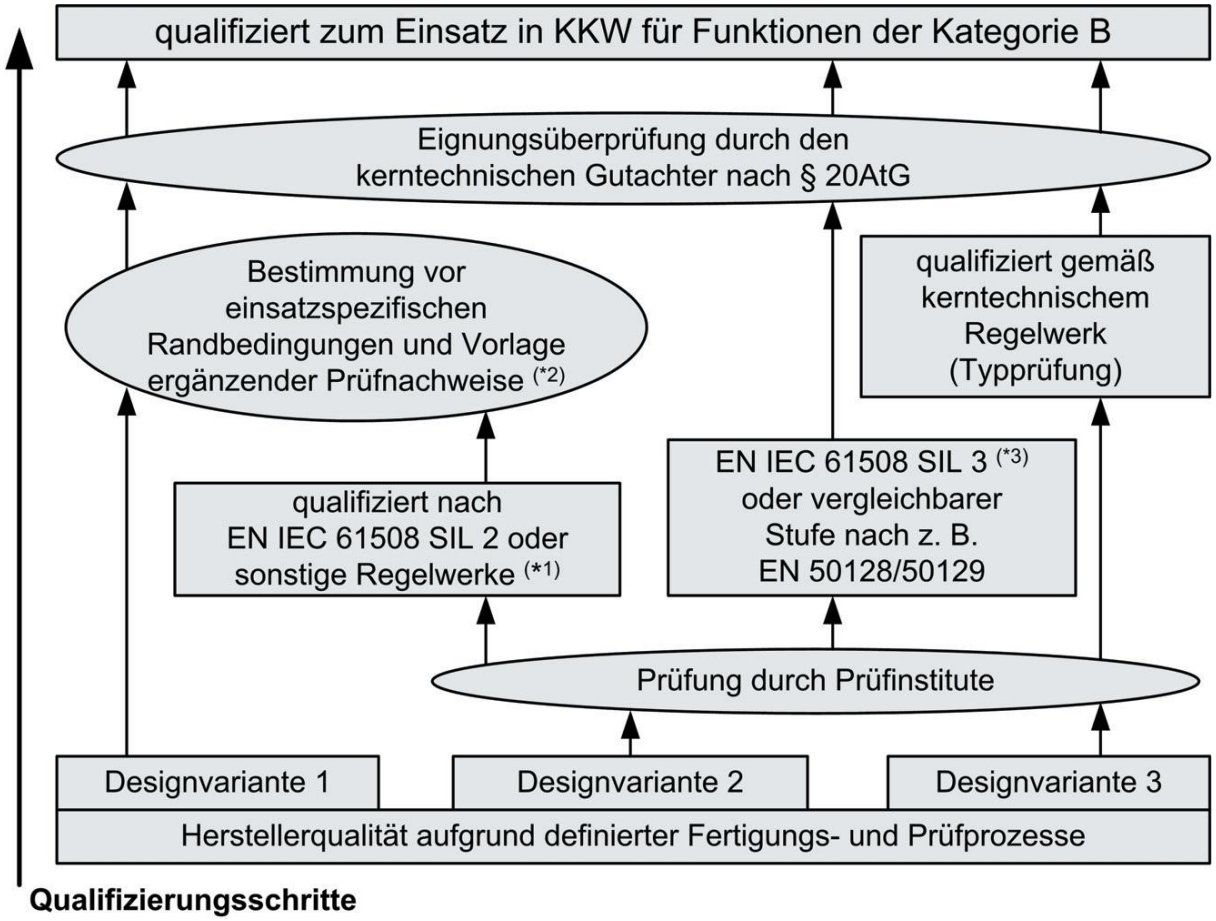

Bild 2.6: Qualifizierungsverfahren von Produkten für Funktionen der Kategorie B /VDI 11/

(*1) Qualifizierungen nach anderen Regelwerken (z. B. VDE, IEEE, Wehrtechnische Dienststelle für Schiffe und Marinewaffen WDT 71, German Lloyd, ATEX, NAMUR, ASME) müssen im Rahmen der einsatzspezifischen Eignungsüberprüfung zunächst hinsichtlich der Abdeckung der zugrunde zu legenden Anforderungen geprüft werden.

(*2) Festlegungen hierzu sind in der VDI 3528 getroffen.

(*3) Die Festlegungen erfolgen hierbei im Einzelfall abgestuft nach der sicherheitstechnischen Bedeutung der leittechnischen Funktion sowie in Abstimmung zu den bestehenden Anlagenrandbedingungen und der beabsichtigten Designvariante. Der geforderte SIL-Level

kann wahlweise durch Komponenten der geforderten Qualifikation oder durch ein Kombinationsprodukt mit der entsprechenden Struktur erreicht werden.

2.5.4 Äquivalenzprinzip

Mit dem Äquivalenzprinzip können leittechnische Systeme mit hoher bzw. höchster Zuverlässigkeit unter Nutzung von Produkten (auch Serienprodukte) mit einem niedrigeren Qualifizierungslevel realisiert werden. Durch den Einsatz von diversitären Produkten mit einem vergleichbaren Qualifizierungslevel in geeignet verschalteten redundanten Strukturen ergibt sich die Möglichkeit, die Erfüllung des nächst höheren Qualifizierungslevels in Anspruch zu nehmen. Dazu muss die Diversität in den zur Fehlerbeherrschung wichtigen Eigenschaften aufgezeigt werden.

Ziel des Äquivalenzprinzips ist es, durch die Kombination industrieller Serienprodukte für die damit realisierte Architektur eine Versagenssicherheit des Gerätes zu erreichen, die äquivalent zu der eines nach kerntechnischen Normen entwickelten, gefertigten und geprüften Gerätes ist. Da es für rechnerbasierte Systeme keine anerkannte Methodik zu einer Berechnung der Zuverlässigkeit gibt, muss die hier angesprochene Vergleichbarkeit mittels einer ingenieurmäßigen Bewertung plausibel gemacht werden.

Bei der Anwendung des Äquivalenzprinzips sind gleichwohl Einschränkungen zu beachten. Das Äquivalenzprinzip darf nicht eingesetzt werden,

- für frei programmierbare oder frei parametrierbare multifunktionale Produkte, da das Zusammenwirken des diversitären Kombinationsprodukts nicht allgemein gültig festgelegt werden kann und damit einer Typprüfung nicht zugänglich ist.
- falls angenommen werden muss, dass ein Mangel, der im Qualifizierungsprozess der diversitären Produkte nicht aufgedeckt sein könnte, im Anforderungsfall zum gleichzeitigen Versagen von beiden Typen führen könnte.
- um durch eine rekursive Anwendung zwei Stufen zur Erfüllung des geforderten Integritätslevels zu überbrücken.
- falls Leittechnikstrukturen zum Einsatz kommen, welche bei bestimmten Anforderungen die gleichzeitige Verfügbarkeit der diversitären Produkte voraussetzen.
- falls die diversitären Produkte einen signifikant unterschiedlichen Qualifizierungslevel aufweisen.

Dabei müssen die aus den unterschiedlichen Systemteilen generierten Signale im Sinne der sicherheitstechnischen Aufgabenstellung bewertet bzw. verknüpft werden.

2.5.5 Aspekte zur Vorauswahl

Vor der Festlegung auf ein Produkt sollte entsprechend DIN EN 61513 dessen Eignung eingeschätzt und untersucht werden. Es sollten die wesentlichen Fragen zur Dokumentation, zu den technischen Eigenschaften und zu den qualitativen und betrieblichen Aspekten beantwortet werden.

So sollten beispielsweise für die auszuwählenden Produkte die wichtigsten beschreibenden und qualifizierenden Dokumente vorliegen (z. B. Systembeschreibung, Aufbau der Haupt-

komponenten, Schnittstellen zu anderen Systemen, Entwicklungsdokumentation, Qualifizierungsnachweise, usw.).

Die erforderlichen sicherheitstechnisch relevanten Eigenschaften und Architekturmerkmale sind nachzuprüfen. Hierbei ist unter anderem auf Überwachungsmechanismen, Fehlererkennung, definiertes Ausfallverhalten und die Möglichkeit zum Aufbau verteilter und redundanter Systeme zu achten. Die für den Betrieb relevanten und spezifizierten Umweltbedingungen sind zu bewerten.

Die in Betracht zu ziehenden Produkte werden auf ihre qualitativen Eigenschaften, auch hinsichtlich ihres Fertigungsprozesses, untersucht. Es sollte auch berücksichtigt werden, inwieweit der Hersteller Rückinformation über Mängel seiner Produkte systematisch erfasst und beseitigt. Der Hersteller sollte eine Produktstrategie verfolgen, die für die Ersatzteilstrategie belastbar ist. Das Produkt sollte ausreichende Eigenschaften zur Instandhaltbarkeit aufweisen und diese sollten ohne Fehlauslösungen durchgeführt werden können. Dazu sind beispielweise Diagnose- und Prüfmöglichkeiten erforderlich und eine gewisse Austauschbarkeit muss gewährleistet sein.

Bei der Bewertung der Akzeptanz stehen die funktionale Eignung und der Korrektheitsnachweis im Vordergrund. Vor dem Hintergrund der langen Einsatzzeiten in kerntechnischen Anlagen sollten jedoch auch Aspekte wie Produktlebensdauer und Langzeitunterstützung abgewogen werden. Serienprodukte sind in der Regel auf eine breite Vermarktbarkeit ausgerichtet. Eine projektbezogene Beeinflussung ist meistens nicht oder nur in geringem Umfang möglich. Serienprodukte unterliegen häufig Produkt- oder fertigungsbezogenen Versionsänderungen.

2.5.6 Qualitäts- und Auslegungsmerkmale

Abhängig von der betroffenen Sicherheitskategorie und der gewählten Designvariante sind unterschiedliche Anforderungen an die Qualität und Systemauslegung zu stellen. Für alle Designvarianten gilt, dass das Qualitätsmanagement des Herstellers durch ein herstellerunabhängiges Zertifikat oder durch ein herstellerunabhängiges, produktspezifisches Audit nachgewiesen werden muss.

Die für den Einsatzfall geforderten und vom Hersteller zugesicherten Produkteigenschaften müssen nachgewiesen und dokumentiert sein. Für das projektspezifische Engineering und die Generierung der Anwendersoftware sollten Softwarewerkzeuge des Herstellers verfügbar sein. Die systemimmanenten Mechanismen zur Selbstüberwachung können durch projektierte, aufgabenspezifische Selbstüberwachungsmechanismen ergänzt werden. Zusätzlich muss die Durchführung von wiederkehrenden Prüfungen vorgesehen werden.

Die bei der Produktentwicklung berücksichtigten Regelwerke sind für die Designvarianten in unterschiedlicher Form zu belegen. Für Designvariante eins ist es ausreichend den Qualitätsstandard der Produkte in Form von Herstellererklärungen aufzuzeigen. Für Designvariante zwei müssen zusätzlich zu diesen Herstellererklärungen Prüfberichte und Zertifizierungen durch unabhängige Prüfinstitutionen in Form einer dokumentierten Typprüfung vorgelegt werden. Bei Designvariante drei müssen darüber hinaus bei der Produktentwicklung die nuklearspezifischen Anforderungen erfüllt sein. Die Nachweise hierzu müssen durch Dokumente zur Typprüfung sowie zur Zertifizierung durch unabhängige Prüfinstitutionen vorgelegt werden.

Als Basis für den projektspezifischen Designprozess muss eine geeignete Dokumentation des Herstellers für den Einsatz der auszuwählenden Produkte vorliegen. Gegebenenfalls müssen Dokumente projektbezogen bis zu einer begutachtbaren Detaillierung ergänzt werden. Wenn Betriebserfahrungen zur Bewertung der einzusetzenden Produkte herangezogen werden sollen, sind folgende Akzeptanzkriterien für die Nachweise zu erfüllen:

- die realisierten Konfigurationen müssen nachvollziehbar dokumentiert sein.
- die Serienprodukte müssen aus einer stabilen Produktphase stammen.
- die Betriebserfahrung muss auf einem relevanten Anforderungsprofil basieren.
- die Daten und Informationen aus der Betriebserfahrung sollten nachvollziehbar und über ein angemessenes Zeitintervall aufgezeichnet sein.
- die Ereignisdaten sollten Aufschluss über das Potenzial für Ausfälle mit gemeinsamer Ursache geben.
- Maßnahmen zur Instandhaltung und Modifikation der softwaregestützten Serienprodukte sollten chronologisch aufgezeichnet werden.
- Bei der Auswertung der Betriebserfahrung sollte zwischen Fehlhandlungen bei Tätigkeiten zur Instandhaltung und Auslegungsfehlern unterschieden werden.

Beim Einsatz von Produkten mit integrierter Software sind Vorkehrungen gegen das systematische Versagen zu treffen. Vom Hersteller ist darzulegen, dass

- bei Eingriffen in die Leittechnik, z. B. zur Instandhaltung, keine unbeabsichtigten Änderungen, insbesondere keine redundanzübergreifenden Änderungen, eingetragen werden können.
- bei Kommunikation zwischen redundanten Komponenten, insbesondere über Datenbusse, keine unzulässigen Rückwirkungen auf die redundanten Komponenten auftreten können.
- fehlerhafte Daten/Eingangssignalen zu einer definierten Reaktion der Leittechnik führen.
- erhöhtes Datenaufkommen zu keiner fehlerhaften Reaktion der Leittechnik führt.
- zeitabhängige Störungen der integrierten Software durch entsprechende Auslegungsmaßnahmen vermieden werden.
- die relevanten Maßnahmen zur Robustheit der Software angemessen implementiert sind.

Ziel ist hier, dem gleichzeitigen Versagen von mehreren Komponenten aufgrund von spezifischen Eigenschaften der integrierten Software entgegenzuwirken. Die Beherrschung von Einzelfehlern muss durch die redundante Realisierung der Hauptfunktion abgedeckt sein.

Bei Projektierung, Inbetriebsetzung und Betrieb sind qualitätssichernde Maßnahmen zu ergreifen. Ein Verifikations- und Validationsplan muss unter Berücksichtigung der zugesicherten Produkteigenschaften erstellt werden. Ein effektives Konfigurations- und Änderungsmanagement sowie Prinzipien zur Identifizierung aller relevanten Produktelemente müssen eingeführt sein.

Falls gleichartige Produkte in verschiedenen Systemen, die Funktionen unterschiedlicher sicherheitstechnischer Bedeutung ausführen, eingesetzt werden, sollen geänderte Produkte zuerst in Systemen mit geringerer sicherheitstechnischer Bedeutung zum Einsatz kommen. Werden geänderte Produkte in redundanten Strängen eines Systems eingesetzt, so soll der Einsatz in den unterschiedlichen Redundanten mit einer hinreichenden zeitlichen Staffelung erfolgen, um das Potenzial für systematische Ausfälle zu begrenzen.

Die Vorgehensweise nach VDI 3528 ist für Geräte aus industrieller Serienfertigung anwendbar. Da Geräten aus Sonderfertigungen wesentliche Merkmale von Serienprodukten fehlen (z.B. Betriebserfahrung) ist sie ist nur für Geräte aus Sonderfertigungen, die Funktionen der Kategorie C ausführen und mit entsprechenden Zusatzprüfungen für Geräte, die Funktionen der Kategorie B ausführen, anwendbar.

2.6 Anforderungen an die WKP, Wartung und Konfigurationsmanagement eines CEC Redesigns anhand internationaler Anforderungen unter besonderer Berücksichtigung deutscher Belange

Ziele der wiederkehrenden Prüfung sind:

- verborgene Hardwarefehler, die nicht von der implementierten Selbstüberwachung aufgedeckt werden, zu erkennen und
- den Nachweis der Erfüllung der spezifizierten Leittechnikfunktionen zu erbringen und damit die vorgegebenen Verfügbarkeitsanforderungen zu bestätigen.

Im Detail wird für die Gestaltung der wiederkehrenden Prüfungen gefordert, dass die o.g. Ziele durch Prüfungen von Teilsystemen zu erreichen sind.

Die Signalpfade sollten rechnerübergreifend von den Messwertaufnehmern bis zu den Stellgliedern durchgehend oder überlappend in Teilbereichen geprüft werden (IEC 61513 Ed. 2, 6.2.2.3.5 Testability).

Der Prüfvorgang muss zu jeder Zeit unterbrechbar sein, entweder manuell durch Aufhebung des Test-Freigabe-Signals oder automatisch in Betriebsarten, in denen kein Testen mehr zulässig ist.

Die Testintervalle sind unter Berücksichtigung der Zuverlässigkeitsanalysen und –vorgaben festzulegen.

Aufgedeckt werden dabei verborgene Hardwarefehler und verborgene zeitabhängige Systemfehler (Software-/Hardware-Interferenzen), die durch die Selbstüberwachungsmaßnahmen nicht erfasst werden können.

Die DIN IEC 60671 (4.4) räumt für leittechnische Einrichtungen mit der Fähigkeit, durch Selbstüberwachung (ausgeführt von systemeigenen oder zusätzlichen Geräten) Fehler innerhalb kurzer Zeitspannen nach ihrem Eintreten aufzudecken die Möglichkeit ein, wiederkehrende Prüfungen durch die Selbstüberwachung zu ersetzen. Dazu ist die Selbstüberwachung zu analysieren, um die durch sie aufgedeckten Ausfallarten zu ermitteln (DIN IEC 60671 (4.4.1)).

Für Teile, die nicht von der Selbstüberwachung erfasst werden, ist zu zeigen, dass die sicherheitstechnisch wichtigen Funktionen durch sie nicht beeinträchtigt werden oder es sind

Prüfungen im Rahmen der WKP vorzusehen (DIN IEC 60671 (4.4.2)). Eine sinngemäße Vorgehensweise wurde in die KTA 3506 (Fassung 2012) in Kap. 5 eingebracht.

Weiterhin fordert die DIN IEC 60671 (4.4.3), dass die durch die Selbstüberwachung aufgedeckten Gerätefehler dem Wartenpersonal durch geeignete Meldungen und Anzeigen zur Kenntnis gebracht werden.

Im Falle von FPGA Anwendungen sind demzufolge ebenfalls analog hierzu im Zuge von WKP die Korrektheit (Unversehrtheit) der auf dem Chip implementierten bzw. projektierten Verbindungen (z.B. Routen von vorkonfigurierten Schaltkreisen), Software, Schnittstellen und nicht zuletzt implementierten leittechnischen Funktion einschließlich der Hardware periodisch nachzuweisen. Dies ist einerseits notwendig da infolge recht kurzer Innovationszyklen von zwei bis drei Jahren kaum die Möglichkeit besteht hinreichende Betriebserfahrungen für die Hardware auszuwerten. Andererseits führt die zunehmende Miniaturisierung, die sich gegenwärtig im Nanobereich bewegt, dazu, dass die an sich recht strahlungsresistente CMOS Technologie im Nanobereich durchaus Sensitivitäten aufweist. In der Praxis hat sich gezeigt, dass ab Technologien von etwa 130 Nanometer die Strahlungssensitivität signifikant zunimmt.

Im Folgenden wird beispielhaft die Wirksamkeit der Selbstüberwachung von TELEPERM XS in Bezug auf die WKP dargestellt.

Die Selbstüberwachung, die durch die dafür implementierten Softwarekomponente in einem TELEPERM XS System ausgeführt wird, teilt sich in drei grundlegende Bereiche auf /SIE 00/:

- Basis Hardware Test (BHT)
- die Selbstüberwachung im Anlauf (SÜA) der Funktionsrechnerbaugruppen SVEx
- die zyklische Selbstüberwachung (ZSÜ) der Funktionsrechnerbaugruppen SVEx

Der Selbsttest im Anlauf (nach RESET, bestehend aus BHT und SÜA) der Funktionsrechnerbaugruppen SVEx prüft auch die Teile der Baugruppen SVEx, die nicht im laufenden Betrieb geprüft werden können. Bei der Feststellung von Fehlern der Baugruppen wird der weitere Anlauf bzw. der Übergang in den Betriebsmodus der Baugruppen verhindert.

Der Selbsttest im Anlauf gliedert sich in den Basis-Hardwaretest und die Selbstüberwachung im Anlauf nach HOT (HOT = Hardware Organisation Tool). Diese Aufteilung ist notwendig, da einerseits bestimmte Tests nur vor der durch HOT ausgeführten Initialisierung der Hardware ausgeführt werden können (z.B. Belegzeitüberwachung SSC/ESSC) und andererseits Tests erst nach der Hardwareinitialisierung ausgeführt werden können (z.B. Teile des RAM-Speichertests).

Die zyklische Selbstüberwachung wird ständig in den Zeiten, die nicht für die Bearbeitung der Anwendungsfunktionen (Funktionspläne) belegt ist, ausgeführt.

Einzelne Tests werden von anderen Komponenten der TELEPERM XS Software ausgeführt (siehe Tabelle 2.5).

Die Selbstüberwachung in einem TELEPERM XS System ist nur in der Kombination von Selbstüberwachung im Anlauf, zyklischer Selbstüberwachung und der Überwachung durch andere Komponenten des TXS Systems vollständig.

Tabelle 2.5: Übersicht über die Tests der Selbstüberwachung in TELEPERM XS /SIE 00/

Test	BHT	SÜA	ZSÜ	Testart	Anmerkung
Prozessorselbsttest	Nein	Nein	Nein	-	Bewertung erfolgt im *Bootlader*
Prozessortest	Ja	Ja	Ja	Funktional	
Coprozessortest	Nein	Ja	Ja	Funktional	
RAM-Speichertest	Ja	Ja	Ja	Stuck-at	
Flash-Speichertest	Nein	Ja	Ja	Prüfsumme	
Belegzeitüberwachung SSC/ESSC2	Ja	Nein	Nein	Funktional	
Kommunikationsspeicher	Ja	Ja	Nein	Stuck-at	
I/O-RAM	Ja	Nein	Ja	Stuck-at	
SSC/ESSC2-Interrupts	Nein	Ja	Ja	Funktional	
Virtual-Interrupts	Nein	Ja	Nein	Funktional	
Timer-Interrupts	Ja	Nein	Ja	Funktional	
Betriebswatchdog	Nein	Ja	Ja	Funktional	
NMI	-	-	-	-	Test erfolgt im Rahmen des Tests der Belegzeitüberwachung des SSCs/ESSC2s
USART	Nein	Ja	Nein	Funktional	
DMA-Controller	-	-	-	-	Wird im Rahmen des Projektes *TELEPERM XS* nicht verwendet und nicht getestet.
Timer-Test	-	-	-	-	Test erfolgt im Rahmen des Tests der Timer-Interrupts
KBUS-Test	-	-	-	-	Test erfolgt im Rahmen des Tests des Kommunikationsspeichers
SPAD	Nein	Ja	Ja	Prüfsumme	
E/A-Bus	Nein	Ja	Ja	Funktional	
Ports für ext. und onboard LEDs	Ja	Nein	Ja	Stuck-at	
LEDs für Laufbesonderheiten	Nein	Nein	Nein	-	
Baugruppenports	Nein	Ja	Ja	Funktional	
GEO- und Parametrierregister	Nein	Ja	Ja	Funktional, Prüfsumme	
Systemports	Nein	Ja	Ja	Funktional	
Brücken	Nein	Ja	Ja	Stellung	

Test	BHT	SÜA	ZSÜ	Testart	Anmerkung
EEPROM	-	-	-	-	Überprüfung erfolgt im Rahmen des *Bootladers* bzw. der *Ablaufumgebung*
Time-counter SVE2	-	Ja	Ja	Funktional	

In Tabelle 2.5 werden der DMA-Controller und die LEDs für Laufbesonderheiten als nicht getestet angegeben. Der DMA-Controller wird im Rahmen der Gerätefamilie TELEPERM XS nicht benutzt. Er ist deaktiviert und kann aus diesem Grund auch nicht bei einer WKP im Rahmen von Funktionstests getestet werden. Die LEDs zur Anzeige von Laufbesonderheiten werden von der Selbstüberwachung nicht erfasst. Sie sind durch Sichtprüfung während eines Reset mit nachfolgendem Anlauf prüfbar.

Die Selbstüberwachung wird durch eine Reihe von Tests realisiert, die in Tabelle 2.6 aufgelistet sind. Die Nummern der Tests sind in der Tabelle 2.7 referenziert.

Tabelle 2.6: Tests der Selbstüberwachung /SIE 00/

Nr.	Testbezeichnung
1	Prozessorselbsttest
2	Prozessortest
3	Test des Coprozessors
4	RAM-Speichertest vor HOT
5	RAM-Speichertest nach HOT
6	Flash-Speichertest
7	Test der Belegzeitüberwachung des SSCs
8	Kommunikationsspeichertest vor HOT
9	Kommunikationsspeichertest nach HOT
10	I/O-RAM-Speichertest
11	SSC/ESSC2-Interrupttest
12	Virtual-Interrupttest
13	Timer-Interrupttest
14	Test des Betriebswatchdogs
15	USART-Test
16	Test des SPADs
17	E/A-Bus-Test
18	Test der Ports für die externen und onboard LEDs
19	Test der Baugruppenports
20	Test der GEO- und Parametrier-Register
21	Test der Systemports
22	Test baugruppenspezifischer Brücken

Nr.	Testbezeichnung
23	Test des Time-Counters der SVE2

Die Testtiefe der einzelnen Tests der Selbstüberwachung ist unterschiedlich. Eine qualitative Bewertung der Testtiefe ist in Tabelle 2.7 angegeben, wobei N für „niedrig“, M für „mittel“ und H für „hoch“ steht.

Tabelle 2.7: Bewertung der Testtiefe der Selbstüberwachung für SVE2 /SIE 00/

Bauelement	Einbau-platz	Anz.	Test-Nummer																						
			1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**
Grundplatine			-	-	-	-	-	-	-	-	H	-	-	-	-	-	-	-	-	-	-	-	-	-	-
74ALS245, K32-Treiber	D1 - D8	8																							
Swapper-EPLD	D33	-	-	-	-	-	-	-	N	-	-	N	N	N	N	N	N	N	N	N	N	N	N	-	-
16245, ZBUS, Z-Swapper	D30, D35	2	-	-	-	-	-	-	-	M	M	-	-	M	-	-	-	-	-	-	-	M	-	-	-
7407, K32-Treiber	D9, D16	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	N	-	-
16244, Prozessor-Adr.	D29	1	N	N	N	H	H	H	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
16244, X6 und K32 Con-troller	D36	1	-	-	-	-	-	-	-	-	M	-	-	-	-	-	-	-	M	-	-	-	-	-	-
16240, BGR-Port	D41	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	M	M	-	-	-	-
RAM256k * 16, KSP	D10, D16	2	-	-	-	-	-	-	-	H	M	-	-	-	-	-	-	-	-	-	-	-	-	-	-
74LVTH125, CLK, divider	D26	1	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
ESSC2	D34	1	-	-	-	-	-	-	M	-	-	-	M	N	N	M	N	-	-	-	-	-	-	-	-
USART im ESSC2	D34	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	H	-	-	-	-	-	-	-	-

Bauelement	Einbau-platz	Anz.	Test-Nummer																					
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Interrupt-Controller im ESSC2	D34	-	-	-	-	-	-	-	-	-	-	-	H	H	M	-	N	-	-	-	-	-	-	-	-
IORAM im ESSC2	D34	-	N	N	N	N	N	N	N	N	N	H	N	N	N	N	N	M	N	M	N	N	N	N	N
Timer im ESSC2	D34	-	-	-	-	-	-	-	N	-	N	-	-	-	H	N	-	-	-	-	-	-	-	-	N
IO-Funktionalität im ESSC2	D34	-	-	-	-	-	-	-	-	-	-	N	-	-	N	N	N	-	-	M	N	-	M	N	n
Time-Counter im ESSC2	D34	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	M
MAX208E, V24-Treiber	N3, N4	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
7032, BGR-Port-EPLD	D37	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	H	-	-	-	M
16240, EXTLED	D41	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
64 MHz-Oszillator	G1	1	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
12 MHz-Oszillator für USB	G3	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
14,74 MHz-Oszillator (Baudr.)	G2	1	-	-	-	-	-	-	-	-	-	-	-	-	M	M	M	-	-	-	-	-	-	-	-
LEDs	H1 – H6	6	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Bauelement	Einbau-platz	Anz.	Test-Nummer																						
			1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**
Optokoppler	U1 – U3	3	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Prozessor Pentium/K6	D17	1	H	M	M	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
7256, ZBUS-EPLD	D19	1	-	-	-	-	-	-	-	M	H	-	-	M	-	-	-	-	-	-	-	M	M	N	N
7512, MEM-Controller	D32	1	N	N	N	M	M	M	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
7512, SPAD	D32	-	N	N	N	N	N	N	N	N	N	H	N	N	N	N	N	M	N	M	N	N	N	N	N
7256, Swapper-EPLD	D33	1	-	-	-	-	-	-	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Speichermodul																									
5C1008, RAM 128k * 8	D9 – D16	8	N	N	N	M	H	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
29DL163, Flash-EPROM	D17 – D20	4	N	N	N	N	N	N	H	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N

Aus der Tabelle 2.7 geht hervor, dass von der Selbstüberwachung nicht alle Bauelemente der SVE2 erfasst werden. Im Folgenden werden deshalb die nicht erfassten Bauelemente und die Erkennung und Meldung von Fehlern dieser Bauelemente betrachtet:

- MAX 208E, V24-Treiber, Einbauplatz N3, N4
  Es handelt sich hierbei um die Treiber der RS232 Schnittstelle. Es gelten dafür die gleichen Randbedingen wie für die V24-Treiber der SVE1.
- Optokoppler, Einbauplatz U1-U3
  Die Optokoppler werden für die Entkopplung von BASP-, WDG- und GATE2-Signal von der Schnittstelle X4.2 verwendet. Aktive Fehler der Optokoppler werden bei Verwendung dieser Signale durch das Auslösen von TELEPERM XS spezifischen Fehlerreaktionen (z.B. Abschaltung der Spannungsversorgung der E/A-Baugruppen) erkannt und gemeldet. Passive Fehler werden durch die Selbstüberwachung nicht erkannt.

Aus den obigen Ausführungen ist erkennbar, dass mit Ausnahme der Optokoppler die von der Selbstüberwachung nicht explizit getesteten Bauelemente der SVE2 von anderen Komponenten des TXS Systems überwacht werden. Im on-line Betrieb nichtverwendete Bauteile (12 MHz-Oszillator für USB, MAX208E, V24-Treiber) sind deaktiviert und können somit die sicherheitstechnische Funktion nicht beeinträchtigen. Die LEDs (16240, EXTLED, LEDs) sind für das TXS System nicht funktionsrelevant und können die Funktion nicht beeinträchtigen.

Der Prozessor einschließlich des arithmetischen Co-Prozessors ist der komplexeste Baustein einer Verarbeitungseinheit und deshalb ist der Test des Prozessors auch die komplexeste Aufgabe im gesamten Testumfang. Der Prozessortest umfasst:

- den Test der bedingten Sprungbefehle,
- den Test der Operationen der vier Grundrechenarten (Addition, Subtraktion, Multiplikation, Division) mit unterschiedlichen Datenformaten,
- den Test der logischen Operationen AND, OR, XOR, NOT.

Der Co-Prozessortest umfasst:

- den Test auf Vorhandensein des Coprozessors,
- den Test der Fehlerreaktion bei einer Division durch Null,
- den Test der vier Grundrechenarten (Addition, Subtraktion, Multiplikation, Division) mit Gleitkommazahlen,
- den Test trigonometrischer Funktionen mit der Beziehung sin2(x) + cos2(x) = 1.

Die genannten Tests sind so gehalten, dass im Fehlerfall eine Endlosschleife ausgeführt wird. Die Tests werden innerhalb der Basis-Hardwaretests, der SÜA und der ZSÜ durchgeführt.

Die Speichertests für die Schreib- / Lesespeicher (RAM) berücksichtigen die Beschreibbarkeit und die Lesbarkeit des Speichers sowie die Fähigkeit den Speicherinhalt zu halten. Durch die Korrelation von Dateninhalt und Adressinformationen wird auch die korrekte Adresse getestet. Der RAM-Speichertest ist nicht in der Lage das zufällige Kippen einzelner Bits innerhalb der Nutzdaten zu erkennen. Für Signaldaten (Wert und Status) und interne

Variablen, die in jedem Zyklus neu beschrieben werden, sind solche Fehler vernachlässigbar, da Signaldaten in jedem Zyklus neu beschrieben und diese Zufallsfehler dadurch korrigiert werden.

Wie im Schreiben von AREVA NP an KWB Biblis vom 19.03.2008 /ARE 08/ ausgeführt, kann die Selbstüberwachung unbeabsichtigte Veränderungen der änderbaren Parameter nicht ausreichend aufdecken. Dieser Sachverhalt trifft auch auf abgeleitete Parameter (diese werden im Anlauf einmalig berechnet und abgelegt) und Zustandsspeicher zu. Diese Speicherbereiche werden jedoch im Anlauf neu initialisiert.

Die Flash-Speicher, die als Festwertspeicher die Programme beinhalten, sind durch CRC-Prüfsummen gesichert. Die Prüfsummen selbst stehen in einem anderen Festwertspeicher (EEPROM). Jede Abweichung zwischen der von der Selbstüberwachung über die Flash-Speicherbereiche berechneten Prüfsumme von den im EEPROM gespeicherten Prüfsummen wird als Speicherfehler der Festwertspeicher behandelt.

3 MACHBARKEITSSTUDIE FÜR EINE KOMPLEXITÄTSMESSUNG ELEKTRONISCHER BAUGRUPPEN

3.1 Wissensrückfluss aus dem HARMONICS-Projekt

Eine der Grundlagen für die ISTec-Arbeiten im Projekt „Aufstellung von Kriterien und Kenngrößen zur deterministischen Prüfung der Eignung von Redesign-Baugruppen für den Einsatz in der Sicherheitsleittechnik von KKW“ war die Teilnahme am Projekt „HARMONICS“ („Harmonised Assessment of Reliability of Modern Nuclear I&C Software“), einem FP-7 Projekt der EU. Im HARMONICS-Projekt wurden auf dem neuesten Stand von Wissenschaft und Technik beruhende Methoden für die Qualifizierung der Software computerbasierter Sicherheitssysteme erprobt.

Am HARMONICS -Projekt waren die folgenden Organisationen beteiligt:

1. Teknologian Tutkimuskeskus VTT (Finnland), Projektkoordinator
2. Électricité de France S.A., EDF (Frankreich),
3. Adelard LLP (Großbritannien),
4. Institut für Sicherheitstechnologie (ISTec) GmbH (Deutschland),
5. Strålsäkerhetsmyndigheten – Swedish Radiation Safety Authority (Schweden).

Im HARMONICS-Projekt wurden verschiedenen Nachweismethoden für die Bewertung von moderner Sicherheitsleittechnik betrachtet und bezüglich ihres Anwendungsbereichs und ihrer Wirksamkeit verglichen. Die Komplexitätsmessung /MAE 10/ diente dazu, die für komplementäre Nachweismethoden auszuwählen Aspekte zu ermitteln. Dazu wurde eine beispielhafte, auf Software beruhende Anwendung bezüglich ihrer Komplexität und ihrer Strukturmerkmale untersucht. Im Ergebnis dieser Untersuchungen wurde eine Teilfunktion ermittelt, die mittels formaler Methoden auf Vollständigkeit und Korrektheit geprüft wurde. In gleicher Weise wurden Teilfunktionen für statistische Tests und weitere Untersuchungsmethoden ermittelt.

Darüber hinaus wurde im Rahmen des HARMONIC-Projekts eine Vorgehensweise für den Sicherheitsnachweis erarbeitet, die auf einem „Claim – Argument – Evidenz“ Prozess auf-

setzt. Diese Vorgehensweise kann für die Bewertung von Redesign-Baugruppen in folgender Weise angewandt werden:

1. Es werden die funktions- und sicherheitsrelevanten Eigenschaften einer zu ersetzenden Baugruppe ermittelt. Diese bilden den „Claim“ für die Redesign-Baugruppe.
2. Es sind die Argumente („arguments“) zusammenzustellen, die den Nachweis der in Anspruch genommenen Eigenschaften auch für die Redesign-Baugruppe beinhalten. Diese Argumente können durch Modellierung, formale Nachweismethoden, Simulation, Tests (z.B. Störfallfestigkeitsprüfungen, statistische Tests; Alterungstests usw.), Metriken (z.B. Komplexitätsmaße), usw. gebildet werden.
3. Der Nachweis wird durch allgemein anerkannte Eigenschaften und Merkmale („Evidenz“) erbracht, auf die die Argumente hinführen.

Das HARMONICS-Projekt ist inhaltlich abgeschlossen, die Berichte stehen jedoch noch nicht zur Verfügung.

3.2 Auswahl der Objekte für die Komplexitätsmessung

Die Auswahl der Objekte für die Machbarkeitsstudie für die Komplexitätsmessung soll ein breites Spektrum unterschiedlicher Technologien abdecken dabei aber überschaubar bleiben. Zum gegenwärtigen Zeitpunkt sind nur Redesign-Projekte initiiert, die Baugruppen in festverdrahteter bzw. Dickschicht-Hybridtechnik[2] nachbauen. Die eingesetzten Dickschicht-Hybridbauteile enthalten nach Aussage des VGB nur konventionelle Bauelemente bzw. Bauelemente geringer Integrationsdichte, d.h. keine FPGAs oder programmierbaren Bausteine / RSK 213/. Der Einsatz von Prozessor-, ASIC- oder FPGA-Baugruppen ist nach Aussage des VGB weder erfolgt noch geplant /RSK 213/.

Um das vorgesehene Spektrum unterschiedlicher Technologien abdecken zu können, wurden Ersatzbaugruppen unterschiedlicher Technologieklassen ausgewählt. Dazu wurden die folgenden Technologieklassen für leittechnische Baugruppen in KKW gebildet.

1. Konventionelle festverdrahtet Leitechnikbaugruppen (beispielhaft GEAMATIC) bzw. deren Redesigns in gleicher Technologie (nicht programmierbar)
2. Redesign einer Baugruppe in Dickschicht-Hybridtechnik (nicht programmierbar)
3. Baugruppen für komplexere Funktionen, die in analoger Technik existierten, und die durch sehr einfache digitale Baugruppen „redesigned“ wurden (beispielhaft Messwertkorrekturrechner, programmierbar)
4. Komplexe analoge Messwertumformer, die durch moderne Rechnerbaugruppen ersetzt wurden (rechnerbasiert).

Als Repräsentanten der Technologieklassen wurden ein Zeitverzögerungsbaugruppe XPH70 der GEAMATIC Baureihe (Technologieklasse 1), ein Signalumformer U/I vom Typ M74003-A9143 (Technologieklasse 2), ein Messwertkorrekturrechner TZA4 des Herstellers Hartmann & Braun als Ersatz für den in Analogtechnik gefertigten TZA20 (Technologieklasse 3), und

[2] Die Dickschicht-Hybridtechnik ist eine Aufbau- und Verbindungstechnik zur Herstellung elektronischer Schaltungen (Dickschicht-Hybridschaltung), bei welcher sowohl integrierte als auch diskrete Bauteile Verwendung finden.

ein intelligenter Messwertumformer DT100 des Herstellers CCI für Ventilstellungsanzeigen als Nachbau der analogen Baugruppe MOM13 (Technologieklasse 4) gewählt.

Die Auswahl der Baugruppen wurde durch die im ISTec vorhandenen Vorkenntnisse zu diesen Baugruppen mit bestimmt.

3.3 Strukturierung und Auswertung der Dokumentation

3.3.1 Zeitverzögerungsbaugruppe XPH70

In Bild 3.1 ist das Schaltbild eines Teilsystems einer Baugruppe XPH70 widergegeben. Auf der Baugruppe sind drei identische Teilsysteme aufgebaut. Ein am Eingang eintreffendes High-Signal wird um eine einstellbare Zeit (r46) verzögert am Ausgang ausgegeben.

Die Funktion dieser Schaltung ist vollständig unter Verwendung konventioneller analoger Bauteile aufgebaut. Eine solche Schaltung besitzt nur an den Ein- und Ausgängen klar definierte Signalflussrichtungen. Im Inneren einer solchen Schaltung sind derartige Signalflussrichtungen nur an ausgewählten Punkten darstellbar. In der Mehrzahl der internen Verdrahtungspunkte laufen dynamische Vorgänge ab, die im Falle eines Signalwechsels am Eingang von einem Gleichgewichtszustand in einen anderen Gleichgewichtszustand übergehen und dadurch das definierte Ausgangssignal nach Ablauf der Verzögerungszeit erzeugen.

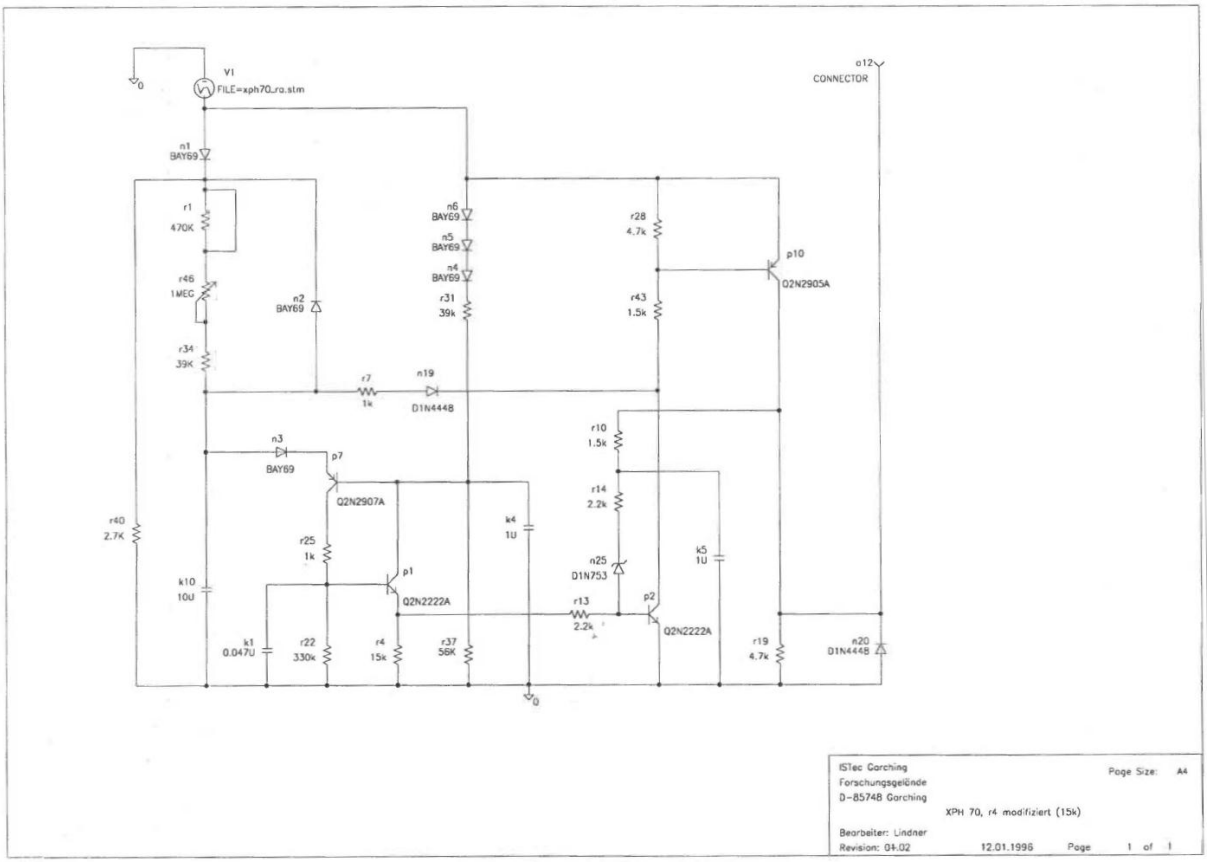

Bild 3.1: Schaltbild der Baugruppe XPH 70 /LIN 97/

Die Funktionalität der Baugruppe entspricht der Funktionalität eines Software-Funktionsbausteins eines gängigen rechnerbasierten Leittechniksystems.

3.3.2 Signalumformer I/U

In Bild 3.2 ist das Blockschaltbild einer Strom-Spannungswandler Baugruppe in konventioneller Technik (Typ M74003-A9143) dargestellt. Die Funktion besteht darin, ein anliegendes Spannungssignal in ein proportionales Stromsignal zu wandeln. Zusätzlich gibt es Prüfsignaleingänge und es wird eine Reihe von Meldesignalen erzeugt.

In diesem Blockschaltbild sind Signalflüsse identifizierbar.

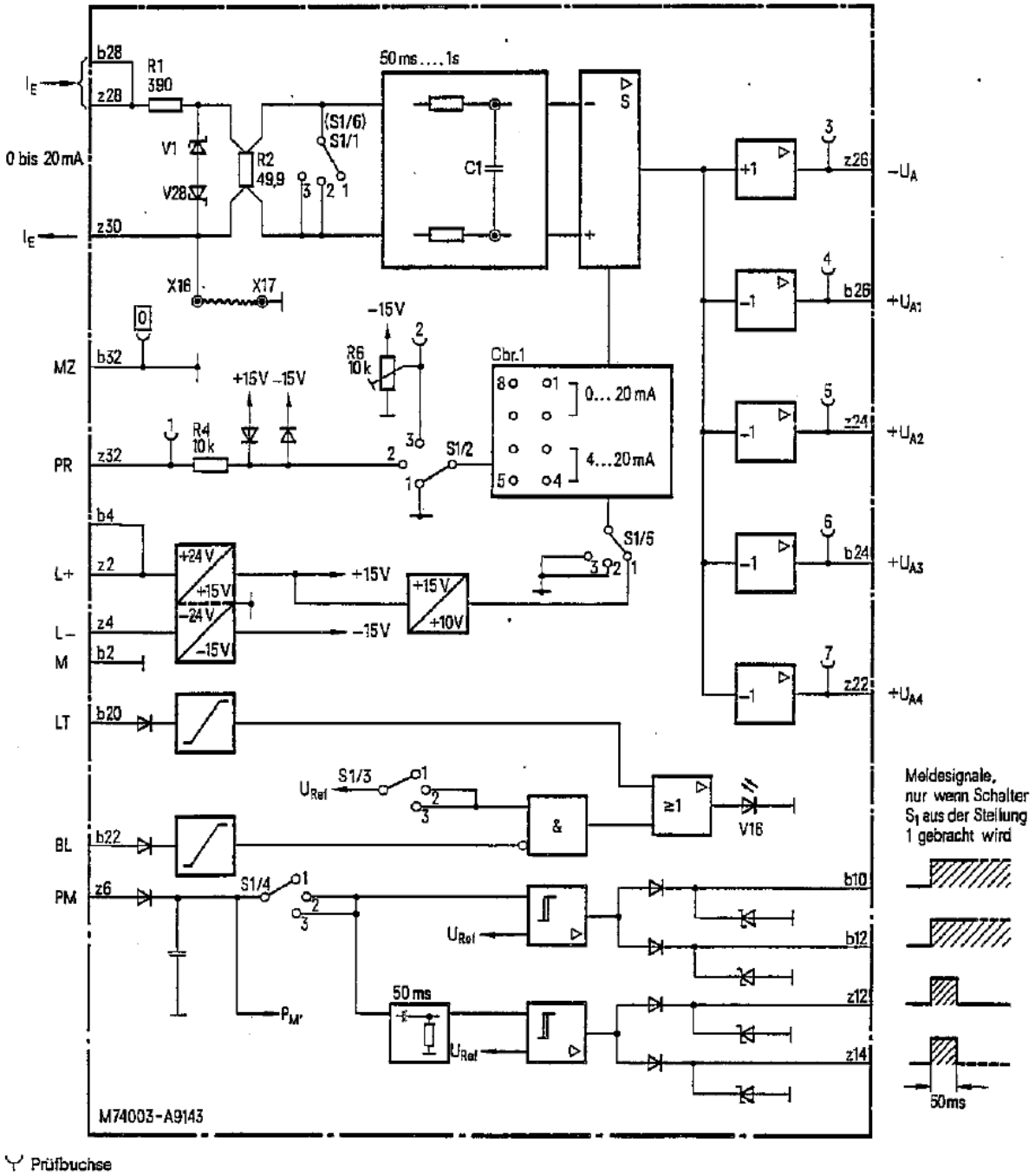

Bild 3.2: Blockschaltbild einer Strom-Spannungswandler Baugruppe (Typ M74003-A9143) /SIE 01/

Das Blockschaltbild des Redesigns ist in Bild 3.3 widergegeben.

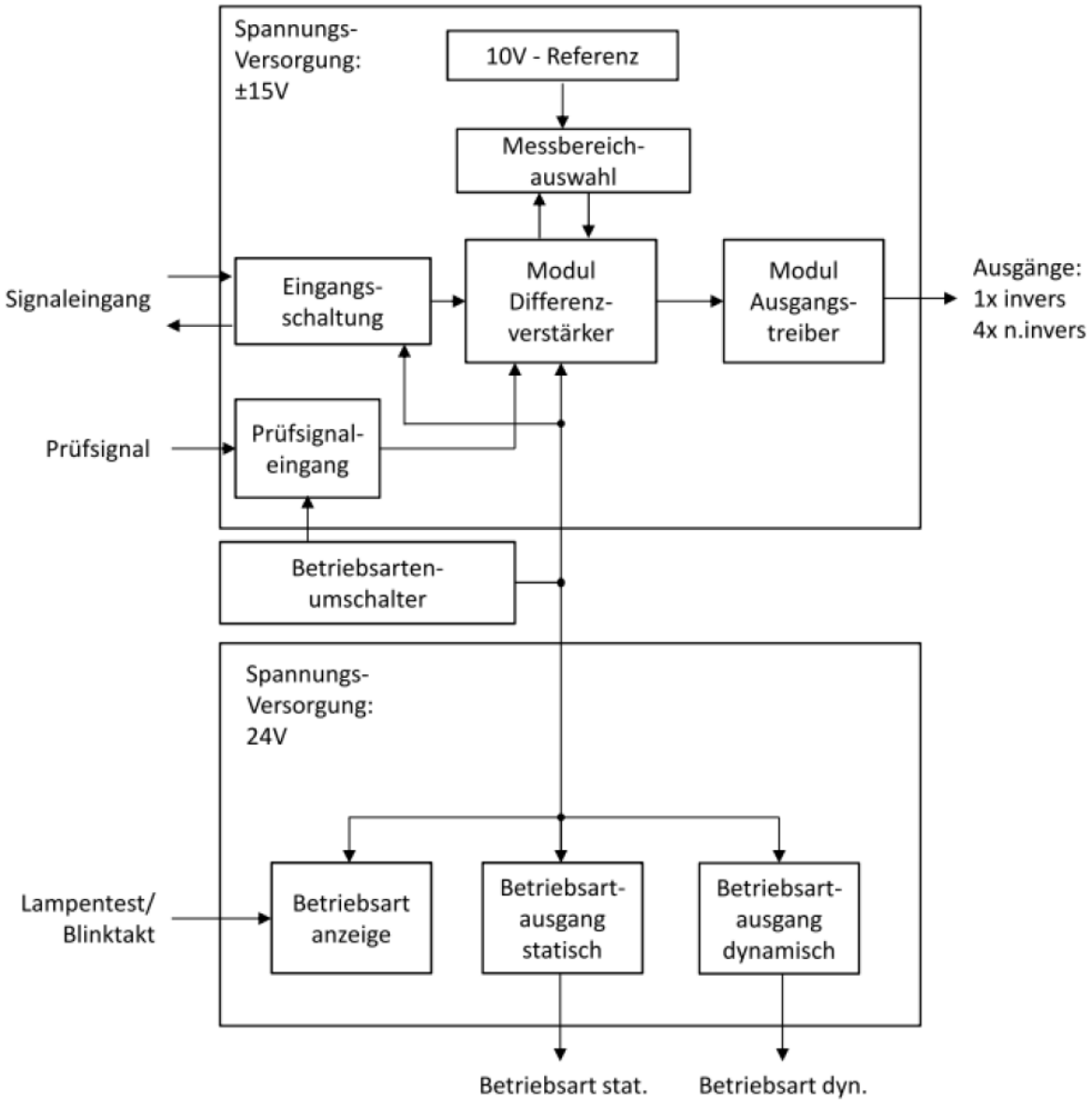

Bild 3.3: Blockschaltbild einer Strom-Spannungswandler - Redesign-Baugruppe /PH 12/

Diese Redesign-Baugruppe ist funktional äquivalent zur Originalbaugruppe.

Auch in diesem Blockschaltbild sind Signalflüsse eindeutig identifizierbar.

Die Funktionalität der Original- und der Redesign-Baugruppe entspricht der Funktionalität eines Software-Funktionsbausteins eines gängigen rechnerbasierten Leittechniksystems.

3.3.3 Messwertkorrekturrechner TZA4

In Bild 3.4 ist das Schaltbild des Messwertkorrekturrechners TZA4 wiedergegeben. Diese Baugruppe ersetzt die Analoge Baugruppe TZA20.

Die Funktion dieser Schaltung wird vollständig durch die implementierte Anwendungssoftware bestimmt, wobei die Baugruppe Grenzen für die Anzahl der Ein- und Ausgänge besitzt.

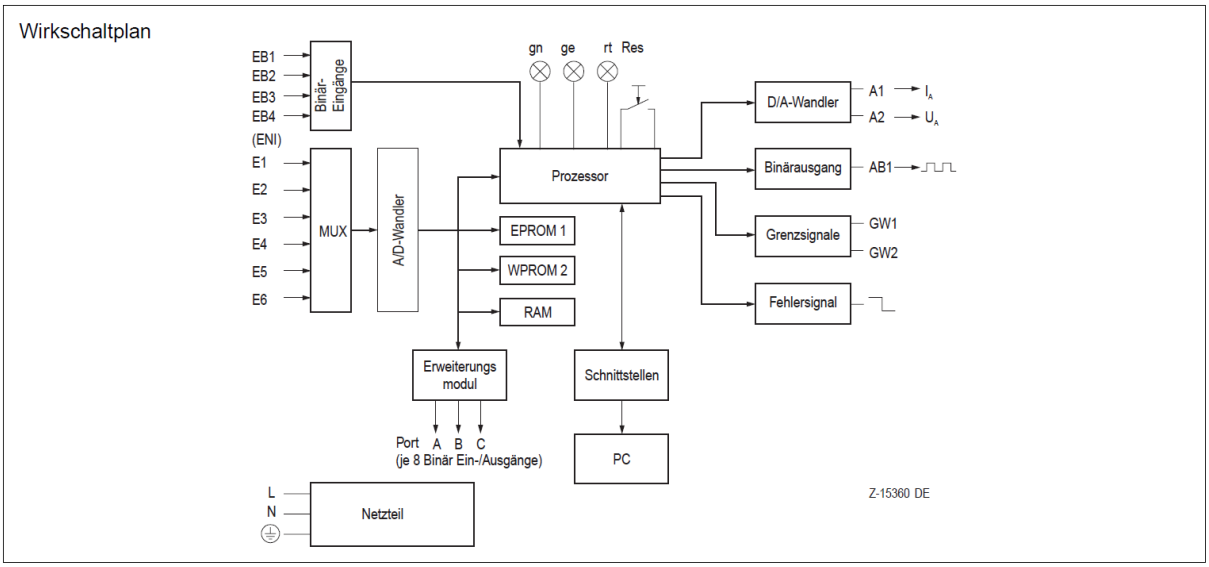

Bild 3.4: Digitaler Messrechner TZA 4 /HB 10/

Die Signalflüsse sind eindeutig bestimmt. Die implementierbare Anwendungssoftware ist frei programmierbar und kann den Funktionsumfang eines aus mehreren Funktionsbausteinen zusammengesetzten Funktionsplans erreichen. Anwendungssoftware für einen TZA4 kann in den Programmiersprachen BASIC und C erstellt werden. Es ist kein Werkzeug zur Spezifikation von Funktionsplänen mit anschließender Softwaregenerierung verfügbar.

3.3.4 Intelligenter Messwertumformer DT100

In Bild 3.5 ist das Logik-Schaltbild des rechnerbasierten Stellungsanzeige-System DT100 widergegeben.

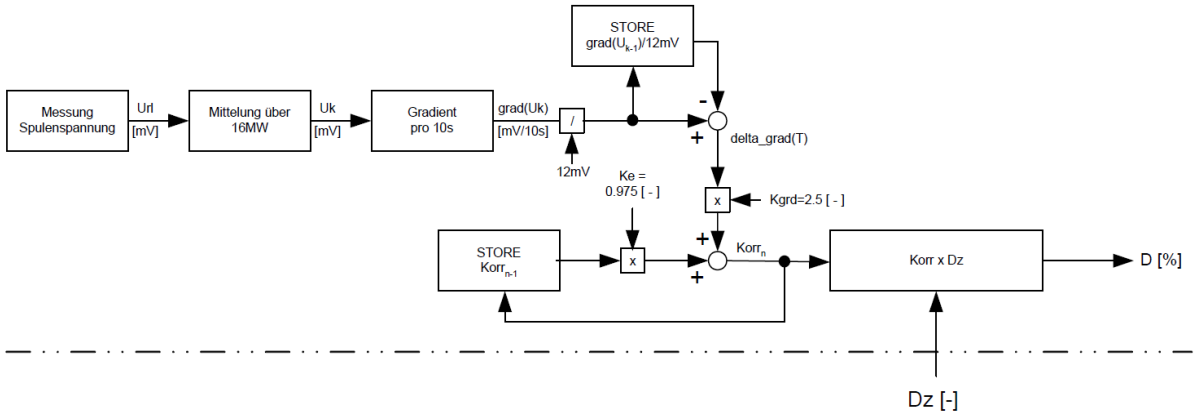

Bild 3.5: Rechnerbasiertes Stellungsanzeige-System DT100 /CCI 07/

Dabei handelt es sich um eine Kombination von Hardware- und Software-Blöcken. Die Software ist in einem, im Vergleich zum TZA4 modernen Prozessor implementiert und nicht vom Anwender veränderbar. Die Parameter der Baugruppe werden über ein Bedienwerkzeug (Notebook mit Bedienprogramm) eingestellt. Die im DT100 realisierte dynamische Tempera-

turdriftkorrektur (Bild 3.6) ist vollständig in Software realisiert, wobei im Logik-Schaltbild auch Hardware-Blöcke (z.B. Stromquelle) dargestellt sind

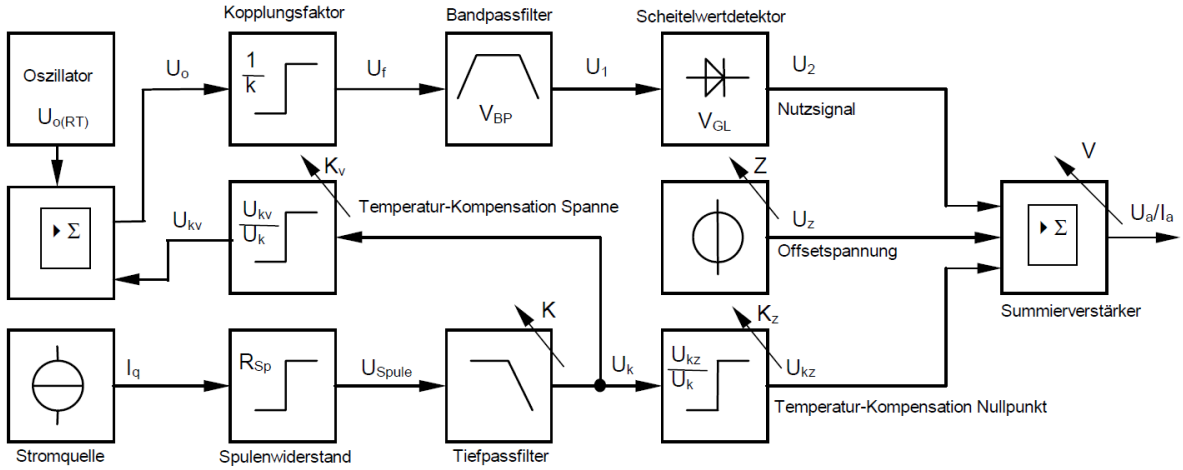

Bild 3.6: Dynamische Temperaturdriftkorrektur /CCI 07/

Die Signalflüsse sind eindeutig bestimmt. Die Funktionalität der Baugruppe ist bis auf Parametereinstellungen fix.

3.4 Übertragung der Komplexitäts-Charakteristika aus der Komplexitätsmessung der Software digitaler I&C-Systeme auf HW-Objekte

Es wurden vier Klassen von Redesign-Baugruppen anhand typischer Beispiele im Hinblick auf ihre Komplexitätseigenschaften betrachtet. Bezüglich der Übertragung der Komplexitäts-Charakteristika aus der Komplexitätsmessung der Software digitaler Leittechniksysteme ergeben sich dabei die im Folgenden dargestellten Bewertungen.

3.4.1 Konventionelle festverdrahtet Leitechnikbaugruppen

Die Funktionalität dieser Baugruppe entspricht der Funktionalität eines Software-Funktionsbausteins eines gängigen rechnerbasierten Leittechniksystems. Deshalb kann hier nur ein Teil des Komplexitätsvektors abgebildet werden, nämlich der für Funktionsbausteine relevante Teil /MAE 10/. Informationen bezüglich der Verschaltung der Signale sind erst bei Betrachtung von Funktionen möglich, die zu ihrer Realisierung die Zusammenschaltung mehrerer Baugruppen erfordern.

Der Gewinn, der sich aus der Anwendung der in /MAE 10/ beschriebenen Methodik auf die isolierte Baugruppe ergäbe, wäre sehr gering. Nutzen könnte erst bei der Betrachtung einer Zusammenschaltung mehrerer Baugruppen gezogen werden. Dazu müssten alle benötigten Daten manuell ermittelt werden, was einen hohen Arbeitsaufwand erfordern würde. Aus diesem Grunde ist eine Übertragung der Komplexitäts-Charakteristika aus der Komplexitätsmessung der Software digitaler leitechnischer Systeme auf konventionelle festverdrahtet Leitechnikbaugruppen nicht als sinnvoll anzusehen.

3.4.2 Redesign einer Baugruppe in Dickschicht-Hybridtechnik

Auch in diesem Fall entspricht die Funktionalität der Baugruppe der Funktionalität eines Software-Funktionsbausteins eines gängigen rechnerbasierten Leittechniksystems. Aufgrund der Möglichkeit, Signalflüsse eindeutig zu identifizieren, könnte die interne Verschaltung der Signale auf der Baugruppe in den Komplexitätsvektor einbezogen werden. Der sich daraus ergebende Gewinn ist aber eher als gering einzuschätzen, da die Funktionalität der einzelnen Baugruppe stark begrenzt ist. Deshalb gelten hier die gleichen Bedingungen wie sie für konventionelle festverdrahtet Leitechnikbaugruppen im vorangegangenen Abschnitt ermittelt wurden.

3.4.3 Baugruppen für komplexere Funktionen in einfacher Digitaltechnik

Die Funktionalität, die auf diese Baugruppen abgebildet werden kann, ist um ein Vielfaches größer als die Funktionalität, die auf konventionelle festverdrahtete bzw. in Dickschicht-Hybridtechnik implementierte Leitechnikbaugruppen abgebildet werden kann. Da in diesem Fall die Anwendungssoftware in allgemeinen Mehrzweck-Programmiersprachen wie BASIC oder C erstellt wird, ist eine Analyse der Software erforderlich. Diese Analyse dient dem Zweck, grundlegende Softwaremodule, die an die Stelle der Funktionsbausteine treten, zu ermitteln. Für monolithische Softwarestrukturen, wie sie für BASIC-Programme typisch sind, ist das ein aufwendiger, meist manuell durchzuführender Prozess. Liegt das Programm in strukturierter, modularer Form vor, so kann die Modularisierung benutzt werden, um entsprechende „Funktionsblockäquivalente“ zu bestimmen. Problematisch ist die zu erwartende Vielzahl unterschiedlicher Daten, die von den Modulen verarbeitet werden. Es sind im Allgemeinen nicht nur Signale sondern beliebige Funktionsparameter. Deshalb ist die in /MAE 10/ beschriebene Methodik grundsätzlich anwendbar, muss aber gegebenenfalls angepasst werden.

3.4.4 Komplexe Rechnerbaugruppen

Für komplexe Rechnerbaugruppen mit umfangreicher Funktionalität ist die in /MAE 10/ beschriebene Methodik meist anwendbar. Diese Baugruppen sind entweder mit einer fixen Software, die nur durch Parametrierung an den Anwendungsfall angepasst wird, versehen (z.B. DT100) oder sie sind mit Hilfe von Funktionsplänen bzw. funktionsplanähnlichen Methoden in gewissen Grenzen frei programmierbar (z.B. SPS).

Aufgrund ihrer Komplexität werden in der Spezifikationsphase eines Redesigns oftmals die in den ursprünglichen Hardwaredesigns vorhandenen Blockstrukturen mit definierten Signalverbindungen herangezogen. Diese Strukturen werden anschließend in modulare Softwaresysteme, die auch in Hardware realisierte Blöcke beinhalten können, übersetzt.

Speicherprogrammierbare Steuerungen (SPS) lassen sich immer dann mit der in /MAE 10/ beschriebenen Methodik analysieren, wenn sie mit Funktionsbausteinsprachen (z.B. FUP in STEP 5 und STEP 7) programmiert werden, was für SPS-basierte Steuerungen in Kernkraftwerken vorwiegend der Fall ist.. Inwieweit Anweisungslisten, Kontaktpläne, Ablaufsprachen und strukturierter Text, die nach EN 61131-3 „Speicherprogrammierbare Steuerungen - Teil 3: Programmiersprachen“ ebenfalls genormte Programmiersprachen für Speicherprogrammierbare Steuerungen (SPS) sind, analysiert werden können, ist noch näher zu untersuchen.

4 ZUSAMMENFASSUNG

Im vorliegenden Bericht werden Anforderungen an die Prüfung und Bewertungskriterien für den Einsatz von Redesign-Komponenten, insbesondere von Komponenten in der Sicherheitsleittechnik von Kernkraftwerken, beschrieben.

Im ersten Teil des Berichts werden Anforderungen an die Prüfung von Redesign-Komponenten mit komplexen, insbesondere digitalen rechnerbasierten, Bauteilen sowie spezifische Testverfahren zusammengestellt.

Dabei wurden sowohl Anforderungen als auch Testverfahren im Hinblick auf die Anwendbarkeit für Leittechnik für Kernkraftwerke bewertet. Es zeigte sich, dass sich Anforderungen bezüglich der Fertigung von Redesign-Baugruppen aus IPC 610 ableiten lassen. Anforderungen für FPGA-basierte Redesign-Baugruppen orientieren sich an den Besonderheiten des Entwicklungslebenszyklus von FPGAs und sind für HDL-programmierte Schaltkreise in der IEC 62566 zu finden.

Von den zusätzlichen Testverfahren hat der Burn-in-Test das Potenzial, die Typprüfung nach KTA 3503 zu ergänzen. Testverfahren zur stark beschleunigten Alterung durch extreme Temperaturwechsel und Vibrationsbelastung (HALT, HASS) erscheinen nicht zielführend, da das Belastungsprofil für Kernkraftwerke untypisch ist. Der Highly Accelerated Stress Test (HAST) ist aufgrund der inhomogenen Zusammensetzung der Leittechnikbaugruppen zu ungenau, um belastbare Ergebnisse zu liefern.

Ergänzend zu den direkten kerntechnischen Qualifizierungsverfahren wurde die Vorgehensweise nach der VDI-Richtlinie 3528 in die Betrachtung einbezogen. Diese Richtlinie zeigt Wege auf, wie industrielle Serienprodukte in sicherheitsrelevanten Anwendungen in der Leittechnik von Kernkraftwerken eingesetzt werden können ohne dabei Abstriche an den Sicherheitsanforderungen zu machen. Damit könnten auch komplexe elektronische Komponenten, die in kleinen Stückzahlen als Sonderfertigung hergestellt werden, hinreichend qualifiziert werden.

Im zweiten Teil des Berichts wurde untersucht, inwiefern und mit welchen Methoden die Komplexitätsmessung, die für Software entwickelt wurde, auf Redesign-Baugruppen anwenden lässt.

Dabei wurde sichtbar, dass konventionelle festverdrahtet Redesign-Baugruppen und Redesign-Baugruppe in Dickschicht-Hybridtechnik als einzelne Baugruppe nicht sinnvoll bezüglich ihrer Komplexität bewertet werden können. Die Anwendung der Methodik ist arbeitsaufwendig und liefert nur Resultate, die mit anderen Methoden ebenfalls gewonnen werden können.

Komplexere rechner-basierte Baugruppen sind weitgehend mit der Methode der Komplexitätsmessung analysierbar. Die dabei gewinnbaren Resultate sind denen der Komplexitätsmessung der Software gleichwertig, da auch hier die Funktionalität in Funktionsbausteinen realisiert wird, die durch Signalverbindungen verschaltet sind. Es ist dabei möglich Hardware- und Software-Funktionsblöcke gemeinsam zu betrachten.

5 ABKÜRZUNGSVERZEICHNIS

ASIC	Application Specific Integrated Circuit
ASME	American Society Of Mechanical Engineers
ATEX	Richtlinien auf dem Gebiet des Explosionsschutzes (Atmosphère Explosibles)
BGR-Port	Baugruppen-Port
BHT	Basis Hardware Test
CCF	Common Cause Failure
CEC	Commission of the European Communities
CLK	Clock (Taktgeber)
CMOS	Complimentary-symmetry Metal-Oxide Semiconductor
DIN	Deutsches Institut für Normung
E/A-Bus	Ein-/Ausgabe-Bus
EDF	Électricité de France
EEPROM	Electrically Erasable Programmable Read Only Memory
EIAJ	Electronic Industries Association of Japan
EMB	Elektromagnetische Beeinflussung
EN	Europäische Norm
EU	European Union
EXTLED	externe LED
FMEA	Failure Mode and Effect Analysis
FP-7	7. Forschungsrahmenprogramm der EU
FPGA	Field Programmable Gate Array
FUP	Funktionsplan
GMA	Mess- Und Automatisierungstechnik
GmbH	Gesellschaft mit beschränkter Haftung
GRS	Gesellschaft für Anlagen- und Reaktorsicherheit
HALT	Highly Accelerated Life Test
HARMONICS	Harmonised Assessment of Reliability of Modern Nuclear I&C. Software
HAST	Highly Accelerated Stress Test
HDL	Hardware Description Language
HOT	Hardware Organisation Tool
HW	Hardware
I&C	Instrumentation and Control
I/O-RAM	Input-/Output-RAM
IAEA	International Atomic Energy Agency

IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IPC	Association Connecting Electronics Industries
ISO	International Organisation for Standardisation
ISTec	Institut für Sicherheitstechnologie (ISTec) GmbH
JEDEC	Joint Electron Device Engineering Council - heute: JEDEC Solid State Technology Association
KKW	Kernkraftwerk
KTA	Kerntechnischer Ausschuss
KWB	Kernkraftwerk Biblis
LED	Light-Emitting Diode
LLP	Limited Liability Partnership
NAMUR	Internationaler Verband der Anwender von Automatisierungstechnik der Prozessindustrie (ursprünglich: Normenarbeitsgemeinschaft für Meß- und Regeltechnik in der chemischen Industrie)
NMI	Non-Maskable Interrupt
RAM	Random-Access Memory - Schreib- / Lesespeicher
RS232	Standardisierte Computerschnittstelle
RSK-LL	RSK Leitlinien für DWR
RTL	Register Transfer Level
SIL	Safety Integrity Level
SPS	Speicherprogrammierbare Steuerung
SÜA	Selbstüberwachung Im Anlauf
SVE	Sicherheitsverarbeitungseinheit
USART	Universal Asynchronous Receiver Transmitter
USB	Universal Serial Bus
V&V	Verification and Validation
VDE	Verband der Elektrotechnik Elektronik Informationstechnik e.V.
VDI	Verein Deutscher Ingenieure
VTT	Valtion teknillinen tutkimuskeskus (Staatliches Technisches Forschungs-zentrum)
WDG	Watch-Dog
WKP	wiederkehrende Prüfung
WTD 71	Wehrtechnische Dienststelle für Schiffe und Marinewaffen der Bundeswehr, Maritime Technologie und Forschung
ZSÜ	Zyklische Selbstüberwachung

6 LITERATUR

/CCI 07/ SW-basiertes Stellungsanzeige-System DT100, Pflichtenheft, CCI 2007

/GRÖ 06/ Gröner, G., Durchgängige Anwendung von IPC-Richtlinien im Entstehungsprozess von Elektronik, 14. FED-Konferenz 2006, Workshop 8

/HB 10/ Digitaler Messrechner TZA 4, Katalog H&B, Listenblatt 18-5.10

/KTA 3506/ KTA 3506 „Systemprüfung der Sicherheitsleittechnik von Kernkraftwerken“ Fassung 2013-11

/LIN 04/ H. Baleanu, E. Hoffmann, A. Lindner, Aktualisierung des kerntechnischen Regelwerks gemäß den Erfordernissen des fortgeschrittenen Standes von Wissenschaft und Technik- Regelwerksarbeit für digitale Sicherheitsleittechnik, ISTec-Technische Notiz, ISTec Garching (Juli 2004)

/LIN 97/ Lindner, A., Herzog, H., Untersuchung des Fehlverhaltens einer GEAMATIC-Baugruppe XPH 70, ISTec-A-201, Rev. 1, 1997

/MAE 95/ J. Märtz, Static Analyzers Experience at the Institute for Safety Technology in ‘Metrics in Software Evolution‘ GMD-Bericht-254
Oldenbourg-Verlag (1995)

/MAE 10/ J. Märtz, H. Miedl, A. Lindner, Ch. Gerst, Komplexitätsmessung der Software digitaler Leittechniksysteme, ISTec-A-1569, ISTec Garching (2010)

/MAI 95/ U. Mainka, J. Märtz, G. Glöe, G. Dahll et al., Werkzeuge für den standardisierten Software-Sicherheitsnachweis (SOSAT-3), Abschlussbericht (1995)

/MID 07/ H. Miedl, J. Märtz, A. Lindner, et al., Qualifizierung integrierter Werkzeugumgebungen zur Entwicklung rechnerbasierter Systeme in KKW , ISTec-A-1285, ISTec Garching (2007)

/PAS 12/ http://www.passmark.com/products/bit.htm

/PH 12/ Pflichtenheft Signalwandler I/U, RHe-Artikelnummer: 99026631, Gerätesachnummer: 79000303, 06.07.2012

/RSK 213/ RSK-Ausschuss ELEKTRISCHE EINRICHTUNGEN
Ergebnisprotokoll der 213. Sitzung am 19.10.2011.

/SIE 00/ Pflichtenheft: Selbstüberwachung für Rechner in der digitalen Sicherheitsleittechnik
44/97 sbüph2, Version 2.00
Siemens, Erlangen 2000

/SIE 01/ Signalumformer I/U, Siemens, Typ M74003-A9143

/VDI 11/ VDI-Richtlinie 3528 „Anforderungen an Serienprodukte und Kriterien für deren Einsatz in der Sicherheitsleittechnik in Kernkraftwerken“
VDI Verlag 2011

/VGB 11/ VGB-Arbeitskreis Gerätequalifizierung E+L in KKW, RICHTLINIE Nr. RL005/A “Design/Redesign von technischen Einrichtungen in Kernkraftwerken”

/VGB 13/ VGB Powertech, VGB-AK „Gerätequalifizierung E- und L-Technik in KKW“ E. Sander (EnKK) und W. Schroeder (VENE „WIL“), „Ersatzbeschaffung von technischen Einrichtungen der E- und L-Technik für KKW“, Foliensatz

/WP 01/ http://de.wikipedia.org/wiki/Highly_Accelerated_Life_Test

VERTEILER

ISTec

Geschäftsführung	(KOL)	1 x
Abteilung	(LIA, MAE, MID, SGU)	je 1 x
Kunde		5 x
Gesamtauflage		**10 Exemplare**