# Entwicklung eines Bewertungsansatzes für den Einsatz von kommerziellen (COTS) Komponenten in Kernkraftwerken

GRS - 766

Gesellschaft für Anlagen-
und Reaktorsicherheit
(GRS) gGmbH

# Entwicklung eines Bewertungsansatzes für den Einsatz von kommerziellen (COTS) Komponenten in Kernkraftwerken

Robert Arians
Björn Becker
Christian Korn

April 2024

**Anmerkung:**

Das diesem Bericht zugrunde liegende Forschungsvorhaben wurde mit Mitteln des Bundesministeriums für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV) unter dem Förderkennzeichen 4721R01550 durchgeführt.

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

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

**GRS - 766**
**ISBN 978-3-910548-58-9**

**Deskriptoren**
commercial off-the-shelf, COTS, Elektro- und Leittechnik, Kernkraftwerk, Kommerzielle Komponenten

## Kurzfassung

In den kommenden Jahren ist im Zuge von Modernisierungen bestehender kerntechnischer Anlagen und dem Neubau kerntechnischer Anlagen sowohl national als auch international mit einem hohen Bedarf an Komponenten zum Einsatz in sicherheitstechnisch wichtigen elektro- und leittechnischen Einrichtungen zu rechnen. Die Herstellung von nach nuklearem Regelwerk qualifizierten Komponenten ist für die Hersteller aufgrund der aufwendigen Qualifizierungsmaßnahmen und dem verglichen zu anderen Industriezweigen niedrigen Stückzahlbedarf mit einem hohen Aufwand verbunden, den die Hersteller immer weniger einzugehen bereit sind. Daher werden Betreiber kerntechnischer Anlagen gezwungen sein, nicht speziell für den Einsatz in kerntechnischen Anlagen gefertigte und qualifizierte Komponenten einzusetzen, sondern in wachsendem Maße auf kommerzielle Massenware, sogenannte COTS-Komponenten (COTS, commercial off-the shelf), zurückzugreifen.

In diesem Vorhaben wird ein Bewertungsansatz für den Einsatz von COTS-Komponenten in sicherheitstechnisch wichtigen elektro- und leittechnischen Einrichtungen in kerntechnischen Anlagen entwickelt. Dazu erfolgt die Ermittlung und Auswertung nationaler und internationaler Vorgehensweisen hinsichtlich des Einsatzes von COTS-Komponenten, wozu diverse Dokumente bezüglich dieser Thematik ausgewertet werden. Zudem erfolgt die Auswertung der Vorgehensweisen hinsichtlich des Einsatzes von COTS-Komponenten in kerntechnischen Anlagen im Ausland. Die aus diesen Schritten gesammelten Erkenntnisse werden hinsichtlich verschiedener Aspekte zusammengefasst und mit Anforderungen aus dem nationalen kerntechnischen Regelwerk hinsichtlich dieser Aspekte verglichen. Basierend auf den Anforderungen an COTS-Komponenten und den Anforderungen aus dem kerntechnischen Regelwerk wird ein Bewertungsansatz für den Einsatz von COTS-Komponenten entwickelt.

## Abstract

In the coming years, the modernization of existing nuclear facilities and the construction of new nuclear facilities, both nationally and internationally, is expected to result in a high demand for components for use in electrical and I&C equipment that is important for safety. The production of components qualified in accordance with nuclear regulations is associated with high costs for manufacturers due to the complex qualification measures and the low demand for components compared to other industry branches, which manufacturers are increasingly unwilling to incur. As a result, operators of nuclear facilities will be forced not to use components specially manufactured and qualified for use in nuclear facilities, but to increasingly rely on commercial mass-produced components, so-called COTS-components (COTS, commercial off-the-shelf).

This project will develop an assessment approach for the use of COTS-components in safety-relevant electrical and I&C equipment in nuclear facilities. For this purpose, national and international procedures regarding the use of COTS-components are determined and evaluated, for which purpose various documents relating to this topic are evaluated. In addition, the procedures regarding the use of COTS-components in nuclear facilities abroad are evaluated. The findings gathered from these steps are summarized regarding various aspects and compared with requirements from the national nuclear regulations regarding these aspects. Based on the requirements for COTS-components and the requirements from the national nuclear regulations, an assessment approach for the use of COTS-components is developed.

## Inhaltsverzeichnis

# 1 Einleitung, Aufgabenstellung und Zielsetzung

Derzeit werden in sicherheitstechnisch wichtigen elektro- und leittechnischen Einrichtungen in Leistungsreaktoren (sowohl in Betrieb als auch in Stilllegung) und weiteren kerntechnischen Anlagen (z. B. Forschungsreaktoren, Zwischenlager, etc.) im In- und Ausland vorwiegend für den Einsatz nach einem nuklearen Regelwerk qualifizierte Komponenten genutzt. Die Herstellung von Komponenten, die für bestimmte Einsatzumgebungen nach nuklearem Regelwerk qualifiziert sind, bedeutet für die Hersteller oftmals einen hohen Produktions- und Kostenaufwand. Aufgrund des relativ niedrigen Stückzahlbedarfs für die Nuklearindustrie sowie der aufwendigen Qualifizierungsmaßnahmen ist dieser Aufwand aus Sicht vieler Hersteller nicht vertretbar, weswegen sich immer mehr Unternehmen aus diesem Produktionsbereich zurückziehen. In den kommenden Jahren ist aber im Zuge der Modernisierung bestehender kerntechnischer Anlagen und beim Neubau von kerntechnischen Anlagen sowohl national als auch international mit einem hohen Bedarf an Komponenten zum Einsatz in sicherheitstechnisch wichtigen elektro- und leittechnischen Einrichtungen zu rechnen. Aufgrund der beschriebenen Problematik sind die Betreiber der Anlagen dabei gezwungen, in wachsendem Maße Komponenten einzusetzen, bei denen es sich um kommerzielle Massenware handelt und die nicht speziell für den Einsatz in kerntechnischen Anlagen entwickelt wurden. Diese kommerziellen Komponenten werden als COTS-Komponenten (COTS, commercial off-the shelf) bezeichnet. In diesem Bericht wird der Begriff COTS-Komponenten verwendet, wobei dieser Begriff stellvertretend für einzelne Komponenten, aber auch für Geräte oder komplette Systeme steht.

Unter COTS-Komponenten sind seriengefertigte Komponenten zu verstehen, die in großen Stückzahlen hergestellt und verkauft werden. COTS-Komponenten sind oftmals komplex aufgebaut und haben viele Funktionalitäten, außerdem beinhalten sie oftmals programmierbare oder rechnerbasierte Bauteile. Da sie nicht für einen speziellen Einsatzbereich gefertigt sind, können sie flexibel in vielen Bereichen eingesetzt werden. In der Regel werden COTS-Komponenten schnell auf den Markt gebracht und sind deutlich günstiger als nuklear qualifizierte Komponenten. Der Einsatz von COTS-Komponenten kann Vorteile mit sich bringen. Zu nennen sind hier neben den geringeren Herstellungskosten, erweiterte Diagnosemöglichkeiten oder integrierte Mechanismen zur Selbstüberwachung. Ein weiterer möglicher Vorteil kommerzieller Komponenten ist die deutlich umfangreichere Betriebserfahrung aufgrund der Produktion in großen Stückzahlen. Inwiefern diese in Betracht gezogen werden kann, hängt allerdings von der Möglichkeit

ab, wie zuverlässig diese ausgewertet wird und ob sie für die spätere Zielanwendung repräsentativ ist. Der Einsatz von COTS-Komponenten in sicherheitskritischen Anwendungsbereichen (z. B. Kerntechnik, Luft- und Raumfahrttechnik, Militär) wird sowohl national als auch international ausführlich diskutiert.

In kerntechnischen Anlagen im In- und Ausland dürfen für den Einsatz in sicherheitstechnisch wichtigen elektro- und leittechnischen Einrichtungen nur nachgewiesen zuverlässige und für die Einsatzbedingungen geeignete Komponenten verwendet werden. Sollen COTS-Komponenten in kerntechnischen Anlagen eingesetzt werden, müssen diese Zuverlässigkeitskennwerte aufweisen, die äquivalent zu denen von Systemen sind, die nach nuklearem Regelwerk gefertigt und qualifiziert wurden. Daher ist für den Einsatz von COTS-Komponenten ein angemessener Prozess anzuwenden, der die Eignung der COTS-Komponenten für den Einsatz in kerntechnischen Anlagen, ohne negative Auswirkungen auf die nukleare Sicherheit der Anlagen zu haben, nachweist.

Das Ziel dieses Vorhabens ist es, einen Bewertungsansatz für den Einsatz von COTS-Komponenten in sicherheitstechnisch wichtigen elektro- und leittechnischen Einrichtungen in kerntechnischen Anlagen zu entwickeln. Aufgrund der unterschiedlichen Nachweistiefen und Qualitätsanforderungen für elektro- und leittechnische Einrichtungen in Abhängigkeit von ihrer sicherheitstechnischen Bedeutung (Kategorie A, B oder C nach DIN EN 61226 /DIN 10a/), werden bei der Entwicklung des Bewertungsansatzes die einzelnen Kategorien berücksichtigt.

Das Arbeitsprogramm zu diesem Vorhaben ist in den nachfolgend kurz dargestellten Arbeitspaketen umgesetzt:

- **Arbeitspaket 1: Ermittlung und Auswertung nationaler und internationaler Vorgehensweisen hinsichtlich des Umgangs mit COTS-Komponenten**
  In diesem Arbeitspaket erfolgt die Ermittlung und Auswertung nationaler und internationaler Vorgehensweisen hinsichtlich des Einsatzes von COTS-Komponenten in sicherheitstechnisch wichtigen elektro- und leittechnischen Einrichtungen. Hierzu werden diverse nationale und internationale Dokumente und Regelwerke bezüglich der Thematik des Einsatzes von COTS-Komponenten ausgewertet. Dazu erfolgt im ersten Schritt eine Literaturrecherche zur Ermittlung solcher Dokumente, wobei bei der Recherche neben der Kerntechnik auch andere Bereiche wie beispielsweise Luft- und Raumfahrt, Bahn oder Militär berücksichtigt werden. In einem anschließenden Erstscreening werden die ermittelten Dokumente hinsichtlich ihrer Relevanz für

das Vorhaben bewertet und die als relevant erachteten Dokumente werden detailliert ausgewertet. Des Weiteren wird im Rahmen dieses Arbeitspaketes nach internationalen Vorgehensweisen hinsichtlich des Einsatzes von COTS-Komponenten in kerntechnischen Anlagen recherchiert. Auf Basis dieser Recherche wird die Vorgehensweise in fünf Ländern detailliert ausgewertet.

- **Arbeitspaket 2: Entwicklung eines Ansatzes zur Bewertung des Einsatzes von COTS-Komponenten**

  In diesem Arbeitspaket erfolgt die Entwicklung eines Bewertungsansatzes zum Einsatz von COTS-Komponenten in sicherheitstechnisch wichtigen elektro- und leittechnischen Einrichtungen in kerntechnischen Anlagen. Dazu werden die in Arbeitspaket 1 ermittelten Erkenntnisse und Anforderungen bezüglich des Einsatzes von COTS-Komponenten, die aus den detailliert ausgewerteten Dokumenten und den detailliert ausgewerteten Vorgehensweisen anderer Länder gewonnen wurden, berücksichtigt. Zudem werden Anforderungen aus dem nationalen kerntechnischen Regelwerk vergleichend hinzugezogen. Die Erkenntnisse und Anforderungen aus Arbeitspaket 1 und dem nationalen kerntechnischen Regelwerk werden bezüglich verschiedener Aspekte zusammengefasst. Darauf aufbauend wird der Ansatz zur Bewertung des Einsatzes von COTS-Komponenten entwickelt, wobei die verschiedenen Kategorien A, B und C berücksichtigt werden.

# 2 Ermittlung und Auswertung nationaler und internationaler Vorgehensweisen hinsichtlich des Umgangs mit COTS-Komponenten

In diesem Kapitel werden die Ergebnisse der Arbeiten zu Arbeitspaket 1 dargestellt. Die Zielsetzung der Arbeiten im Arbeitspaket 1 war die Ermittlung und Auswertung nationaler und internationaler Vorgehensweisen hinsichtlich des Einsatzes von kommerziellen Komponenten (COTS-Komponenten) in sicherheitstechnisch wichtigen elektro- und leittechnischen Einrichtungen. Hierzu wurden diverse Dokumente bezüglich der Thematik des Einsatzes von COTS-Komponenten ausgewertet. Die ausgewerteten Dokumente sind in Abschnitt 2.1 zusammengefasst. Des Weiteren wurde nach internationalen Vorgehensweisen hinsichtlich des Einsatzes von COTS-Komponenten in kerntechnischen Anlagen recherchiert und für das Vorhaben relevante Ergebnisse dieser Recherche für fünf Länder ausgewertet. Die Vorgehensweisen dieser fünf Länder hinsichtlich des Einsatzes von COTS-Komponenten in kerntechnischen Anlagen wird in Abschnitt 2.2 zusammengefasst.

## 2.1 Auswertung nationaler und internationaler Literatur bezüglich der Thematik des Einsatzes von kommerziellen Komponenten

Zur Auswertung nationaler und internationaler Vorgehensweisen hinsichtlich des Einsatzes von COTS-Komponenten in sicherheitstechnisch wichtigen elektro- und leittechnischen Einrichtungen wurden diverse Dokumente zu dieser Thematik ausgewertet. Dazu wurden im Rahmen einer Literaturrecherche verschiedene nationale und internationale Dokumente ermittelt, in denen die Thematik des Einsatzes von COTS-Komponenten behandelt wird. Bei der Suche nach infrage kommenden Dokumenten wurden neben der Kerntechnik auch andere, nicht kerntechnische Bereiche, wie beispielsweise Luft- und Raumfahrttechnik, Bahn oder Militär berücksichtigt, sofern öffentlich verfügbare Dokumente gefunden werden konnten. In einem Erstscreening wurden die ermittelten Dokumente hinsichtlich ihrer Relevanz für das Vorhaben untersucht. Dabei wurde darauf geachtet, dass die für das Vorhaben tatsächlich verwendeten Dokumente Anforderungen an die Qualifizierung und Kategorisierung programmierbarer oder rechnerbasierter Komponenten im Allgemeinen und COTS-Komponenten im Speziellen enthalten.

Folgende Dokumente wurden bei dem Erstscreening als für das Vorhaben relevant bewertet:

- VDI/VDE-Richtlinie 3528 „Anforderungen an Serienprodukte und Kriterien für deren Einsatz in der Sicherheitsleittechnik in Kernkraftwerken“ /VDI 11/
- IAEA NR-T-3.31 „Challenges and Approaches for Selecting, Assessing and Qualifying Commercial Industrial Digital Instrumentation and Control Equipment for Use in Nuclear Power Plant Applications” /IAE 20/
- BS IEC 62671 „Nuclear Power Plants – Instrumentation and control important to safety – Selection and use of industrial digital devices of limited functionality” /BSI 13/
- “Guidance for Commercial Grade Dedication” /DOE 11/
- DIN EN 61513 „Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen“ /DIN 13/
- DIN EN 60880 „Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie A“ /DIN 10b/
- IEC 62138 „Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category B or C functions” /IEC 18/
- DIN EN 60987 „Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen an die Hardware-Auslegung rechnerbasierter Systeme“ /DIN 10c/
- “Commercial-Off-The-Shelf (COTS) Hardware and Software for Train Control Applications: System Safety Considerations” /DOT 03/
- “Simple and Complex Electronic Hardware Approval Guidance” /DOT 17/
- AMC 20-152A „Development Assurance for Airborne Electronic Hardware” /EAS 21/
- “Commercial off the Shelf (COTS) security issues and approaches” /DOA 06/
- “Joint Software Systems Safety Engineering Handbook” /DOD 10/
- “Space product assurance – Commercial electrical, electronic and electromechanical (EEE) components” /ESA 13/

Diese Dokumente wurden detailliert ausgewertet und die für das Vorhaben relevanten Inhalte dieser Dokumente wurden in Arbeitspaket 2 zur Entwicklung des Ansatzes zur Bewertung des Einsatzes von COTS-Komponenten verwendet. In den nachfolgenden Abschnitten werden die relevanten Inhalte der detailliert ausgewerteten Dokumente kurz vorgestellt.

### 2.1.1 VDI/VDE-Richtlinie 3528

Die VDI/VDE-Richtlinie 3528 „Anforderungen an Serienprodukte und Kriterien für deren Einsatz in der Sicherheitsleittechnik in Kernkraftwerken“ /VDI 11/ beschäftigt sich mit Fragen zur Qualifizierung von am Markt verfügbaren Serienprodukten, die in der Sicherheitsleittechnik von Kernkraftwerken eingesetzt werden sollen. Da diese zumeist nicht nach kerntechnischen Gesichtspunkten qualifiziert sind, gibt die VDI/VDE-Richtlinie 3528 Empfehlungen hinsichtlich grundsätzlicher Anforderungen, die Serienprodukte erfüllen müssen, um in der Sicherheitsleittechnik von Kernkraftwerken eingesetzt werden zu können. Dabei wird auch berücksichtigt, welche zusätzlichen Maßnahmen getroffen oder Randbedingungen geschaffen werden müssen, damit Serienprodukte in sicherheitstechnisch relevanten Funktionen Verwendung finden können. Das Ziel ist dabei, für leittechnische Systeme auch Komponenten nutzen zu können, die nach konventionellem Regelwerk qualifiziert wurden. Die Empfehlungen der VDI/VDE-Richtlinie 3528 beziehen sich auf elektro- oder leittechnische Einrichtungen, die Funktionen der Kategorien A, B oder C nach DIN EN 61226 /DIN 10a/ ausführen.

In /VDI 11/ werden Empfehlungen hinsichtlich grundsätzlicher Anforderungen gegeben, die kommerzielle Komponenten erfüllen müssen. Zudem werden Kriterien für den Einsatz kommerzieller Komponenten in der Sicherheitsleittechnik in Kernkraftwerken definiert. Eine in /VDI 11/ beschriebene Möglichkeit ist die Feststellung der Eignung der kommerziellen Komponente bei Vorliegen entsprechender Qualifizierungen oder Prüfzeugnisse aus anderen technischen Bereichen, wobei gegebenenfalls zusätzliche Prüfungen zur Ergänzung der vorliegenden Qualifizierung erforderlich sind. Eine weitere Möglichkeit ist der Einsatz von Architekturen, die beispielsweise durch höhere Redundanzgrade einen höheren Grad der Fehlertoleranz aufweisen. Das Ziel der VDI/VDE-Richtlinie 3528 ist es, mit nach konventionellem Regelwerk gefertigten COTS-Komponenten Leittechniksysteme realisieren zu können, die gleichwertige Zuverlässigkeitswerte aufweisen wie Leittechniksysteme, die nach nuklearen Standards hergestellt und qualifiziert wurden.

Um bei der Verwendung von COTS-Komponenten mit unterschiedlicher Qualifikationstiefe die Auslegungsziele eines Leittechniksystems zu erreichen, werden in der VDI/VDE-Richtlinie 3528 drei konzeptionelle Designvarianten definiert, damit die gleiche Zuverlässigkeit für Funktionen einer bestimmten Sicherheitskategorie durch unterschiedliche Schwerpunkte in der leittechnischen Anlagenkonfiguration erreicht werden kann. Die erste Designvariante umfasst COTS-Komponenten, für die keine Typprüfung oder eine andere Qualifizierung/Zertifizierung vorhanden ist, Designvariante zwei umfasst COTS-Komponenten, für die eine Qualifizierung/Zertifizierung basierend auf konventionellen Industriestandards vorliegt und die dritte Designvariante umfasst COTS-Komponenten mit einer durchgeführten Qualifizierung basierend auf nuklearen Standards.

In der ersten Designvariante dürfen laut /VDI 11/ nur solche COTS-Komponenten eingesetzt werden, die aus technischer Sicht geeignet sind, hochzuverlässige Systeme aufzubauen. Es sollten möglichst große Stückzahlen dieser Komponenten in unterschiedlichen Anwendungen eingesetzt sein, damit der Hersteller nachprüfbare und belastbare Angaben zur Betriebserfahrung machen kann. Diese Designvariante ist laut /VDI 11/ nur zur Realisierung von Funktionen zulässig, die Kategorie B oder C nach DIN 61226 /DIN 10a/ entsprechen. Dabei müssen Voraussetzungen erfüllt sein, die im Rahmen einer detaillierten Analyse anwendungsspezifisch geklärt und nachgewiesen werden müssen. Unter anderem muss nachgewiesen werden, dass die COTS-Komponenten mit ausreichenden Selbstüberwachungsmechanismen und der Fähigkeit zur Bildung fehlertoleranter Redundanzstrukturen sowie gerichtetem Ausfallverhalten ausgestattet sind. Die COTS-Komponenten zum Einsatz in Designvariante eins müssen außerdem über ausreichende Möglichkeiten zur Protokollierung von Fehlerzuständen und für Instandhaltungsmaßnahmen verfügen. Außerdem muss der Hersteller den Erfahrungsrückfluss für diese Komponenten sammeln, auswerten und bereitstellen und es muss eine ausreichende Anzahl an Ersatzteilen vorgehalten werden.

In der zweiten Designvariante werden solche COTS-Komponenten eingesetzt, die speziell für industrielle (nicht nukleare) Sicherheitsanwendungen entwickelt worden und für die jeweilige Anwendung mit geeigneten Zuverlässigkeitsmerkmalen ausgestattet sind. Die Zertifizierung dieser Komponenten (z. B. nach DIN 61508 /DIN 11/) muss durch ein akkreditiertes Prüfinstitut dokumentiert und bestätigt werden.

In Designvariante drei kommen ausschließlich COTS-Komponenten zum Einsatz, die nach kerntechnischem Regelwerk qualifiziert wurden und damit im Prinzip kerntechnisch qualifizierten Komponenten entsprechen.

Unter Berücksichtigung entsprechender Maßnahmen zur Beherrschung von zufälligen Fehlern, Folgefehlern und systematischen Fehlern sowie unter Berücksichtigung des Instandhaltungsfalls bei der Systemauslegung ist es laut /VDI 11/ möglich, Funktionen der Kategorie A nach DIN 61226 /DIN 10a/ unter Einsatz von COTS-Komponenten der Designvarianten zwei oder drei oder einer Kombination dieser beiden Designvarianten zu realisieren. Funktionen der Kategorien B oder C können mit COTS-Komponenten der Designvarianten eins bis drei realisiert werden. Insbesondere bei Funktionen der Kategorie A ist auf der Beherrschung des systematischen Fehlers ein besonderer Schwerpunkt zu legen. In jedem Fall ist die Prüfung der Eignung eines Systems für den spezifischen Einsatzfall erforderlich.

Für alle drei Designvarianten werden in /VDI 11/ Anforderungen aufgestellt. Diese beziehen sich beispielweise auf Aspekte zur Vorauswahl von COTS-Komponenten, d. h. Aspekte, die zur Einschätzung der Eignung der zur Auswahl stehenden Komponenten berücksichtigt werden sollten. Dies sind z. B. die Dokumentation von Hard- und Software, das Vorhandensein von Prüfdokumenten und anderen Qualifizierungen, das Vorhandensein der erforderlichen technischen Eigenschaften, eine ausreichende Robustheit, der Fertigungsprozess der Komponenten, die Ersatzteilstrategie des Herstellers sowie mögliche Instandhaltungsmaßnahmen. Weitere Anforderungen, die in /VDI 11/ aufgestellt werden, beziehen sich beispielweise auf das Qualitätsmanagement des Herstellers, bei der Produktentwicklung berücksichtigte Regelwerke, die Dokumentation und Tools zu ausgewählten Komponenten, Vorgaben und Anweisungen für die spätere Zielanwendung, den Nachweis der Eigenschaften der Komponenten, Vorkehrungen gegen systematische Ausfälle von programmierbaren oder rechnerbasierten Komponenten, Aspekte zur Systemauslegung, die Fehlererkennung, die Instandhaltbarkeit sowie Qualitätssicherungsmaßnahmen bei Projektierung, Inbetriebsetzung und Betrieb.

### 2.1.2 IAEA NR-T-3.31

Das IAEA-Dokument NR-T-3.31 „Challenges and Approaches for Selecting, Assessing and Qualifying Commercial Industrial Digital Instrumentation and Control Equipment for Use in Nuclear Power Plant Applications” /IAE 20/ beschäftigt sich mit dem Einsatz von digitalen kommerziellen Komponenten in der Sicherheitsleittechnik von Kernkraftwerken.

Die wichtigsten Ziele von /IAE 20/ sind die Erörterung von Herausforderungen im Zusammenhang mit dem Einsatz digitaler COTS-Komponenten sowie die Bereitstellung von Anforderungen für einen angemessenen Qualifizierungsprozess für COTS-Komponenten.

Herausforderungen im Zusammenhang mit dem Einsatz digitaler COTS-Komponenten in der Sicherheitsleittechnik von Kernkraftwerken folgen laut /IAE 20/ u. a. aus dem Umstand, dass COTS-Komponenten in der Regel Funktionen enthalten, die für die vorgesehene Anwendung nicht erforderlich sind und damit deutlich komplexer sind, als sie sein müssten. Daher ist vor der Qualifizierung von COTS-Komponenten die Komplexität der Komponenten zu bewerten, um sicherzustellen, dass die Komponente nicht zu komplex für einen Qualifizierungsprozess ist. Außerdem beinhalten COTS-Komponenten häufig Software, was bei einem Einsatz einer Komponente in mehreren Redundanten dazu führen kann, dass ein eventuell vorhandener Softwarefehler zu einem Ausfall der Komponenten in allen Redundanten führt. Daher ist laut /IAE 20/ das CCF-Potential von COTS-Komponenten zu bewerten.

Weitere Herausforderungen für den Einsatz digitaler COTS-Komponenten stehen laut /IAE 20/ im Zusammenhang mit spezifischen Hard- und Softwareschwachstellen solcher Komponenten. Es besteht die Möglichkeit des Auftretens neuer Fehlerarten, was eine zusätzliche Fehler- und/oder Gefahrenanalyse der COTS-Komponenten erforderlich macht. Außerdem sind Maßnahmen hinsichtlich Cybersicherheit zu ergreifen, wobei diese aufgrund der Möglichkeit von Eingriffen zu verschiedenen Zeitpunkten (z. B. bei Herstellung, Versand, Inbetriebnahme, Betrieb, usw.) mehrfach durchgeführt werden müssen. Des Weiteren sind organisatorische Herausforderungen zu bewältigen, die beispielsweise die Beschaffung von COTS-Komponenten, die Auswahl der Komponenten und insbesondere der Bereitschaft der Hersteller, Informationen zu diesen bereitzustellen, die Fragestellung, ob eine anwendungsspezifische oder generische Qualifizierung durchgeführt werden soll, die Bewertung von Änderungen (z. B. Hard- und Softwareupdates) an den COTS-Komponenten sowie die Problematik des Mangels an qualifizierten und erfahrenem Personal für den Qualifizierungsprozess umfassen.

In /IAE 20/ wird eine mögliche Strategie zur Qualifizierung von COTS-Komponenten vorgestellt, wobei herausgestellt wird, dass bei der Qualifizierung sowohl die nukleare Sicherheit als auch die Sicherung betrachtet werden muss. Hinsichtlich der Definition des erforderlichen Umfangs der Qualifizierung wird in /IEA 20/ festgestellt, dass der Umfang der Qualifizierung in erheblichem Maße von dem späteren Einsatz der COTS-

Komponenten abhängt. Insbesondere von Bedeutung ist dabei, ob die Komponenten nur auf eine bestimmte Anwendung ausgerichtet ist (anwendungsspezifische Qualifizierung) oder ob ein Einsatz der Komponenten in verschiedenen Anwendungen erfolgen soll (generische Qualifizierung). Vor dem Qualifizierungsprozess sind u. a. die Anforderungen an die COTS-Komponenten (z. B. gewünschte Funktionen, unerwünschtes Verhalten, Umgebungsbedingungen) sowie eventuelle Nutzungseinschränkungen und nicht benötigte Funktionalitäten der COTS-Komponenten zur Verringerung von deren Komplexität festzulegen und zu dokumentieren.

Bei der Bewertung von COTS-Komponenten sind laut /IEA 20/ im Rahmen einer Schwachstellenanalyse potentielle Schwachstellen der COTS-Komponenten zu ermitteln, welche im Rahmen des Qualifizierungsprozesses akzeptiert oder abgemildert werden müssen. Zudem ist zu überprüfen, wie die wichtigsten Anforderungen an das Verhalten der COTS-Komponenten erfüllt werden (z. B. Zuverlässigkeit, Genauigkeit, Reaktionszeit, Prüfbarkeit, usw.) und ob die COTS-Komponenten die Anforderungen aus den einschlägigen Regelwerken erfüllen. Weiterhin wird in /IAE 20/ beschrieben, dass bei der Integration der COTS-Komponenten in die Zielarchitektur die Qualifizierung und der Qualifizierungsumfang im Kontext der gesamten Leittechnikarchitektur der späteren Zielanwendung betrachtet werden muss. Dabei muss bewertet werden, ob das Verhalten, die Einschränkungen und alle anderen berücksichtigten Annahmen für die COTS-Komponenten für die spezifische Zielanwendung geeignet sind. Außerdem ist zu beachten, dass die tatsächlich eingebauten COTS-Komponenten auch dem Komponententyp entsprechen, der qualifiziert wurden.

Weitere in /IAE 20/ genannte Punkte hinsichtlich einer Strategie zur Qualifizierung von COTS-Komponenten betreffen die Einbeziehung bereits vorhandener Nachweise zur Qualifizierung der COTS-Komponenten (z. B. Herstellernachweise, Zertifizierungen, zusätzliche Tests und Analysen, Betriebserfahrungen) sowie die Auswahl des an der Qualifizierung beteiligten Personals, welches eine hohe Kompetenz und ein hohes Maß an Fachwissen aufweisen muss (z. B. hinsichtlich Hard- und Softwarearchitektur, Fehlermöglichkeiten und Schwachstellen, Regelwerk, Systemauslegung, Sicherheitsphilosophie, usw.). Außerdem wird beschrieben, dass die Tiefe der Nachweisführung während des Qualifizierungsprozesses der Sicherheitskategorie der Funktion entsprechen muss, in der die Komponenten später eingesetzt werden sollen. Soll ein Einsatz in Funktionen unterschiedlicher Sicherheitskategorien erfolgen, ist die Qualifizierung gemäß der höchsten Kategorie durchzuführen.

Neben den beschriebenen Herausforderungen für den Einsatz digitaler COTS-Komponenten und der möglichen Strategie zur Qualifizierung von COTS-Komponenten wird in /IAE 20/ ein möglicher Qualifizierungsprozess für COTS-Komponenten vorgestellt. Dieser soll mit der Festlegung von Anforderungen zur Gewährleistung, dass die COTS-Komponenten ihre späteren Funktionen erfüllen können und der Identifizierung von Voraussetzungen (z. B. Energieversorgung, Kommunikation, Umwelteinflüsse, Wartungsanforderungen) zur Erfüllung der Anforderungen beginnen. Daran anschließend erfolgt die Auswahl infrage kommender Komponenten, wobei sowohl die Funktionalität der COTS-Komponenten als auch die Bereitschaft des Herstellers, am Qualifizierungsprozess teilzunehmen, zu berücksichtigen sind. Der Hersteller muss im Rahmen des Qualifizierungsprozesses von COTS-Komponenten erforderliche Nachweise und Unterlagen sowie gegebenenfalls den Quellcode zur Verfügung stellen. Im Rahmen des Qualifizierungsprozesses wird geprüft, ob die COTS-Komponenten unter Anwendung geeigneter Verfahren und Techniken hergestellt wurden und ob Funktion, Leistung und Zuverlässigkeit der Komponenten den Anforderungen entsprechen. Zudem wird geprüft, ob potentielle Schwachstellen und Fehler behoben wurden und ob für die Betriebsbedingungen repräsentative Daten zu Einsatzbedingungen vorliegen, die zeigen, dass die Komponenten ihre Funktion für alle geforderten Betriebsumgebungen erfüllen. Zudem sind im Rahmen des Qualifizierungsprozesses Einschränkungen und Bedingungen zu ermitteln, die erforderlich sind, um die Verhaltenseigenschaften der COTS-Komponenten während ihrer gesamten Lebensdauer aufrecht zu erhalten. Der gesamte Qualifizierungsprozess ist zu dokumentieren.

In /IAE 20/ werden zudem Gründe genannt, bei deren Vorliegen zu prüfen ist, ob die Qualifizierung der COTS-Komponenten noch Gültigkeit besitzt. Dies sind beispielsweise Änderungen an Hard- oder Software oder dem Herstellungsprozess, die Meldung von Mängeln an den Komponenten, die fehlende Aufrechterhaltung einer Zertifizierung, die als Grundlage für die Qualifizierung verwendet wurde sowie das Auftreten neuer Schwachstellen oder Bedrohungen.

### 2.1.3 BS IEC 62671

Das Dokument BS IEC 62671 „Nuclear Power Plants – Instrumentation and control important to safety – Selection and use of industrial digital devices of limited functionality” /BSI 13/ befasst sich mit der Auswahl und Bewertung von rechnerbasierten oder programmierbaren, nicht speziell für den Einsatz in Kernkraftwerken hergestellten Komponenten mit begrenzter, spezifischer Funktionalität und begrenzter Konfigurierbarkeit, die

in Kernkraftwerken eingesetzt werden sollen. Das Dokument soll dabei Leitlinien zur Verfügung stellen, die es ermöglichen, entsprechende Komponenten auszuwählen und auf ihre Eignung zur Verwendung in Kernkraftwerken zu prüfen. In dem Dokument werden Systeme der Sicherheitsklassen 1, 2 und 3 angesprochen, in denen entsprechende Komponenten eingesetzt werden sollen. Dabei zeigt das Dokument die Möglichkeit eines graded approach auf, wobei für höhere Sicherheitsklassen strengere Anforderungen gelten sollen.

In den allgemeinen Anforderungen von /BSI 13/ werden Anforderungen aufgestellt, die bei der Auswahl infrage kommender COTS-Komponenten helfen sollen. Zur Auswahl von Komponenten sind zu Beginn die Anforderungen an die Komponenten zu definieren, wobei die später geplante Zielanwendung zu berücksichtigen ist. Ziel dabei ist es, bereits früh im Prozess der Auswahl der Komponenten zu betrachten, wie die Erfolgswahrscheinlichkeit für die Qualifizierung sowie die Auswirkungen der Nutzung der Komponenten sind. Des Weiteren werden allgemeine Anforderungen an den Qualifizierungsprozess aufgestellt, wobei der Ablauf der Qualifizierung dargestellt wird. Nach der Erstellung eines Qualifizierungs- und Anwendungsplans für die COTS-Komponenten erfolgt die Qualifizierung gemäß diesem Plan und abschließend die Dokumentation zur durchgeführten Qualifizierung. Der Qualifizierungs- und Anwendungsplan muss Themen behandeln wie beispielsweise den Umfang der Qualifizierung in Abhängigkeit von der späteren Zielanwendung, notwendige technische Ressourcen für die Qualifizierung, Anforderungen, Kriterien und Gewichtungsfaktoren sowie mögliche Ausgleichsmaßnahmen für den Fall, dass die Komponenten nicht alle Anforderungen erfüllt.

In /BSI 13/ werden außerdem funktionale und leistungsbezogene Kriterien für die Eignung der COTS-Komponenten zum Einsatz in der Sicherheitsleittechnik in Kernkraftwerken aufgestellt. Bei der Prüfung der Komponenten ist die Frage zu beantworten, ob der Prüfling die geforderten Funktionen (Hauptfunktionen) erfüllt, die sich aus den Anlagenanforderungen ableiten. Neben den Hauptfunktionen gibt es noch weitere Funktionalitäten (sekundäre Funktionen), die nicht Teil der Hauptfunktion sind, aber erforderlich sind, um Parameter der Hauptfunktion anzupassen oder die Zuverlässigkeit zu erhöhen (z. B. Selbstüberwachung). Diese müssen ebenfalls hinsichtlich ihrer Erfüllung überprüft werden, wobei außerdem nachzuweisen ist, dass der Betrieb oder eine Ausfallart einer Sekundärfunktion die Hauptfunktion nicht beeinträchtigen kann oder dass ein dadurch ausgelöster Ausfall der Komponenten sicherheitsgerichtet ist. Außerdem ist zu prüfen, ob die Komponenten noch weitere Funktionen haben, die nicht Teil der erforderlichen

Sicherheitsfunktion sind. Ihr Vorhandensein bedeutet möglicherweise eine unnötige Komplexität sowie zusätzliche Fehlermöglichkeiten, weshalb solche Funktionen bei höheren Sicherheitsklassen unerwünscht sind. Weitere Anforderungen beziehen sich auf die Konfigurierbarkeit, die Robustheit der Hardware (z. B. Qualifizierung hinsichtlich Umgebungsbedingungen), die Zuverlässigkeit (z. B. Ausfallarten, Selbstüberwachung), die Prüfbarkeit sowie die Cybersicherheit.

Des Weiteren sind laut /BSI 13/ Nachweise zu erbringen und zu bewerten, dass die COTS-Komponenten für den Einsatz in einem Kernkraftwerk geeignet sind. Dies kann z. B. durch eine Bewertung des Prozesses, der bei der Entwicklung der Komponenten zugrunde gelegt wurde einschließlich der Prüfung, ob das Design beibehalten wurde, oder durch eine Bewertung der Eigenschaften der Komponenten erfolgen. Wichtigste Elemente sind dabei der Nachweis eines geeigneten Entwicklungs- und Wartungslebenszyklus für Design und Fertigung, der Nachweis der Verwendung geeigneter Werkzeuge, der Nachweis einer Zertifizierung durch eine akkreditierte Instanz, der Nachweis von Vorkehrungen gegen systematische Fehler sowie die Überprüfung der Dokumentation über Auslegung, Herstellung und Verwendung der Komponenten. Sind diese Nachweise nicht vollumfänglich zu erbringen, besteht die Möglichkeit, etwaige Schwachstellen zu kompensieren. Dies kann z. B. erfolgen durch aussagekräftige Betriebserfahrung, komponentenspezifische ergänzende Prüfungen oder einer Kompensation auf Systemebene, um Komponentenausfälle abzumildern. Zusätzlich können ergänzende Prüfungen aus einer Vielzahl von Gründen durchgeführt werden, z. B. zur Berücksichtigung von Änderungen an den Komponenten, zur Schließung von Lücken im Qualifizierungsprozess oder zur Kompensation mangelhafter Betriebserfahrung.

In /BSI 13/ werden auch Kriterien für die Integration der COTS-Komponenten in die Zielanwendung gegeben, wobei Bedingungen und Grenzen für die Verwendung aufgestellt werden. Bedingungen und Einschränkungen zur Verwendung der Komponenten können sich aus Ergebnissen der Eignungsbeurteilung ergeben oder sie können auferlegt werden, um Komponenten ausschließlich für die Verwendung unter den auferlegten Einschränkungen und Bedingungen zu qualifizieren. Diese Einschränkungen können beispielsweise die Verwendung bis zu einer bestimmten Sicherheitskategorie, eine erforderliche Redundanz zur Verwendung der Komponenten, Grenzen hinsichtlich der Betriebsumgebung oder weitere begrenzende Faktoren sein. Des Weiteren können Komponenten als geeignet für die Verwendung in bestimmten Anwendungen bewertet

werden, wenn bestimmte Änderungen an der Hardware oder sehr geringfügige Änderungen an der Software vor der Verwendung der Komponenten vorgenommen werden. Dabei ist darauf zu achten, dass solche Änderungen nicht dazu führen, dass neue Komponenten entstehen. Die Änderungen müssen so beschaffen sein, dass sie nicht die Betriebserfahrungen, die bei der Qualifizierung berücksichtigt wurden, beinträchtigen. Zumindest dürfen die Änderungen nicht die Hauptfunktion der Komponenten konzeptionell ändern.

Außerdem werden in /BSI 13/ Anforderungen hinsichtlich der Wahrung der Qualifizierung der Komponenten gegeben. Dabei ist die gesamte Produktlebensdauer zu berücksichtigen, in welcher der Hersteller eine langfristige Unterstützung bereitstellen muss. Ausfälle der Komponenten, die nach dem Zeitraum der Auswertung der Betriebserfahrung aufgetreten sind, sind zu bewerten. Des Weiteren sollten die Komponenten im Hinblick auf die zu erwartende Supportlebensdauer sowie auf ihre eigene Lebensdauer bewertet werden. Im ersten Fall sind längere Supportzeiten wünschenswert und möglicherweise mit dem Hersteller verhandelbar. Im zweiten Fall dient das Wissen dazu, den Austausch der Komponenten vor dem Ende ihrer Lebensdauer zu planen. In dem Fall, dass Komponenten verwendet werden, nachdem der Hersteller die direkte Unterstützung eingestellt hat, kann es entscheidend sein, Fähigkeiten zur Instandhaltung der Komponenten verfügbar zu machen. Aus diesem Grund sollte die Bewertung die zukünftige Notwendigkeit berücksichtigen, die Komponenten ohne Hilfe des Herstellers zu betreiben.

### 2.1.4 Guidance for Commercial Grade Dedication

Das Dokument “Guidance for Commercial Grade Dedication” /DOE 11/ vom U. S. Department of Energy beschäftigt sich mit dem Einbau kommerzieller Komponenten in sicherheitsrelevanten Einrichtungen in Kernkraftwerken. Das Dokument soll einen Leitfaden zur Anwendung des Verfahrens der Commercial Grade Dedication bieten, anhand dessen Komponenten, die nicht entsprechend qualifiziert worden sind, in sicherheitsrelevanten Funktionen in Kernkraftwerken eingesetzt werden können. Dabei wird ein Verfahren beschrieben, welches eine hinreichende Gewähr liefern soll, dass die COTS-Komponenten die geforderten Sicherheitsfunktionen erfüllen und in dieser Hinsicht als gleichwertig zu nach nuklearen Richtlinien qualifizierten Komponenten betrachtet werden können. Des Weiteren enthält das Dokument auch Anleitungen für die Erstellung der zugehörigen Dokumentation.

Zu Beginn von /DOE 11/ wird der Prozess der Commercial Grade Dedication beschrieben. Dabei wird erwähnt, dass für die COTS-Komponenten ein Plan zu erstellen ist, welcher die kritischen Merkmale für das Bestehen des Prozesses, die verwendeten Methoden und die Akzeptanzkriterien festlegt. Zur Erstellung dieses Plans muss kompetentes Personal eingesetzt werden und es muss festgelegt werden, ob eine einzelne Komponente oder eine Gruppe von Komponenten betrachtet werden soll. Sollen COTS-Komponenten Sicherheitsfunktionen ausführen, sind laut /DOE 11/ Untersuchungen durchzuführen, um sicherzustellen, dass die Komponenten dazu geeignet sind. Dazu sind die auszuführenden Sicherheitsfunktionen festzulegen und dann zu bestätigen, dass die Komponenten die geltenden Anforderungen erfüllen. Außerdem muss eine technische Bewertung erfolgen, in welcher die kritischen Merkmale für das Design der Komponenten und deren Einsatz identifiziert werden. Nach der Auswahl einer oder mehrerer Akzeptanzmethoden und der Entwicklung von Akzeptanzkriterien erfolgt die Bewertung, ob die Komponenten diese erfüllen.

Bei der im Rahmen der Commercial Grade Dedication durchgeführten technischen Bewertung sollen laut /DOE 11/ der Umfang und die Grenzen des Einsatzes der COTS-Komponenten bewertet werden. Bei einem geplanten Einsatz der Komponenten in mehreren Sicherheitsfunktionen muss die Bewertung auf den Anforderungen der höchsten Sicherheitsklasse beruhen. Zur technischen Bewertung sind Auslegungsdokumente, technische Informationen vom Hersteller und Zulieferern sowie weitere einschlägige technischen Informationen und Informationen zur Betriebserfahrung heranzuziehen. Die technische Bewertung wird durchgeführt, um die Sicherheitsfunktionen der Komponenten zu bestimmen, die Klassifizierung sowie Leistungsanforderungen und anwendbare Betriebsbedingungen zu identifizieren, kritische Merkmale und Akzeptanzkriterien zu identifizieren sowie Methoden zur Überprüfung der Akzeptanzkriterien festzulegen. Bei der Identifizierung der kritischen Merkmale sind die Ausfallarten der Komponenten in ihrer Betriebsumgebung und die Auswirkungen dieser Ausfallarten auf die Sicherheitsfunktionen zu berücksichtigen. Außerdem sind während der technischen Bewertung die Umgebungsbedingungen, unter welcher die Sicherheitsfunktionen von den Komponenten ausgeführt werden müssen, festzulegen und zu bewerten.

Die kritischen Merkmale sind laut /DOE 11/ Merkmale, die für die Leistung der COTS-Komponenten wichtig sind und deren Erfüllung es ihnen erlauben, ihre Sicherheitsfunktionen auszuführen. Zur Identifizierung der kritischen Merkmale ist ein vollständiges Verständnis der Produktspezifikationen (z. B. Ausrüstung, Hardware, Software, Mensch-

Maschine-Schnittstelle, Qualitäts- und Zuverlässigkeitsanforderungen) der Komponenten eine wichtige Voraussetzung. Designanforderungen und Ausfallmodi sind ebenfalls zu berücksichtigen bei der Ermittlung der kritischen Merkmale. Insbesondere wenn die Komponenten Software enthalten, ist es wichtig, Spezifikationen und Designmerkmale zu ermitteln, die sich auf nicht genutzte, unbeabsichtigte oder verbotene Funktionen beziehen. Eine Fehlermöglichkeits- und Einflussanalyse (FMEA) liefert Informationen zur Bewertung und Verifizierung kritischer Merkmale. Es ist wichtig, die Ausfallarten und deren Auswirkungen zu verstehen, da dies bei der Identifizierung kritischer Merkmale hilfreich ist.

Die kritischen Merkmale lassen sich in drei Kategorien unterteilen. Zu den physikalischen Merkmalen gehören Eigenschaften der COTS-Komponenten wie z. B. Montage, Abmessungen, Teilenummer oder Softwareversion. Die Leistungsmerkmale sind spezifische Leistungserwartungen, welche die COTS-Komponenten erfüllen müssen, um die Sicherheitsfunktion ausführen zu können, wie z. B. die Reaktionszeit. Auch Anforderungen an die Umgebungsbedingungen mit Bezug zur Leistung (z. B. Erfüllung von Genauigkeitsanforderungen in einem bestimmten Temperaturbereich) oder Merkmale, die sich auf das Fehlermanagement und auf Funktionen, die nicht ausgeführt werden, beziehen, gehören zu den Leistungsmerkmalen. Die Zuverlässigkeitsmerkmale sind Merkmale, die bewertet werden müssen, um eine hinreichende Gewähr für die Qualität der COTS-Komponenten zu erhalten. Bei Hardware sind sie typischerweise mit Herstellungsfehlern, Alterung oder Abnutzung verbunden, bei Software mit Konstruktionsfehlern der Software oder Unstimmigkeiten zwischen Spezifikation und tatsächlichem Design. Die Zuverlässigkeitsmerkmale werden stark von den Prozessen und dem Personal beim Hersteller beeinflusst.

Zur Bewertung, dass die COTS-Komponenten die kritischen Merkmale erfüllen, ist laut /DOE 11/ im Verlauf der Commercial Grade Dedication die Auswahl einer oder mehrerer Akzeptanzmethoden zu treffen. Die Auswahl der Methode basiert dabei auf der Art der zu überprüfenden kritischen Merkmale, den verfügbaren Herstellerinformationen, der Qualität der Komponenten und des Herstellers und dem Grad der Standardisierung. Die nachfolgenden Methoden können entweder einzeln oder in Kombination angewendet werden, um ein Mittel der Gewährleistung zu bieten, dass die Komponenten die identifizierten Anforderungen erfüllen. Die Methode spezieller Tests und Inspektionen (Special Tests and Inspections) umfasst Aktivitäten in Form spezieller Tests und Inspektionen,

die bei oder nach dem Erhalt der Komponenten durchgeführt werden, um die Übereinstimmung mit den Akzeptanzkriterien zu prüfen. Es handelt sich um Prüfungen und Tests der Komponenten, wobei diese bereits als Teil des Lieferprozesses stattfinden können. Es sind aber auch Tests eingeschlossen, die nach der Installation der Komponenten in der vorgesehenen Zielanwendung durchgeführt werden. Die Methode der Überprüfung des Herstellers (Commercial Grade Survey of Supplier) beschreibt eine leistungsbasierte Bewertung des Herstellers der Komponenten. Sie wird durchgeführt, um die Angemessenheit der Qualitätskontrollen des Herstellers zu bestimmen, die in direktem Zusammenhang mit der Erfüllung der kritischen Merkmale der Komponenten stehen. Der Zweck der Methode der Überprüfung des Herstellers besteht darin, Komponenten auf Grundlage der Genehmigung der Prozesse des Herstellers zu qualifizieren. Dabei muss eine Besichtigung beim Hersteller durchgeführt werden und der Hersteller für akzeptabel befunden werden, bevor die Bestellung für die Komponenten aufgegeben werden darf. Die Methode der Überprüfung der Herkunft (Source Verification) beschreibt eine Prüfung der Komponenten im Werk des Herstellers oder einem anderen geeigneten Ort, die vor dem Versand der Komponenten stattfindet. Dies kann z. B. dazu dienen, den Herstellungsprozess an verschiedenen Stellen zu überwachen, beim Hersteller durchgeführte Tests zu bezeugen oder technische Arbeiten zu prüfen. Diese Methode umfasst Tätigkeiten wie z. B. die Beobachtung der Herstellungs- und Montageprozesse, die Entwicklung von Software, zerstörungsfreie Prüfungen, Leistungstests von Software oder Endkontrollen. Die Methode des Leistungsnachweises für Hersteller/Komponenten (Acceptable Supplier/Item Performance Record) basiert auf der dokumentierten, nachgewiesenen Leistung der Komponenten über einen bestimmten Zeitraum für identische oder ähnliche Komponenten. Die Methode lässt sich am besten anwenden, wenn die historische Betriebserfahrung zusammengestellt werden kann unter Verwendung von Produkttests der Industrie, nationalen Normen, überwachter Leistung der Komponenten in ähnlicher Umgebung wie vorgesehen und Datenbanken der Industrie oder Leistungsdaten, die sich aus der Verwendung der anderen Methoden ergeben. Diese Methode beinhaltet die Verwendung dokumentierter Aufzeichnungen der Betriebserfahrung der Komponenten.

Des Weiteren stellt /DOE 11/ Anforderungen an den Hersteller. Jeder Hersteller muss durch ein Audit im Rahmen eines Qualitätssicherungsprogramms qualifiziert werden und auf die Liste der zugelassenen Hersteller/Lieferanten gesetzt werden. Regelmäßige Re-Audits sind durchzuführen, damit der Hersteller qualifiziert bleibt. Ebenfalls muss jeder

Zulieferer gemäß dem Qualitätssicherungsprogramm des Herstellers für den Lieferumfang qualifiziert und in die Liste der zugelassenen Hersteller/Lieferanten aufgenommen werden. Festgestellte Mängel in Prozessen oder Kontrollen beim Hersteller müssen vom Hersteller korrigiert werden, wenn diese die Akzeptanzkriterien für kritische Merkmale beeinflussen.

### 2.1.5 DIN EN 61513

Die DIN EN 61513 „Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen“ /DIN 13/ enthält Anforderungen an leittechnische Systeme und Komponenten, welche zur Ausführung von Funktionen in Systemen mit sicherheitstechnischer Bedeutung in Kernkraftwerken eingesetzt werden. Dabei enthält /DIN 13/ Anforderungen und Empfehlungen für die gesamte leittechnische Architektur, wobei diese auf fest verdrahteten Komponenten, rechnerbasierten Komponenten oder einer Kombination beider Technologien beruhen kann. Die Anforderungen wurden aus den Sicherheitszielen der Anlage abgeleitet. Ein Abschnitt von /DIN 13/ befasst sich mit der Gesamtarchitektur des Leittechniksystems. In diesem Abschnitt werden Anforderungen an leittechnische Funktionen sowie zugehörige Systeme und Komponenten definiert und Auslegungskriterien hinsichtlich der Struktur der gesamten Leittechnikarchitektur, der Einteilung der Systeme und der Zuordnung der leittechnischen Funktionen zu den Systemen festgelegt. Ein weiterer Abschnitt befasst sich mit Anforderungen an einzelne Leittechniksysteme, die sicherheitstechnisch wichtige Funktionen ausführen, wobei insbesondere rechnerbasierte Systeme berücksichtigt werden. Des Weiteren beinhaltet /DIN 13/ Anforderungen an die Integration, die Inbetriebnahme, den Betrieb sowie die Wartung von Leittechniksystemen. Die Thematik des Einsatzes kommerzieller Komponenten wird in /DIN 13/ in einzelnen Abschnitten ebenfalls angesprochen. Relevante Anforderungen aus /DIN 13/ mit Bezug zu kommerziellen Komponenten werden nachfolgend zusammengefasst.

Ein Abschnitt von /DIN 13/ befasst sich mit der Auswahl bereits verfügbarer Komponenten, wobei unter bereits verfügbaren Komponenten neben kommerziellen Komponenten auch proprietäre Produkte verstanden werden, die vom Hersteller intern genutzt werden. Bei der Auswahl von COTS-Komponenten ist laut /DIN 13/ deren Eignung für den Einsatz in der Zielanwendung zu untersuchen, wobei gezeigt werden muss, dass die Eigenschaften der COTS-Komponenten den Anforderungsspezifikationen für das Zielsystem entsprechen. Die Einschätzung und Untersuchung der Eignung der COTS-

Komponenten sollte dabei auf zwei Arten von Dokumenten basieren, deren Inhalte miteinander zu vergleichen sind. Dies sind zum einen die Anforderungsspezifikationen für das Zielsystem und zum anderen die Dokumentation der COTS-Komponenten, die beispielsweise aus der Komponentenspezifikation und bereits vorhandenen Dokumenten zu vorherigen Qualifizierungen bestehen kann.

Bei der Einschätzung und Untersuchung der Eignung der COTS-Komponenten ist laut /DIN 13/ zu analysieren, ob in der zur Verfügung stehenden Dokumentation der COTS-Komponenten deren Funktionalitäten und Eigenschaften ausreichend erläutert werden. Ist dies nicht der Fall oder haben die COTS-Komponenten nicht explizit dokumentierte Eigenschaften, müssen diese mittels Analyse und Prüfung bestimmt und dokumentiert werden. Anhand der Dokumentation der COTS-Komponenten muss es möglich sein, die Zuverlässigkeit und die Leistungsfähigkeit der Komponenten bei Verwendung in der vorgesehenen Funktion unter der vorgesehenen Konfiguration und unter der vorgesehenen Betriebsumgebung zu bestimmen. Hinsichtlich des Softwareengineerings wird in /DIN 13/ erwähnt, dass in der Dokumentation der COTS-Komponenten die Funktionalität und die Eigenschaften der verwendeten Werkzeuge und Verfahren festgehalten sein müssen.

Laut /DIN 13/ müssen nicht genutzt Funktionen der COTS-Komponenten, also Funktionen, die in den Komponenten integriert sind, die in der beabsichtigten Zielanwendung aber nicht benötigt werden, offengelegt werden. Außerdem muss nachgewiesen werden, dass nicht genutzte Funktionen die geforderten Funktionen nicht unzulässig beeinträchtigen können.

Sollen COTS-Komponenten in sicherheitstechnisch wichtigen leittechnischen Systemen der Klassen 1 und 2, also in der Regel Systeme, die Funktionen der Kategorien A und B nach DIN 61226 ausführen, eingesetzt werden, ist laut /DIN 13/ die Machbarkeit der Qualifizierung der COTS-Komponenten in Übereinstimmung mit den in /DIN 13/ genannten Anforderungen für den Qualifizierungsprozess klassischer Leittechniksysteme festzustellen. Es besteht die Möglichkeit, Ergebnisse einer bereits vorhandenen Qualifizierung zu berücksichtigen. Dabei müssen die dort qualifizierten Eigenschaften der COTS-Komponenten explizit festgestellt werden und der Zugriff auf entsprechende Begründungen muss durch eine ausreichende Dokumentation sichergestellt werden. Sind zusätzliche Arbeiten und Einschränkungen für eine anlagenspezifische Qualifizierung notwendig, sind diese ebenfalls zu dokumentieren. Bei Berücksichtigung einer bereits vorhandenen Qualifizierung der COTS-Komponenten ist darauf zu achten, dass

sich diese immer nur auf eine spezielle Version der Komponenten bezieht. Jede Änderung an den COTS-Komponenten bedeutet eine Versionsänderung, woraufhin die Qualifizierung neu beurteilt werden muss.

### 2.1.6 DIN EN 60880

Die DIN EN 60880 „Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie A“ /DIN 10b/ stellt Anforderungen an die Software von softwarebasierten Leittechniksystemen auf, die in Kernkraftwerken Funktionen der Kategorie A ausführen sollen. Da Software zum Einsatz in Leittechniksystemen zur Ausführung von Funktionen der Kategorie A hochzuverlässig sein muss, wird in /DIN 10b/ jede Stufe der Software-Entwicklung und Dokumentation angesprochen, einschließlich Anforderungsspezifikationen, Auslegung, Realisierung, Verifizierung, Validierung und Betrieb. Es werden Anforderungen an die Software, die Auslegung und Implementierung, Software-Verifizierung, Integration, Modifizierung, Installation und Betrieb aufgestellt. Die Thematik des Einsatzes wieder verwendbarer, bereits verfügbarer Software, was im Prinzip COTS-Software entspricht, wird in /DIN 10b/ in einzelnen Abschnitten ebenfalls angesprochen, wobei Kriterien für den Einsatz solcher Software gegeben werden. Relevante Anforderungen aus /DIN 10b/ mit Bezug zu COTS-Software werden nachfolgend zusammengefasst.

Hinsichtlich der Konfiguration von COTS-Software wird in /DIN 10b/ gefordert, dass die Fähigkeit der Software evaluiert und analysiert werden muss. Dadurch ist sicherzustellen, dass die COTS-Software für den geplanten Einsatz im Zielsystem geeignet ist. Um die Möglichkeit menschlicher Fehler einzuschränken, ist bei der Konfiguration der Software eine werkzeugbasierte Vorgehensweise vorzuziehen. Außerdem sind alle relevanten Randbedingungen und Konfigurationsdaten zu dokumentieren. Zudem wird gefordert, dass die COTS-Software für die geplante Zielanwendung qualifiziert sein muss. Die Verifizierung muss durch die Verwendung einer Kombination von Inspektion (z. B. Betrachtung des Software-Codes), Analyse (statische Prüfung, z. B. Modellüberprüfung) und dynamischen Prüfungen (z. B. Simulation der Software) durchgeführt werden.

Hinsichtlich der Qualifizierung von COTS-Software wird in /DIN 10b/ generell ausgesagt, dass auch COTS-Software allen in /DIN 10b/ entwickelten Anforderungen entsprechen sollte. Dabei muss die Fähigkeit der COTS-Software festgestellt werden, die funktionalen, Leistungs- und Architekturanforderungen zu erfüllen. Außerdem muss ihre Eignung

zum Einsatz in der Zielfunktion nachgewiesen werden. Erforderliche Änderungen an der COTS-Software für ihre Korrektur oder Anpassung sind während der Bewertung festzulegen und ihre Qualität zu beurteilen. Falls erforderlich ist die Betriebserfahrung der COTS-Software zu berücksichtigen.

Der Prozess zur Bewertung der COTS-Software muss laut /DIN 10b/ eine Bewertung der Funktions- und Leistungsmerkmale und der Dokumentation ihrer Qualifizierung umfassen. Außerdem sind die Qualität des Software-Entwurfs- und Entwicklungsprozesses sowie die Betriebserfahrung (wenn diese zum Ausgleich von Schwächen erforderlich ist) zu bewerten. Die Erkenntnisse aus der Bewertung sowie erforderliche Maßnahmen zur Ertüchtigung der COTS-Software sind in einer umfassenden Dokumentation zu beschreiben. Um den Entwickler beim Entwurf einer Systemarchitektur zu unterstützen und sicherzustellen, dass die Funktionalität und Leistungsfähigkeit der COTS-Software die Anforderungen des Zielsystems erfüllt, sollte die Bewertung der Eignung der COTS-Software in einem frühen Stadium der Erstellung der Systemspezifikation abgeschlossen werden.

Bei der Qualifizierung der COTS-Software muss die Spezifikation der COTS-Software laut /DIN 10b/ im Vergleich zur Anforderungsspezifikation des Zielsystems bewertet werden. Sind Abweichungen vorhanden, darf die COTS-Software entweder nicht verwendet werden oder es sind entsprechende Änderungen durchzuführen, damit die spezifizierten Anforderungen des Zielsystems erfüllt werden. Ebenfalls möglich ist eine Änderung der Anforderungsspezifikation, damit die COTS-Software diese erfüllen kann. Dabei ist darauf zu achten, dass durch die Änderung keine sicherheitstechnisch wichtigen Funktionen beeinträchtigt werden. Bei der Bewertung der Eignung der COTS-Software sind enthaltene Funktionen zu identifizieren, die für die vorgesehene Zielanwendung nicht benötigt werden. Außerdem sind Maßnahmen festzulegen, dass diese Funktionen die Sicherheitsfunktion nicht beeinflussen können.

Wurden während der Qualifizierung Mängel an der COTS-Software aufgedeckt, können diese laut /DIN 10b/ mittels der Berücksichtigung geeigneter Betriebserfahrung kompensiert werden. Dabei sind die für die Sammlung der Betriebserfahrung, die Aufzeichnung der Betriebszeiten und die Erstellung der Betriebshistorie verwendeten Verfahren zu bewerten. Bei der Auswertung der Betriebserfahrung sind Befunde, Mängel und Fehlerberichte zu berücksichtigen sowie Änderungen an der COTS-Software im Laufe der Betriebshistorie zu bewerten. Die Betriebserfahrung darf dann berücksichtigt werden,

wenn sie sich auf Betriebsbedingungen bezieht, die mit denen in der vorgesehenen Zielanwendung vergleichbar sind und wenn sie sich auf die gleiche Version der COTS-Software bezieht, die für die Verwendung vorgesehen ist. Soll Betriebserfahrung anderer Versionen berücksichtigt werden, sind die Unterschiede dieser Versionen zu analysieren. Informationen über Fehler und Ausfälle in anderen Anlagen und Anwendungen sowie über entsprechende Änderungen der COTS-Software sollten auch während deren Verwendung kontinuierlich aufgenommen und ausgewertet werden.

Für die COTS-Software ist laut /DIN 10b/ ein Konfigurationsmanagement zu erstellen, damit die genutzte Version und Konfiguration exakt bekannt sind. Nur die in der Qualifizierung der COTS-Software beschriebene Version mit den dort identifizierten erforderlichen Änderungen darf später im Zielsystem verwendet werden.

### 2.1.7 IEC 62138

Die IEC 62138 „Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category B or C functions" /IEC 18/ stellt Anforderungen an die Software von softwarebasierten Leittechniksystemen auf, die in Kernkraftwerken Funktionen der Kategorien B oder C ausführen sollen. Es werden unter anderem Anforderungen an die Software, das Software-Design sowie die Implementierung, die Installation und die Modifizierung der Software aufgestellt. Dabei wird auch die Thematik des Einsatzes vorgefertigter Software angesprochen, die nicht notwendigerweise für den Einsatz in kerntechnischen Anlagen entwickelt wurde, was COTS-Software entspricht. Relevante Anforderungen aus /IEC 18/ mit Bezug zu COTS-Software werden nachfolgend zusammengefasst.

Hinsichtlich der Auswahl von COTS-Software wird in /IEC 18/ ausgesagt, dass COTS-Software über eine Dokumentation verfügen muss, welche die notwendigen Informationen liefert, die für die sichere Verwendung der COTS-Software erforderlich sind. Dies umfasst neben der von Hersteller gelieferten Benutzerdokumentation weitere Dokumente, wie z. B. Informationen aus zusätzlichen Tests, Messungen und Analysen sowie Informationen aus der Betriebserfahrung. Dabei muss die Dokumentation Punkte wie z. B. die bereitgestellten Funktionen, Schnittstellen zur Anwendungssoftware, Funktionen, Typen, Formate, Bereiche und Einschränkungen von Eingängen, Ausgängen, Signalen, Parametern und Konfigurationsdaten, Informationen zur Leistungsfähigkeit der

Funktionen (z. B. in Bezug auf die Reaktionszeit), verschiedene Betriebsarten und entsprechende Übergangsbedingungen sowie Einschränkungen, die bei der Verwendung zu beachten sind umfassen.

Für COTS-Software, die Funktionen der Kategorie B ausführen soll, muss die Dokumentation laut /IEC 18/ außerdem Informationen zu vorhandenen Selbstüberwachungsmechanismen, zur Toleranz gegen Fehler sowie Fehlermöglichkeiten, zu Anforderungen an die Laufzeitumgebung der COTS-Software sowie zu Interaktionen und Schnittstellen der COTS-Software mit der Hardware beinhalten. Außerdem müssen Informationen bereitgestellt werden, die korrekte Vorhersagen über die wichtigsten sicherheitsrelevanten Elemente des Systems ermöglichen, wobei insbesondere maximale Antwortzeiten und die maximale Nutzung von Ressourcen zu beachten sind.

Hinsichtlich der Qualifizierung der COTS-Software wird in /IEC 18/ ausgesagt, dass die Korrektheit der Software in Bezug auf ihre Dokumentation während der Qualifizierung nachzuweisen ist. Bei der Qualifizierung ist zu unterscheiden zwischen einem Gesamtbetriebssystem und einzelnen Softwarekomponenten. Die Qualifizierung einzelner Softwarekomponenten (z. B. Bibliotheken, Firmware) kann laut /IEC 18/ durch relevante, ausreichende und positive Betriebserfahrung oder eine bereits vorhandene Zertifizierung erfolgen, während im Gegensatz dazu die Qualifizierung für ein Gesamtbetriebssystem deutlich anspruchsvoller ist.

Zur Qualifizierung eines Gesamtbetriebssystems sollte laut /IEC 18/ die Erfüllung der in /IEC 18/ an die COTS-Software gestellten Anforderungen bewertet werden. Ergeben sich begrenzte Abweichungen, können diese Abweichungen durch für die Zielanforderung relevante, positive Betriebserfahrung kompensiert werden. Liegt keine Betriebserfahrung vor, können ergänzende Tests verwendet werden. Begrenzte Abweichungen sind Fälle, in denen der in /IEC 18/ beschriebene Sicherheitslebenszyklus für die COTS-Software befolgt und dokumentiert wurde, aber nicht alle Anforderungen aus /IEC 18/ vollumfänglich erfüllt wurden. Ergeben sich erhebliche Abweichungen, sollten diese durch ergänzende Prüfungen kompensiert werden. Erhebliche Abweichungen sind Abweichungen, in denen ein vollständiger Sicherheitslebenszyklus der COTS-Software nicht eingehalten und dokumentiert wurde.

Durch ergänzende Prüfungen ist laut /IEC 18/ der Nachweis zu erbringen, dass die COTS-Software sich unter den vorgesehenen Einsatzbedingungen (z. B. Konfiguration, Nutzung von Funktionen und Schnittstellen, Hardwareumgebung, Prozessor) so verhält,

wie es in der Sicherheitsdokumentation beschrieben ist. Werden ergänzende Prüfungen durchgeführt, sind diese zu dokumentieren. Dabei sind die geprüfte Version der COTS-Software, die vorhandene Konfiguration, eine detaillierte Beschreibung der durchgeführten Prüfungen, der Aufbau der Testumgebung, den Prüfungen zugrunde gelegte Annahmen, die Ergebnisse der Prüfungen und der Nachweis deren Korrektheit sowie aus den Prüfungen gezogene Schlussfolgerungen zu dokumentieren.

Soll die Betriebserfahrung bei der Qualifizierung von COTS-Software berücksichtigt werden, ist der Umfang der berücksichtigten Betriebserfahrung zu dokumentieren. Bei COTS-Software, die in Funktionen der Kategorie B eingesetzt werden soll, sollte die Betriebserfahrung genau der verwendeten Version der COTS-Software entsprechen. Zudem ist der Nachweis zu erbringen, dass die Betriebserfahrung den Einsatzbedingungen entspricht. Die bei der Sammlung der Betriebserfahrung berücksichtigten Methoden sind zu dokumentieren. Insbesondere ist zu nachzuweisen, dass die aufgetretenen Fehler korrekt erkannt und gemeldet wurden. Außerdem ist der Nachweis zu erbringen, dass diese Fehler korrekt analysiert und entsprechend behoben wurden.

Laut /IEC 18/ besteht auch die Möglichkeit, eine bereits vorhandene, nicht notwendigerweise nukleare Zertifizierung einer COTS-Software bei deren Qualifizierung zu berücksichtigen. Dazu muss die Zertifizierung unter bestimmten Bedingungen durchgeführt worden sein. Die für die Zertifizierung verwendete Sicherheitsdokumentation muss ausdrücklich auf den Softwareentwicklungsprozess eingehen. Außerdem muss die Zertifizierung dokumentiert worden sein, wobei die genaue Identifizierung der COTS-Software ersichtlich sein muss. Bei COTS-Software, die in Funktionen der Kategorie B eingesetzt werden soll, müssen die Nachweise, die die Zertifizierung stützen, zudem bewertbar sein. Dies gilt insbesondere für die Bedingungen (z. B. Einsatzbedingungen und Annahmen), die zur Zertifizierung getroffen wurden, für die bei der Zertifizierung genutzten Werkzeuge und Methoden sowie für die Ergebnisse der Zertifizierung.

Laut /IEC 18/ ist sicherzustellen, dass die COTS-Software für den Einsatz im Zielsystem geeignet und nicht zu komplex ist. Außerdem ist die Dokumentation der COTS-Software im Hinblick auf die Spezifikation und das Design des Zielsystems zu bewerten und Unstimmigkeiten sind zu beseitigen. Bei COTS-Software, die in Funktionen der Kategorie B eingesetzt werden soll, sind die Funktionen, die nicht zur Unterstützung der Anforderungsspezifikation des Zielsystems benötigt werden, zu identifizieren. Es ist zu begründen, dass diese Funktionen keine nachteiligen Auswirkungen auf die Sicherheit haben. Generell sollten unnötige Funktionen in der COTS-Software vermieden werden und die

Software sollte nicht mehr Funktionen haben als erforderlich, um die Komplexität zu minimieren.

Werden an einer bereits qualifizierten COTS-Software Änderungen vorgenommen, sind diese Änderungen laut /IEC 18/ zu bewerten. Außerdem ist durch dokumentierte Nachweise in Bezug auf die Änderungen zu rechtfertigen, dass die Ziele der Änderungen erfüllt sind, dass keine Fehler eingeführt wurden und dass die geänderte Software mit der aktualisierten Dokumentation übereinstimmt. Bei COTS-Software, die in Funktionen der Kategorie B eingesetzt werden soll, ist zudem zu begründen, dass diese Nachweise ausreichen, gegebenenfalls auch unter Berücksichtigung der Änderungen und der Einsatzbedingungen.

### 2.1.8 DIN EN 60987

Die DIN EN 60987 „Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen an die Hardware-Auslegung rechnerbasierter Systeme“ /DIN 10c/ enthält Anforderungen an die Rechnerhardware für Systeme, die Funktionen der Kategorien A und B in Kernkraftwerken ausführen. Dabei werden beispielsweise Hardwareanforderungen (z. B. Leistungsanforderungen, Anforderungen an die Umgebungsbedingungen, Zuverlässigkeitsanforderungen), Anforderungen an die Auslegung der Hardware, an die Verifizierung und Validierung sowie an Qualifizierung, Herstellung, Installation, Wartung und Änderungen angesprochen. Obwohl /DIN 10c/ primär Aspekte der Hardwareentwicklung anspricht, werden auch Anleitungen zur Beurteilung und Verwendung vorgefertigter Hardware, was COTS-Komponenten entspricht, gegeben. Relevante Anforderungen aus /DIN 10c/ mit Bezug zu COTS-Komponenten werden nachfolgend zusammengefasst.

Generell wird in /DIN 10c/ ausgesagt, dass COTS-Komponenten, die in sicherheitstechnisch relevanten Systemen eingesetzt werden sollen, vor deren Einsatz überprüft, verifiziert und getestet werden müssen. Außerdem muss bei Verwendung von COTS-Komponenten deren Nutzung im Hardware-Qualitätssicherungsplan angesprochen werden.

Bei der Verwendung von COTS-Komponenten müssen laut /DIN 10c/ vor deren Verwendung Untersuchungen durchgeführt werden, durch die sichergestellt wird, dass die Leistungscharakteristiken der COTS-Komponenten mit den Systemanforderungen übereinstimmen. Wird bei diesen Untersuchungen festgestellt, dass Abweichungen vorliegen,

sind diese Abweichungen entweder durch Änderungen an den COTS-Komponenten oder durch Anpassungen der Systemauslegung zu beheben. Dabei darf es zu keiner Beeinträchtigung der Sicherheitsanforderungen für das System kommen.

Bezüglich der Auslegung und Entwicklung von COTS-Komponenten erfolgt in /DIN 10c/ die Aussage, dass die Möglichkeit besteht, dass für die ganze Systemhardware COTS-Komponenten benutzt werden können. Es besteht aber auch die Möglichkeit, nur für eine Teilmenge der Hardwarekomponenten COTS-Komponenten zu verwenden. In der Hardwareauslegung müssen Anforderungen an das System berücksichtigt werden. Es ist der Nachweis zu erbringen, dass diese Anforderungen (z. B. Rechengenauigkeit, Ansprechzeit, Umgebungsbedingungen, Energieversorgung) durch die Hardwareauslegung erfüllt werden. Hinsichtlich COTS-Komponenten ist zu verifizieren, dass die Hardwarespezifikation der COTS-Komponenten den Anforderungen an die Systemhardware entspricht. Dabei ist sicherzustellen, dass die COTS-Komponenten die spezifizierten Anforderungen erfüllen. Kann dies nicht nachgewiesen werden, ist die Leistungsfähigkeit der COTS-Komponenten durch Prüfungen nachzuweisen. Generell wird ausgesagt, dass die COTS-Komponenten ihre Aufgaben innerhalb der Systemhardware erfüllen können müssen.

Hinsichtlich der Verifizierung und Validierung wird in /DIN 10c/ ausgesagt, dass die Eignung von COTS-Komponenten für die vorgesehene Verwendung untersucht werden muss. Dabei müssen diverse Aspekte der Auslegung berücksichtigt werden. Der bei der Entwicklung der COTS-Komponenten verwendete Auslegungsprozess ist in die Untersuchung einzubeziehen. Außerdem ist die Betriebserfahrung der COTS-Komponenten zu berücksichtigen. Dadurch kann erreicht werden, dass durch aktuelle Daten zur Zuverlässigkeit der COTS-Komponenten bestätigt wird, dass die Zuverlässigkeitsziele erreichbar sind, was Vertrauen in die Leitungsfähigkeit der COTS-Komponenten schaffen kann. Wenn bei der Untersuchung des bei der Entwicklung der COTS-Komponenten verwendeten Auslegungsprozesses Abweichungen zu den Anforderungen festgestellt werden, können relevante, der vorgesehenen Anwendung entsprechende Daten aus der Betriebserfahrung mit guter Anwendungserfahrung diese Abweichungen kompensieren. Ergeben sich aus der Untersuchung des bei der Entwicklung der COTS-Komponenten verwendeten Auslegungsprozesses keine ausreichenden Informationen, um den Einsatz der COTS-Komponenten in der vorgesehenen Anwendung zu rechtfertigen, besteht die Möglichkeit, weitere Arbeiten zur Unterstützung der Untersuchungen durchzuführen, wie z. B. Tests, Analysen oder sonstige Begründungen.

### 2.1.9 COTS Hardware and Software for Train Control Applications

Das Dokument “Commercial-Off-The-Shelf (COTS) Hardware and Software for Train Control Applications: System Safety Considerations” /DOT 03/ von der Federal Railroad Administration des U. S. Department of Transportation beschäftigt sich mit der Machbarkeit des Einsatzes kommerzieller, rechnerbasierter Komponenten in sicherheitsrelevanten Einrichtungen bei der Bahn. Grundlegende Herausforderungen für den Einsatz von COTS-Komponenten werden vor allem in der Bewertung der Komponenten sowie der Gewährleistung der Sicherheit in allen Phasen des Lebenszyklus der Komponenten gesehen. Zur Auswahl und Bewertung von COTS-Komponenten sind laut /DOT 03/ die technischen und betriebswirtschaftlichen Anforderungen zu berücksichtigen. Außerdem muss der gesamte Lebenszyklus angepasst werden, um Dingen wie der Bewertung der Komponenten oder der großen Geschwindigkeit von Änderungen auf dem Markt Rechnung zu tragen. Deshalb wird in /DOT 03/ ein neuer Lebenszyklus für Systeme mit COTS-Komponenten vorgeschlagen. Außerdem werden Methoden zur Sicherheitsüberprüfung und -validierung ohne COTS-Komponenten den Ansätzen zur Validierung bei der Integration von COTS-Komponenten gegenübergestellt.

In /DOT 03/ wird ein Überblick über die wichtigsten Vor- und Nachteile von COTS-Komponenten gegeben. Dazu werden zu mehreren Themengebieten Fragen hinsichtlich der Verwendung von COTS-Komponenten aufgeworfen. Hinsichtlich der Kosten wird ausgesagt, dass Marktforschungs- und Produktanalysen durchzuführen sind, um geeignete COTS-Komponenten zu finden. Gerade bei sicherheitsrelevanten Anwendungen können die Kosten hierfür schnell den Nutzen übersteigen. Ebenfalls relevant hinsichtlich der Kosten sind beispielsweise Softwareänderungen zur Sicherstellung, dass Probleme regelkonform behandelt werden Hinsichtlich der Qualität wird ausgesagt, dass die Qualität der COTS-Komponenten ausreichen muss, um diese zu verwenden. Daher muss ein COTS-basierter Lebenszyklus die Bewertung der Qualität der COTS-Komponenten einbeziehen. Das Ausmaß der Veränderungen, die bei der Verwendung von COTS-Komponenten im Lebenszyklus auftreten, sollte berücksichtigt werden. Wird das System, in dem COTS-Komponenten eingebaut werden sollen, über einen längeren Zeitraum in Betrieb sein, ist es laut /DOT 03/ wichtig, den Hersteller in die Überlegungen einzubeziehen. Stellt der Hersteller seine Geschäftstätigkeit ein, kann der Support und die Wartung für die COTS-Komponenten wegfallen.

Die Auswirkungen von Aktualisierungen der COTS-Komponenten auf den Entwicklungs- und Wartungszyklus sollten laut /DOT 03/ ebenfalls berücksichtigt werden. Die aktualisierte Funktionalität entspricht möglicherweise nicht den Bedürfnissen des Nutzers oder kann zu einer potentiellen Inkompatibilität führen. Zudem unterstützt der Hersteller oftmals nur eine begrenzte Anzahl an Versionen. Die potentiellen Auswirkungen unbeabsichtigter Funktionen sowie die Aktivierung nicht genutzter Funktionen müssen bei der Qualifizierung von COTS-Komponenten bewertet werden, was bei komplexen COTS-Komponenten oftmals mit erheblichem Aufwand verbunden ist. Sollen die COTS-Komponenten in sicherheitsrelevanten Funktionen eingesetzt werden, ist die mangelnde Einsicht in den Entwicklungsprozess der COTS-Komponenten oder der Zugriff auf den Quellcode laut /DOT 03/ ein übergeordnetes Problem. Dies kann dazu führen, dass die Eignung der Komponente oder deren Zuverlässigkeit nur schwer oder gar nicht bestimmt werden kann. Zudem ist es notwendig zu bewerten, wie gut die COTS-Komponenten mit der Software-Architektur des Systems gekoppelt werden können. Dies hat neben Kostenfragen (z. B. durch evtl. Anpassung der Software-Architektur) auch unmittelbare Auswirkungen auf die Verfügbarkeit von in Frage kommenden Komponenten.

Aufgrund der Schnelllebigkeit von COTS-Komponenten wird in /DOT 03/ eine grundlegende Herausforderung beim Einsatz von COTS-Komponenten gesehen. Diese Herausforderung besteht darin, sowohl kurz- als auch langfristige Aspekte zu berücksichtigen. Kurzfristig ist ein Gleichgewicht zwischen Systemarchitektur, Marktanforderungen und Integrationsaspekten herzustellen. Langfristig ist es notwendig, dass auf COTS-Komponenten basierte System zu erhalten und weiterzuentwickeln. Der Lebenszyklus muss in der Lage sein, auf die durch technologischen Wandel und die Weiterentwicklung erforderlichen Aktualisierungen zu reagieren. Dabei sind zu jeder Zeit sicherheitsrelevante Maßnahmen durchzuführen, um die Sicherheit nicht zu beeinträchtigen. Da COTS-Komponenten sich während der Entwicklung und Integration verändern können, muss der Lebenszyklus entsprechend flexibel sein, um Upgrades und Änderungen an COTS-Komponenten zu ermöglichen. Dabei ist es wichtig, dass das erforderliche Leistungsniveau auch nach der Einführung von COTS-Komponenten beibehalten wird.

Außerdem werden in /DOT 03/ Anforderungen hinsichtlich der Bewertung und Prüfung von COTS-Komponenten gegeben. Die Bewertung von COTS-Komponenten muss bereits bei der Konzeption des Systems beginnen und ist Teil aller weiteren Aktivitäten. Dabei ist die Qualität der COTS-Komponenten im Hinblick auf ihre Eignung für den vorgesehenen Einsatz zu bestimmen. Die Bewertung muss Alternativen identifizieren,

Bewertungskriterien in Bereichen wie Funktion, Leistung, Schnittstellen, Wartung, Support vom Hersteller, Kosten, Zuverlässigkeit sowie Sicherheit definieren und Alternativen anhand der Kriterien bewerten. Die Aktivitäten für den Nachweis der Qualität der COTS-Komponenten sind während der gesamten Lebensdauer eines Systems durchzuführen, vor der Entwicklung eines neuen Systems, während der Implementierung eines Systems und beim Austausch einer Komponente eines Systems. Es ist zu bewerten, ob die COTS-Komponenten zuverlässig sind und wie angekündigt funktionieren und ob das Zielsystem und die COTS-Komponenten kompatibel sind. Zur Qualifizierung von COTS-Komponenten können laut /DOT 03/ diverse Quellen für benötigte Informationen herangezogen werden. Entsprechende Quellen wären beispielweise Untersuchungen des Entwicklungsprozesses des Herstellers und der zugehörigen Dokumentation, durchgeführte Tests an COTS-Komponenten oder die Auswertung der Betriebserfahrung der COTS-Komponenten.

Des Weiteren werden in /DOT 03/ Empfehlungen für den Einsatz von COTS-Komponenten gegeben. Hinsichtlich des Schutzes vor unerwünschten Funktionalitäten von COTS-Komponenten wird ausgesagt, dass geeignete Methoden zur Kontrolle der COTS-Komponenten eingesetzt werden sollten, um Sicherheitsbedenken zu berücksichtigen. Eine Methode besteht beispielsweise darin, nur Komponenten zu verwenden, die die Erwartungen des Endnutzers erfüllen, ohne unerwünschte Funktionalitäten zu bieten. Techniken zur Gefahrenanalyse (z. B. Functional Hazard Analysis) können dabei helfen, zu bestimmen, welche Funktionen zu vermeiden sind. Sicherheitsanalysetechniken (z. B. Fehlerbaumanalyse) können verwendet werden, um zu untersuchen, wie die Komponenten die Sicherheit des Systems beeinflussen können. Eine weitere Möglichkeit ist die Nutzung eines Software-Wrappers, der um eine Software platziert wird, um alle Interaktionen zu kontrollieren. Dadurch wird verhindert, dass unerwünschte Ein- und Ausgänge die Systemfunktionalität beeinträchtigen. Es werden keine Änderungen am Quellcode vorgenommen, sondern die Funktionalität wird verändert und eingeschränkt. Damit COTS-Komponenten sicher und effektiv eingesetzt werden können, sollte eine fehlertolerante Softwarearchitektur implementiert werden. Ein weiterer Ansatz besteht darin, neben dem auf COTS-Komponenten basierenden System ein einfaches Backup-System mit gesicherter Zuverlässigkeit bereitzustellen.

### 2.1.10 Simple and Complex Electronic Hardware Approval Guidance

Das Dokument “Simple and Complex Electronic Hardware Approval Guidance” /DOT 17/ von der Federal Aviation Administration des U. S. Department of Transportation soll einen Leitfaden zur Genehmigung sowohl einfacher als auch komplexer elektronischer Komponenten in der Luftfahrt in den USA geben. Der Leitfaden gilt für Systeme und die elektronische Hardware dieser Systeme zur Verwendung in der Luftfahrt und ist eine Ergänzung zum Standard RTCA/DO-254, der von der RTCA (Radio Technical Commission for Aeronautics) entwickelt wurde und von Luftfahrtaufsichtsbehörden wie der Federal Aviation Administration (FAA) oder der European Aviation Safety Agency (EASA) für die Entwicklung von luftgestützter elektronischer Hardware übernommen wurde, aber nicht öffentlich zugänglich ist. In diesem Leitfaden werden diverse Themen bezüglich der Qualifizierung einfacher und komplexer elektronischer Komponenten angesprochen, wie beispielsweise modifizierbare Komponenten, Zertifizierungspläne, Validierungsprozesse, Konfigurationsmanagement, Bewertung und Qualifizierung von Werkzeugen oder Rückverfolgbarkeit. In einem Unterkapitel dieses Leitfadens wird der Einsatz von COTS-Komponenten behandelt.

Zu Beginn erfolgt in /DOT 17/ die Definition von COTS-Komponenten, wobei COTS-Komponenten als Komponenten beschrieben werden, die von einem Hersteller für mehrere Kunden entwickelt werden und deren Entwurf und Konfiguration durch eine Spezifikation des Herstellers oder einer Branche gesteuert werden. COTS-Komponenten werden in der Regel nicht von dem Unternehmen entwickelt, welches die Qualifizierung der Komponenten benötigt. Sie können, müssen aber nicht nach einem Industriestandard entwickelt worden sein. Aus diesem Grund ist sicherzustellen, dass die Verwendung von COTS-Komponenten den geltenden Anforderungen, Vorschriften, Grundsätzen und Leitlinien entspricht.

In /DOT 17/ wird darauf hingewiesen, dass die Verfügbarkeit von COTS-Komponenten nicht automatisch garantiert, dass diese in einer Weise verwendet werden können, die mit den Anforderungen, Vorschriften, Grundsätzen und Leitlinien übereinstimmt. Je nach Komplexität der COTS-Komponenten und Verfügbarkeit ihrer Dokumentation muss unter Umständen erheblicher Aufwand betrieben werden, um die Konformität mit dem Zielsystem nachzuweisen. Dabei ist nachzuweisen, dass COTS-Komponenten die geltenden funktionalen und sicherheitsbezogenen Anforderungen erfüllen. Um dies zu bewerkstelligen, müssen unter Umständen die Systemarchitektur, die Komponentenprüfung, die Tests, die Analyse und andere Daten aus dem Lebenszyklus entwickelt oder

ergänzt werden. Dies ist erforderlich, um die beabsichtigten Funktionen der COTS-Komponenten nachzuweisen und zu zeigen, dass das System bei Einsatz der COTS-Komponenten kein anormales Verhalten zeigt und den geltenden Vorschriften entspricht sowie die Anforderungen erfüllt.

Zum Nachweis, dass bei einem Einsatz von COTS-Komponenten die Anforderungen, Vorschriften, Grundsätze und Leitlinien eingehalten werden, können laut /DOT 17/ diverse Methoden zur Anwendung kommen. Durch Reverse-Engineering kann man beispielsweise erforderliche Daten aus dem Lebenszyklus von COTS-Komponenten anhand bekannter Informationen über Funktionalität und Design erhalten. Mittels der Durchführung umfassender Tests und Analysen von COTS-Komponenten können detaillierte Informationen über deren Funktionalität sowie über deren Verhalten unter Grenz- und Fehlerbedingungen erhalten werden. Dabei sind auch alle Funktionen, die in der spezifischen Zielanwendung nicht verwendet oder aktiviert werden, zu prüfen und zu analysieren. Jegliche Funktionalität von COTS-Komponenten, die in der spezifischen Zielanwendung nicht verwendet oder aktiviert wird, ist möglichst abzuschalten. Zudem können dokumentierte Nachweisen des Herstellers herangezogen werden, um dessen Erfahrung bei der Erlangung von Zertifizierungen von COTS-Komponenten zu belegen.

### 2.1.11 AMC 20-152A

Das Dokument AMC 20-152A „Development Assurance for Airborne Electronic Hardware” /EAS 21/ der Europäischen Agentur für Flugsicherheit (EASA) ist ein Leitfaden, um die Einhaltung der geltenden Lufttüchtigkeitsvorschriften für elektronische Hardware von Bordsystemen und Ausrüstungen bei der Produktzertifizierung oder Zulassung nachzuweisen. Dabei werden digitale kundenspezifische Produkte behandelt, die in die Kategorien einfach oder komplex eingestuft werden. Es werden Leitlinien zur Entwicklung komplexer und einfacher kundenspezifischer Produkte vorgestellt. Einzelne Abschnitte dieses Leitfadens befassen sich mit der Verwendung von COTS-Komponenten.

Ein Unterkapitel von /EAS 21/ befasst sich mit COTS-IP (IP – intellectual property, geistiges Eigentum). Hierunter sind kommerzielle, handelsübliche Entwurfsfunktionen (z. B. Entwurfsmodule oder Funktionsblöcke, Bibliotheken) zu verstehen, die für den Entwurf und die Implementierung kundenspezifischer Produkte verwendet werden. Bei COTS-IP handelt es sich also um kommerziell verfügbare Funktionen, die von einer Reihe verschiedener Nutzer in einer Vielzahl von Anwendungen verwendet werden. In /EAS 21/ wird gefordert, dass ein Sicherheitskonzept bei der Entwicklung von COTS-IP vorhanden

sein muss, welches auf den ermittelten Ausfallrisiken aufgrund eines Entwurfsfehlers im COTS-IP selbst oder eines Fehlers in dessen Verwendung basieren sollte. Dabei sollten Aspekte wie die Auswahl der COTS-IP, die Bewertung des Herstellers, die Definition der Anforderungen oder die Entwurfsintegration, Implementierung und Verifizierung berücksichtigt werden.

Hinsichtlich der Auswahl von COTS-IP wird in /EAS 21/ erwähnt, dass COTS-IP in verschiedenen Formen/Quellformaten und verschiedenen Qualitätsstufen verfügbar sein können, von denen einige möglicherweise nicht zur Verwendung geeignet sind. Daher sind wesentliche Merkmale von COTS-IP nachzuweisen, die als Mindestvoraussetzung für deren Verwendung angesehen werden. Es ist beispielsweise nachzuweisen, dass der COTS-IP technisch geeignet ist, die vorgesehene Funktion zu erfüllen. Außerdem muss die Beschreibung der Architektur des COTS-IP ein Verständnis der Funktionalität, der Modi und der Konfiguration vermitteln. Die Qualität der Daten und der Dokumentation ermöglichen das Verständnis aller Aspekte der Funktionalität, Modi und des Verhaltens und ermöglichen die Integration und Verifizierung der COTS-IP.

Der Hersteller der COTS-IP muss laut /EAS 21/ ebenfalls bewertet werden. Dabei ist sicherzustellen, dass der Hersteller alle Informationen zur Verfügung stellt, die für die Integration der COTS-IP und zur Unterstützung der Implementierung erforderlich sind. Außerdem sind Dokumentationen der Konfigurationen, auswählbaren Optionen und skalierbaren Module des COTS-IP-Designs bereitzustellen, damit die Implementierung ordnungsgemäß verwaltet werden kann. Es ist sicherzustellen, dass der COTS-IP nach einem vertrauenswürdigen und zuverlässigen Verfahren geprüft wurde, wobei die Prüfung sich auf den spezifischen Anwendungsfall erstrecken muss. Bekannte Fehler und Einschränkungen müssen dem Endnutzer zur Verfügung gestellt werden und es muss ein Verfahren geben, um die Informationen bezüglich Fehler und Einschränkungen aktuell zu halten und die aktualisierten Informationen bereitzustellen. Es müssen Daten aus der Betriebserfahrung der COTS-IP vorhanden sein, die einen zuverlässigen Betrieb für den spezifischen Anwendungsfall belegen.

Laut /EAS 21/ sollte im Hardware-Verifizierungsplan oder einem damit zusammenhängenden Planungsdokument eine Strategie zur Verifizierung der COTS-IP beschrieben werden. Die Strategie zur Verifizierung der COTS-IP sollte sicherstellen, dass der COTS-IP die ihm zugewiesenen Funktion erfüllt und dass keine Designfehler entstanden sind, dass der COTS-IP ordnungsgemäß angeschlossen und konfiguriert wurde und dass zuverlässige und vertrauenswürdige Testdaten, Testfälle oder Verfahren des Herstellers

als Teil der Verifizierung verwendet wurden. Basieren die Funktionen der COTS-IP auf einer Industrienorm, können bewährte standardisierte Tests, die die Einhaltung der Norm überprüfen, bei der Verifizierung verwendet werden.

Ein weiteres Unterkapitel von /EAS 21/ befasst sich mit dem Einsatz von elektronischen COTS-Komponenten in Bordsystemen und Ausrüstungen von Flugzeugen. Ein wichtiger Punkt dabei ist laut /EAS 21/ die Betrachtung der Komplexität der COTS-Komponenten. Zur Bestimmung, wie komplex COTS-Komponenten sind, sollten diverse Kriterien herangezogen werden, wobei alle Funktionen der Komponenten einschließlich der nicht genutzten zu betrachten sind. Werden COTS-Komponenten als komplex bewertet, ist es praktisch nicht möglich, alle möglichen Konfigurationen der Komponenten vollständig zu prüfen und es ist schwierig, alle potentiellen Fehler zu erkennen. COTS-Komponenten gelten laut /EAS 21/ als komplex, wenn sie mehrere funktionale Elemente haben, die miteinander agieren können, eine beträchtliche Anzahl von Funktionsmodi bieten und eine Konfigurierbarkeit der Funktionen bieten, die unterschiedliche Daten-/Signalflüsse und eine unterschiedliche gemeinsame Nutzung von Ressourcen ermöglichen. Zudem gelten COTS-Komponenten als komplex, wenn sie fortgeschrittene Datenverarbeitung, fortgeschrittene Schaltungen oder mehrere Verarbeitungselemente (z. B. Mehrkernprozessoren, Grafikverarbeitung, Vernetzung, komplexe Busumschaltung, usw.) enthalten. Bei der Auswahl komplexer COTS-Komponenten sollte die Ausgereiftheit der Komponenten berücksichtigt werden. Bei Feststellung von Risiken sind diese in angemessener Weise zu mindern.

Hinsichtlich der Verwendung komplexer COTS-Komponenten wird in /EAS 21/ ausgesagt, dass diese mehrere Funktionen und viele Konfigurationen dieser Funktionen aufweisen können. Die Konfiguration dieser Komponenten sollte so verwaltet werden, dass die erforderlichen Einstellungen konsistent angewendet werden können, die Konfiguration auf einer anderen Komponente repliziert werden kann und die Konfiguration kontrolliert geändert werden kann, wenn eine Änderung erforderlich ist. Die Dokumentation zur Konfiguration muss mindestens die verwendeten Funktionen, die nicht verwendeten Funktionen und die Mittel, die zu ihrer Deaktivierung verwendet werden, die Mittel zur Kontrolle einer versehentlichen Aktivierung der nicht verwendeten Funktionen oder einer versehentlichen Deaktivierung verwendeter Funktionen, die Mittel zu Verwaltung von Resets, die Konfiguration beim Einschalten, die Taktkonfiguration sowie die Betriebsbedingungen (z. B. Taktfrequenz, Stromversorgung, Temperatur) umfassen.

Die Zuverlässigkeit der COTS-Komponenten ist laut /EAS 21/ vom Hersteller im Rahmen des Qualifizierungsprozesses festzustellen. Die Auswahl der Komponenten erfolgt auf Grundlage ihrer technischen Eignung für die vorgesehene Zielanwendung. Ist es erforderlich, dass die COTS-Komponenten außerhalb der vom Hersteller garantierten Betriebsbedingungen verwendet werden, ist die Zuverlässigkeit und technische Eignung der Komponenten für die vorgesehene Anwendung nachzuweisen.

Der Endnutzer sollte laut /EAS 21/ sicherstellen, dass die Verwendung der COTS-Komponenten entsprechend der vorgesehenen Funktion definiert und überprüft wurde. Dies gilt auch für die Schnittstelle zwischen Hard- und Software. Es sollte nachgewiesen werden, dass die nicht genutzten Funktionen der COTS-Komponenten die Integrität und Verfügbarkeit der genutzten Funktionen nicht beeinträchtigen. Für nicht genutzte Funktionen wird empfohlen, ein wirksames Mittel zur Deaktivierung zu verwenden und zu überprüfen. Für kritische Konfigurationseinstellungen (Einstellungen, die für die ordnungsgemäße Nutzung notwendig sind und die, bei versehentlicher Änderung, das Verhalten der COTS-Komponenten so beeinflussen können, dass die vorgesehene Funktion nicht mehr erfüllt wird) sind geeignete Abhilfemaßnahmen für den Fall einer versehentlichen Änderung festzulegen.

### 2.1.12 COTS security issues and approaches

Das Dokument “Commercial off the Shelf (COTS) security issues and approaches” /DOA 06/ beschäftigt sich mit der Sicherheit von COTS-Komponenten beim Einsatz in militärischen Systemen in den USA. Aufgrund der hohen Kosten und langwierigen Entwicklungszeiten von kundenspezifischen Komponenten werden auch in militärischen Anwendungen immer häufiger kommerzielle Komponenten eingesetzt. Neben Vorteilen z. B. hinsichtlich aktueller Technologie und Entwicklungszeiten bringen COTS-Komponenten aber auch für militärische Systeme Nachteile mit sich, wobei eines der größten Probleme laut /DOA 06/ die Sicherheit von COTS-Komponenten ist. Daher werden in /DOA 06/ Ansätze zur Identifizierung von Sicherheitslücken analysiert und Empfehlungen zu deren Minimierung gegeben. Dabei befasst sich /DOA 06/ ausschließlich mit softwarebasierten COTS-Komponenten.

Die Software in COTS-Komponenten hat laut /DOA 06/ oftmals einen Quellcode in Form einer „Black Box“. Außerdem hat sie meist einen großen Funktionsumfang und ist sehr komplex und es gibt regelmäßig neue Releases mit neu hinzugefügten Funktionen, Fehlerkorrekturen oder Upgrades. Die Software von COTS-Komponenten ist im Allgemeinen

so konzipiert, dass sie nicht mit anderen COTS-Komponenten kompatibel ist. Daraus ergeben sich laut /DOA 06/ vor allem Probleme hinsichtlich der Sicherheit von COTS-Komponenten. Da die Software von COTS-Komponenten häufig relativ groß und komplex ist, sind Programmierfehler schwerer zu detektieren, was zu Sicherheitslücken führen kann. Daher sind laut /DOA 06/ Anforderungen an die Sicherheit der Software von COTS-Komponenten zu stellen. Beispielsweise müssen alle Systeme ein angemessenes Niveau an Vertraulichkeit, Integrität, Authentifizierung, Nachweisbarkeit und Verfügbarkeit aufrechterhalten. Systeme sind daher entsprechend der Klassifizierung oder Sensibilität der über das System übertragenen Informationen zu schützen.

In /DOA 06/ werden mehrere Ansätze zur Lösung der Sicherheitsprobleme der Software von COTS-Komponenten genannt. Eine Möglichkeit ist der Gebrauch von Software-Wrappern. Ein Software-Wrapper ist als Hülle oder Gehäuse zu betrachten, welches eine Komponente von anderen Komponenten und ihrer Verarbeitungsumgebung isoliert. Zur Steigerung der Sicherheit bietet ein Wrapper die notwendigen Transformationen und Filterungen der ein- und ausgehenden Daten. Er verhindert das Eindringen unerwünschter Informationen in die COTS-Komponenten, indem er eine Softwarebarriere um die Komponenten aufbaut. Er kontrolliert auch die Ausgaben der Komponenten. Der Nachteil von Wrappern ist, dass sie nicht vor Ereignissen schützen können, die von den Entwicklern nicht vorhergesehen wurden. Eine weitere Möglichkeit ist der Einsatz von COTS-Komponenten, die bereits für die erforderliche Sicherheitskategorie zertifiziert sind. Zur Zertifizierung reicht der Hersteller die Produktdokumentation und die COTS-Komponenten bei einer zur Zertifizierung berechtigten Zertifizierungsstelle ein. In der Zertifizierungsstelle wird ein Prozess zur Bewertung, Prüfung und Validierung der COTS-Komponenten durchlaufen und anschließend ein Bericht dazu erstellt. Erfüllen die Komponenten alle Kriterien für die gewünschte Sicherheitskategorie, wird die Zertifizierung ausgestellt. Kommt es zu Aktualisierungen der Software der COTS-Komponenten, muss entweder der aktualisierte Teil oder die gesamte Software einer neuen Zertifizierung unterzogen werden. Eine weitere Möglichkeit ist der Einsatz von softwarebasierten COTS-Komponenten und eine interne Zertifizierung. Bei dem Ansatz der internen Zertifizierung werden COTS-Komponenten beschafft, die den Anforderungen am besten entsprechen. Diese werden dann gemäß der geforderten Sicherheitskategorie zertifiziert. Dabei ist nicht der Hersteller, sondern der Endnutzer verantwortlich für die Einhaltung der Sicherheitsanforderungen und das Zertifizierungsverfahren. Bei der internen Zertifizierung kann laut /DOA 06/ beispielsweise ein Black-Box-Test der COTS-Komponenten erfol-

gen, wobei die zu testenden Komponenten als „Black Box“ behandelt und ihre Funktionalitäten getestet werden. Die Software wird dabei ohne jegliche Analyse des Quellcodes getestet und die Tester müssen keine Kenntnisse über die Software haben. Es wird lediglich getestet, ob die Software funktionsfähig ist, indem Signale an den Eingängen angelegt werden und getestet wird, was an den Ausgängen ausgegeben wird. Die Verwendung eines Black-Box-Tests allein zur Zertifizierung der Komponenten ist aufgrund der Beschränkung der Testfälle unzureichend. Ein Prüfer ist möglicherweise nicht in der Lage, alle Fälle zu testen oder alle Testfälle zu erstellen, in denen die zu testenden Komponenten versagen könnten. Eine weitere Methode bei der internen Zertifizierung ist die Fehlerinjektion. Diese Methode kann verwendet werden, um Schwachstellen der Software zu finden. Das Hauptziel besteht darin, Fehler in die Software einzubringen, um deren Sicherheitstoleranz zu testen. Dabei können diverse Methoden zur Fehlerinjektion angewandt werden, wie beispielswiese Pre-Execution-Fehlerinjektion (Einfügen eines Fehlers vor der Ausführung der Anwendung), Execution-Fehlerinjektion (Einfügen eines Fehlers bei Ausführung der Anwendung) oder eine Kombination aus den beiden genannten Methoden.

In /DOA 06/ werden auch Empfehlungen hinsichtlich der Beschaffung von COTS-Komponenten gegeben. Es wird empfohlen, dass die Sicherheitsanforderungen an COTS-Komponenten klar zu definieren sind. Dazu ist ein Dokument zu erstellen, in dem alle Sicherheitsanforderungen und -ziele klar und vollständig aufgeführt sind. Außerdem muss eine Methode zur Auswahl von COTS-Komponenten festgelegt werden. Empfohlen wird der Kauf von zertifizierten COTS-Komponenten und zusätzlich die Verwendung der Fehlerinjektion, da auch bereits zertifizierte COTS-Komponenten noch Fehler aufweisen können. Die Verwendung der Fehlerinjektion kann dabei helfen, Sicherheitslücken zu minimieren und erhöht das Vertrauen in die COTS-Komponenten. Des Weiteren sollte sorgfältig geprüft werden, ob die Sicherheitsanforderungen der Software der COTS-Komponenten der Zielanwendung entsprechen. Sind die COTS-Komponenten bereits zertifiziert, bedeutet dies laut /DOA 06/ nicht, dass die Komponenten für den spezifischen Einsatz geeignet sind. Die Zertifizierung sollte in der Umgebung erfolgen, in der die Komponenten später eingesetzt werden sollen.

Hinsichtlich eines Qualifizierungsprozesses für COTS-Komponenten wird in /DOA 06/ ausgesagt, dass dieser sich aus vier Phasen zusammensetzt, wobei jeder Phase spezifische Aufgaben und Dokumentationen zugewiesen sind, die abgeschlossen werden müssen, um die Phase zu beenden und in die nächste Phase überzugehen. Die erste

Phase ist die Definition. Hierunter fällt das Verstehen von Auftrag, Umgebung und Architektur, um das Niveau der Sicherheitsanforderungen zu bestimmen. Es sind Informationen über das Zielsystem und seine Umgebung zu sammeln sowie Sicherheitsanforderungen, Aufwand, Zeitplan und Ressourcen zu vereinbaren. In der zweiten Phase, der Prüfung, ist die Übereinstimmung der Zielsystems mit dem festgelegten Prozess zu überprüfen. Außerdem erfolgt eine Überprüfung des Zielsystems mit den in der vorherigen Phase vereinbarten Informationen sowie eine Identifizierung und Analyse von Schwachstellen und eine Überprüfung, ob geeignete Sicherheitskontrollen vorhanden sind. In der dritten Phase sind Tests zur Validierung durchzuführen, um sicherzustellen, dass die Sicherheitskontrollen des Zielsystems den Anforderungen entsprechen. Außerdem sind der Genehmigungsbehörde Nachweise zu deren Unterstützung zu erbringen, damit diese eine Entscheidung über die Erteilung einer Genehmigung treffen kann. Die letzte Phase dient der Aufrechterhaltung der Sicherheit, da auch nach der Qualifizierung die Aufrechterhaltung der Sicherheit zu gewährleisten ist. Dies erfolgt beispielsweise durch eine Meldung und Analyse von Veränderungen an den COTS-Komponenten. Es ist sicherzustellen, dass selbst bei Bedrohungen das Restrisiko akzeptabel bleibt. Die Durchführung regelmäßiger Überprüfungen von Sicherheitsmanagement und Konfigurationsmanagement ist erforderlich.

Für die Hersteller von COTS-Komponenten wird in /DOA 06/ empfohlen, dass diese Methoden wie beispielsweise Qualitätskontrollen und Managementprozesse haben sollten, um Sicherheitsanforderungen des Endkunden zu erfüllen und ihre Produkte vor Sicherheitsbedrohungen zu schützen.

### 2.1.13 Joint Software Systems Safety Engineering Handbook

Das “Joint Software Systems Safety Engineering Handbook” /DOD 10/ wurde in Zusammenarbeit von der Armee, der Küstenwache, der Luftfahrtbehörde (Federal Aviation Administration, FAA), der Raumfahrtbehörde (National Aeronautics and Space Administration, NASA) sowie der Verteidigungsindustrie und wissenschaftlichen Institutionen in den USA entwickelt. Generell befasst sich /DOD 10/ mit der Sicherheit von Softwaresystemen, wobei der Zweck darin besteht, Management- und Entwicklungsrichtlinien bereitzustellen, um ein angemessenes Maß an Sicherheit zu erreichen, damit Software im Zielsystem mit einem akzeptablen Sicherheitsrisiko ausgeführt wird. In einzelnen Abschnitten von /DOD 10/ wird auf den Einsatz von COTS-Komponenten eingegangen.

In /DOD 10/ werden generelle Überlegungen hinsichtlich des Einsatzes von COTS-Komponenten angesprochen. Dabei wird erwähnt, dass Hersteller von COTS-Komponenten in der Regel in diesen Komponenten keine Software einsetzen, die speziell zur Anwendung in sicherheitsrelevanten Systemen entwickelt wurde und dass die Software häufig nicht angemessen dokumentiert ist und vom Hersteller oftmals kein Quellcode zur Verfügung gestellt wird. Daher müssen COTS-Komponenten laut /DOD 10/ unter Berücksichtigung der Sicherheitskategorie des Zielsystems eingehend analysiert und getestet werden. Gerade im Hinblick auf die kurze Lebensdauer von COTS-Komponenten und die schnelle Einführung neuer Komponenten ist es wichtig, dass jede Änderung analysiert und bei Bedarf getestet wird. Bei der Bewertung der Sicherheit von COTS-Komponenten ist sicherzustellen, dass alle Sicherheitsrisiken, die sich aus der Verwendung der COTS-Komponenten ergeben können, identifiziert und dokumentiert werden.

Ist der Einsatz von COTS-Komponenten geplant, sind laut /DOD 10/ alle Vor- und Nachteile zu ermitteln und sorgfältig gegen die Anforderungen des Zielsystems und sicherheitskritische Fragestellungen abzuwägen. Potentielle Vorteile von COTS-Komponenten sind beispielsweise Kosteneinsparungen aufgrund geringerer Entwicklungskosten, die schnelle Einführung neuer Technologien, eine möglicherweise breite Benutzerbasis sowie möglicherweise eine technische Unterstützung durch den Hersteller. Mögliche Nachteile von COTS-Komponenten sind begrenzte Entwicklungs-, Test- und Konfigurationsdokumentationen, die Nichtverfügbarkeit von Konstruktions- und Testdaten, unbekannte oder unnötige Funktionalitäten, eine eingeschränkte oder fehlende Unterstützung des Herstellers, die Nichtverfügbarkeit von Sicherheitsanalysen sowie der potentielle Bedarf an regelmäßigen Aktualisierungen mit unbekannten Auswirkungen. Aufgrund der Kosten für die Durchführung einer vollständigen Bewertung der COTS-Komponenten ist laut /DOD 10/ die Verwendung von COTS-Komponenten nicht zwangsläufig der günstigste Ansatz, auch wenn die Beschaffung solcher Komponenten die günstigste Alternative zu sein scheint.

In /DOD 10/ werden Empfehlungen hinsichtlich Kriterien gegeben, die bei der Auswahl geeigneter COTS-Komponenten berücksichtigt werden sollten. Dabei werden die drei Kriterien „Vertrauen“, „Einfluss“ und „Komplexität“ betrachtet. Unter „Vertrauen“ ist das Erlangen der Gewissheit zu verstehen, dass die COTS-Komponenten ihre vorgesehenen Funktionen in der vorgesehenen Betriebsumgebung im vorgesehenen System erfüllen werden. Dazu ist eine Bewertung der COTS-Komponenten durchzuführen, die

auch die Entwicklungsgeschichte und Betriebshistorie der COTS-Komponenten einbezieht. Wichtig dabei sind laut /DOD 10/ die Unterstützung durch den Hersteller (z. B. Bereitstellung von Handbüchern, Schulungen, Änderungsmitteilungen, Konfigurationsmanagement, Quellcode der Software) und die Zugänglichkeit der Dokumentation (z. B. Konstruktionsdokumente, Sicherheitsanalysen, Testverfahren und -ergebnisse, Betriebshistorie). Unter dem Kriterium „Einfluss“ ist laut /DOD 10/ der Einfluss der COTS-Komponenten auf das Zielsystem zu verstehen. Dieser Einfluss, insbesondere sicherheitstechnisch wichtige Auswirkungen, ist zu bewerten, wobei unerwünschte Ereignisse, Gefahren und ursächliche Faktoren, die zu solchen Ereignissen führen können, zu ermitteln sind. Zur Bewertung des Kriteriums „Einfluss“ ist eine Gefahrenanalyse durchzuführen, deren Ergebnis eine Liste der sicherheitsrelevanten Funktionen, welche die COTS-Komponenten im Zielsystem ausführen sollen, sowie eine Liste der Sicherheitsanforderungen ist. Alle sicherheitsrelevanten Funktionen sind hinsichtlich ihrer Auswirkungen auf das System im Falle eines Ausfalls der COTS-Komponenten zu bewerten. Das Kriterium „Komplexität“ erfasst laut /DOD 10/ die Komplexität der COTS-Komponenten, wobei Attribute wie z. B. die Anzahl der Software-Codezeilen und die Anzahl der sicherheitsrelevanten Funktionen zu berücksichtigen sind. Ein weiterer Punkt hinsichtlich des Kriteriums „Komplexität“ ist die Betrachtung der Möglichkeit zur Modifizierung der COTS-Komponenten.

Des Weiteren werden in /DOD 10/ Möglichkeiten dargestellt, dass mit der Verwendung von COTS-Komponenten in sicherheitsrelevanten Systemen verbundene Risko zu minimieren. Durch ihr spezielles Design kann die Anwendungssoftware für alle Eventualitäten entwickelt werden, was jedoch sehr schwierig ist, insbesondere wenn nicht der volle Funktionsumfang der COTS-Software bekannt ist. Es wären alle ursächlichen Faktoren für unerwünschte Ereignisse zu ermitteln und sicherzustellen, dass die Anwendungssoftware sicher auf diese reagiert. Middleware (Zwischenschicht, anwendungsneutrales Programm zur Übermittlung von Daten zwischen verschiedenen Komponenten) oder Wrapper bieten die Möglichkeit, den Einfluss der COTS-Komponenten auf sicherheitsrelevante Funktionen des Systems zu reduzieren, indem die COTS-Software von sicherheitsrelevanten Funktionen isoliert wird. Eine Möglichkeit zur Isolierung sicherheitsrelevanter Daten von COTS-Software besteht darin, alle Kommunikations- und Datenübertragungen in robuster Weise zu verpacken. Dies kann z. B. durch die Festlegung eines Kommunikationsprotokolls erfolgen, welches eine eindeutige Identifizierung des Nachrichtentyps und eine Validierung des korrekten Empfangs der Datenübertragung ermöglicht. Durch Einbettung und Ausnahme von Interrupt-Behandlungen in der

Anwendungssoftware wird sichergestellt, dass die Anwendungssoftware die Kontrolle über das System behält. Die Methode der Analyse der COTS-Software kann dann erfolgen, wenn detaillierte Entwicklungsunterlagen verfügbar sind. Diese Analyse bietet die größte Sicherheit, dass das gesamte Softwarepaket sicher ausgeführt werden kann. Es können gezielte Tests entwickelt werden, um festzustellen, ob identifizierte ursächliche Faktoren für unerwünschte Ereignisse tatsächlich zu einem unerwünschten Zustand führen können. Die Beseitigung unnötiger Funktionen verringert das Risiko, dass diese Funktionen sicherheitsrelevante Funktionen der Anwendungssoftware beeinträchtigen. Durch den Einsatz von Watchdog-Timern werden Prozessoren daran gehindert, in Schleifen einzutreten, die unendlich lange dauern oder die Verarbeitung wird beendet, wenn diese länger als erwartet dauert. Ähnliche Timer können für sicherheitsrelevante Zeitvorgaben verwendet werden, wobei darauf zu achten ist, dass sicherheitskritische Ausgänge und externe Komponenten beim Auslösen solch eines Timers in einen sicheren Zustand zurückzuführen sind. Außerdem sollte der Endkunde die Kontrolle über die Konfiguration der COTS-Komponenten erhalten, was Vereinbarungen zwischen Hersteller und Endkunden erforderlich machen kann. Hersteller müssen bereit sein, Änderungen an den COTS-Komponenten allen Kunden mitzuteilen. Prüfungen können helfen, dass mit der Verwendung von COTS-Komponenten in sicherheitsrelevanten Systemen verbundene Risiko zu bewerten. Da in den meisten Fällen nicht alle möglichen Pfade, Bedingungen, Timing- und Datenprobleme untersucht werden können und nicht alle möglichen Fehlerzustände erzeugt werden können, sind gezielte Prüfungen zu entwickeln, die sich auf die sicherheitsrelevanten Aspekte der Interaktion zwischen COTS-Software und Anwendungssoftware konzentrieren.

Zudem wird in /DOD 10/ erwähnt, dass bei der Verwendung von COTS-Komponenten Sicherheitsnachweise für diese Komponenten zu erstellen sind. Dabei ist das Sicherheitsrisiko beim Einsatz der COTS-Komponenten zu bewerten und es wird eine Empfehlung für die Annahme, Ablehnung, weitere Bewertung (z. B. Test oder Analyse) oder Änderung der COTS-Komponenten gegeben. Die Entscheidung soll sich auf mehrere Faktoren stützen, wie z. B. die sicherheitstechnische Einstufung der Funktionen der COTS-Komponenten, den Umfang und die Qualität der verfügbaren Entwicklungs- und Testdaten, den möglichen Beitrag der COTS-Komponenten zu Systemfehlern, Gefahren und Ausfallarten, die Erfüllung der Sicherheitsanforderungen durch die COTS-Komponenten sowie die Erfüllung der Anforderungen an Integrations- und Qualifikationstests der COTS-Komponenten.

### 2.1.14 Space product assurance – Commercial EEE components

Das Dokument “Space product assurance – Commercial electrical, electronic and electromechanical (EEE) components” /ESA 13/ ist ein Standard der Europäischen Weltraumorganisation ESA, in dem Anforderungen an kommerzielle elektrische, elektronische oder elektromechanische Komponenten aufgestellt werden. Das Ziel der Anforderungen an Auswahl, Kontrolle, Beschaffung und Verwendung dieser Komponenten ist es, sicherzustellen, dass bei einem Raumfahrtprojekt auch bei Verwendung von COTS-Komponenten die Missionsanforderungen erfüllt werden. Es werden u. a. Anforderungen hinsichtlich Auswahl, Bewertung und Genehmigung der Komponenten, Beschaffung, Handhabung und Lagerung, Qualitätssicherung und Dokumentation aufgestellt. Relevante Anforderungen aus /ESA 13/ werden nachfolgend zusammengefasst. Dazu ist zu sagen, dass sich /ESA 13/ in vielen Teilen auf ein anderes ESA-Dokument (ECSS-Q-ST-60C) bezieht und dieses ergänzt bzw. Änderungen zu diesem aufzeigt für den Fall, dass COTS-Komponenten eingesetzt werden. Da das Dokument ECSS-Q-ST-60C der GRS nicht vorliegt, werden im Rahmen dieses Vorhabens nur die Änderungen zu diesem Dokument durch die Verwendung kommerzieller Komponenten, die in /ESA 13/ beschrieben werden, betrachtet.

In /ESA 13/ wird zwischen drei Klassen von Komponenten unterschieden, wobei die drei Klassen drei Stufen der Abwägung zwischen Sicherheit und Risiko bieten. Anhand der Projektziele, -definitionen und -beschränkungen wird bestimmt, welche Klasse von Komponenten für eine Weltraummission verwendet werden darf. Entsprechend ihrer Klasse werden in /ESA 13/ unterschiedliche Anforderungen an COTS-Komponenten gestellt. Die drei Klassen sind:

- Klasse 1: höchste Sicherheit, geringstes Risiko
- Klasse 2: mittlere Sicherheit, mittleres Risiko
- Klasse 3: geringste Sicherheit, höchstes Risiko

Hinsichtlich der Bewertung von COTS-Komponenten der Klassen 1 und 2 muss der Hersteller laut /ESA 13/ alle verfügbaren Daten über die Komponenten bereitstellen. Die Herstellerdokumentation ist auf Vollständigkeit in Bezug auf die Kennzeichnung der Komponenten sowie die mechanische, elektrische und thermische Beschreibung zu prüfen. Zur Evaluierung der COTS-Komponenten sind diverse Tests durchzuführen. Diese umfassen eine Konstruktionsanalyse, eine elektrische Charakterisierung, elektrische

Tests bei unterschiedlichen Temperaturen, Dichtheitsprüfungen, visuelle Untersuchungen, Untersuchung der Auswirkung mechanischer Vibrationen, Untersuchung der Auswirkungen von Beschleunigungen, Langzeittests, Tests mittels akustischer Rastermikroskopie (Scanning Acoustic Microscopy – SAM, bildgebendes Verfahren zur Qualitätskontrolle, Inspektion und Fehleranalyse mikroelektronischer Komponenten und Materialien) sowie eine Bewertung der Auswirkungen von Strahlung. Der Verzicht auf eine der Prüfungen oder die Einführung alternativer Aktivitäten ist zu begründen. Die Ergebnisse der Komponentenevaluierung sind vom Hersteller dahingehend zu prüfen, wie sie sich auf den Inhalt der Losannahmeprüfungen auswirken. Außerdem sind die Ergebnisse der Komponentenevaluierung durch ein geeignetes Verfahren zu dokumentieren.

Bei COTS-Komponenten der Klasse 3 ist hinsichtlich der Bewertung der Komponenten der Hersteller ebenfalls verpflichtet, alle verfügbaren Daten über die Komponenten bereitzustellen. Die Herstellerdokumentation ist auf Vollständigkeit in Bezug auf die Kennzeichnung der Komponenten sowie die mechanische, elektrische und thermische Beschreibung zu prüfen. Zur Evaluierung der COTS-Komponenten sind ebenfalls Tests durchzuführen, diese umfassen allerdings nur eine Konstruktionsanalyse sowie eine Bewertung der Auswirkungen von Strahlung. Der Verzicht auf einen der Tests oder die Einführung alternativer Aktivitäten ist zu begründen. Die Ergebnisse der Komponentenevaluierung sind vom Hersteller dahingehend zu prüfen, wie sie sich auf den Inhalt der Losannahmeprüfungen auswirken. Außerdem sind die Ergebnisse der Komponentenevaluierung durch ein geeignetes Verfahren zu dokumentieren.

Hinsichtlich der Beschaffung von COTS-Komponenten der Klassen 1, 2 und 3 wird in /ESA 13/ empfohlen, dass die Komponenten mittels einem vom Hersteller zugewiesenen Rückverfolgungscodes, der über die gesamte Lieferkette unverändert beibehalten werden muss, rückverfolgbar sein müssen. In einer Losannahmeprüfung sind für Komponenten der Klassen 1 und 2 diverse Prüfungen, wie z. B. eine Konstruktionsanalyse, eine elektrische Charakterisierung, elektrische Tests bei unterschiedlichen Temperaturen, Dichtheitsprüfungen, visuelle Untersuchungen, Untersuchung der Auswirkung mechanischer Vibrationen, Untersuchung der Auswirkungen von Beschleunigungen, Langzeittests, Tests mittels akustischer Rastermikroskopie sowie eine Bewertung der Auswirkungen von Strahlung, durchzuführen. Für Komponenten der Klasse 3 ist nur eine Konstruktionsanalyse sowie eine Bewertung der Auswirkungen von Strahlung durchzu-

führen, die anderen Prüfungen können bei Vorhandensein repräsentativer Daten entfallen. Der Verzicht auf eine der Prüfungen oder die Einführung alternativer Prüfungen ist zu begründen.

Hinsichtlich der Qualitätssicherung für COTS-Komponenten der Klassen 1, 2 und 3 wird in /ESA 13/ ausgesagt, dass die Rückverfolgbarkeit von Komponenten auch während und nach dem Einbau sicherzustellen ist. Alle Ergebnisse der durchgeführten Inspektionen oder Kontrollen für COTS-Komponenten der Klassen 1, 2 und 3 sind laut /ESA 13/ zu dokumentieren.

## 2.2 Vorgehensweise in anderen Ländern

Im Rahmen der Arbeiten von Arbeitspaket 1 wurde nach internationalen Vorgehensweisen hinsichtlich des Einsatzes von COTS-Komponenten in elektro- und leittechnischen Einrichtungen in kerntechnischen Anlagen recherchiert. Dazu wurde anhand diverser Informationsquellen (z. B. vorliegende Dokumente, internationale Kontakte, Internetrecherche) nach Vorgehensweisen und Methoden zur Thematik des Einsatzes von COTS-Komponenten in elektro- und leittechnischen Einrichtungen in kerntechnischen Anlagen im Ausland gesucht. Bei dieser Recherche wurden Informationen aus 23 Ländern ermittelt, wobei der Detaillierungsgrad und die Menge der verfügbaren Informationen sich von Land zu Land stark unterschieden hat. Zudem konnte festgestellt werden, dass sich viele Länder nach der Vorgehensweise in den USA richten. Es wurden fünf Länder (Belgien, Finnland, Kanada, Vereinigtes Königreich, USA) ausgewählt, wobei die Auswahl der Länder auf Basis der zuvor gesammelten Unterlagen erfolgte. Die für diese fünf Länder vorliegenden Unterlagen wurden detailliert ausgewertet und die für das Vorhaben relevanten Inhalte wurden in Arbeitspaket 2 zur Entwicklung des Ansatzes zur Bewertung des Einsatzes von COTS-Komponenten verwendet. In den nachfolgenden Abschnitten werden die Vorgehensweisen dieser fünf Länder hinsichtlich des Einsatzes von COTS-Komponenten in elektro- und leittechnischen Einrichtungen in kerntechnischen Anlagen zusammengefasst.

### 2.2.1 Belgien

In Belgien wird hinsichtlich der Vorgehensweise zur Qualifizierung von kommerziellen Komponenten zwischen zwei Arten von COTS-Komponenten unterschieden:

- COTS-Komponenten, welche keine Software beinhalten

- COTS-Komponenten, welche Software beinhalten

Generell muss für alle Komponenten, also auch COTS-Komponenten, die keine Software enthalten, zumindest eine Qualifizierung bezüglich der Umgebungsbedingungen erfolgen. Dabei wird sichergestellt, dass die zu qualifizierenden Komponenten bei den in der Zielanwendung zu erwartenden Umgebungsbedingungen (z. B. Temperatur, Luftfeuchtigkeit, Erschütterungen) eingesetzt werden können. Je nach geplanter Anwendung der COTS-Komponenten kann die Durchführung des Verfahrens der Commercial Grade Dedication notwendig sein, wobei aus den vorliegenden Unterlagen nicht ersichtlich wird, wann ein solches Verfahren notwendig ist. Die Qualifizierung anhand der Commercial Grade Dedication basiert auf einer der möglichen US-amerikanischen Vorgehensweisen zur Qualifizierung von COTS-Komponenten, welche in Abschnitt 2.2.5 dieses Berichtes beschrieben wird. Je nach COTS-Komponenten und geplantem Einsatz können aus diversen Methoden eine oder mehrere ausgewählt werden, die bei der Qualifizierung zum Einsatz kommen. Dies können beispielsweise spezielle Tests und Inspektionen der COTS-Komponenten, eine leistungsbasierte Überprüfung des Herstellers der Komponenten, eine Prüfung der Herkunft der Komponenten zur Verifizierung des Herstellungsprozesses oder die Verwendung dokumentierter Aufzeichnungen der Betriebserfahrung der Komponenten sein. Das vorrangige Ziel der Qualifizierung der COTS-Komponenten ist die Feststellung, ob die COTS-Komponenten in der vorgesehenen Zielanwendung eingesetzt werden können und welche der verfügbaren Komponenten für die Verwendung am besten geeignet ist.

Bei COTS-Komponenten, die Software beinhalten, erfolgt die Qualifizierung anhand dem von der belgischen Behörde und der belgischen TSO Bel V entwickelten Leitfaden „Assessment of Pre-existing and Commercial-Off-The-Shelf Software For Use in Functions Important to Safety“ /BEL 13/. Auf dessen Basis muss der Betreiber einer kerntechnischen Anlage eigene Prozeduren und/oder Spezifikationen für die Qualifizierung der Software entwickeln. In diesem Leitfaden wird beschrieben, welche Nachweise und Informationen der Antragsteller für die Qualifizierung von COTS-Komponenten der Aufsichtsbehörde vorzulegen hat, wenn die verwendeten Komponenten Software beinhalten und zur Ausführung von sicherheitstechnisch wichtigen Funktionen in Kernkraftwerken eingesetzt werden sollen.

Hinsichtlich des Einsatzes von COTS-Komponenten werden in /BEL 13/ allgemeine Anforderungen aufgestellt, die durch softwarebasierte COTS-Komponenten mindestens erfüllt werden müssen. Eine Anforderung bezieht sich dabei auf die Komplexität der COTS-

Software. Es wird gefordert, dass die in der COTS-Software implementierte Funktionalität einfach und begrenzt sein muss. Dabei müssen die Funktionen eindeutig umschrieben und spezifiziert sowie für eine Verifikation und/oder eine Prüfung unter allen möglichen Betriebsarten geeignet sein. Durch diese Forderung wird der Einsatz von auf COTS-Software basierenden, komplexen Softwaresystemen (z. B. komplette Betriebssysteme, Mensch-Maschine-Schnittstellen, Prozesssteuerungssysteme) ausgeschlossen. Eine weitere allgemeine Anforderung in /BEL 13/ bezieht sich auf die Hard- und Softwareumgebung, in der die COTS-Software eingesetzt werden soll. Es wird gefordert, dass diese sowie die entsprechenden Schnittstellen spezifisch und eindeutig definiert werden müssen. Eine erfolgreiche Qualifizierung einer COTS-Software gilt ausschließlich für die Anwendung, Umgebung und Schnittstellen, für welche die Qualifizierung durchgeführt wurde. Des Weiteren wird allgemein gefordert, dass ein bei der Qualifizierung von softwarebasierten COTS-Komponenten berücksichtigter Erfahrungsrückfluss ausreichend, angemessen dokumentiert sowie für die geplante Nutzung geeignet sein muss.

Außerdem werden in /BEL 13/ diverse weitere Anforderungen aufgestellt, die bei der Qualifizierung von softwarebasierten COTS-Komponenten mindestens einzuhalten sind. Es sind alle sicherheitstechnisch wichtigen Funktionen zu bestimmen, die unter Verwendung von COTS-Software ausgeführt werden sollen und für jede dieser Funktionen ist die Bedeutung für die Sicherheit zu analysieren. In dieser Analyse müssen alle anormalen Hard- und Softwarezustände berücksichtigt werden (z. B. Speicherdefekte, Prozessordefekte, Ausfälle der Stromversorgung, Ausfälle der Software). Außerdem sind bei der Analyse jegliche anderen Ereignisse, welche die vorgesehenen Funktionen beeinträchtigen können, zu berücksichtigen. Für jede Funktion ist eine Sicherheitskategorie zu definieren.

Zudem wird in /BEL 13/ gefordert, dass die Software-Implementierung der sicherheitstechnisch wichtigen Funktionen, welche die COTS-Software ausführen soll, zu validieren ist. Bei der Validierung sind alle möglichen anormalen Betriebsbedingungen und Ereignisse sowie Selbsttests und Selbstdiagnosen des Systems zu berücksichtigen. Die Validierung kann sich auf vom Hersteller durchgeführte Tests stützen, welche durch ergänzende spezifische Tests erweitert werden können. Fehler, die mittels durchgeführter Tests oder anderweitiger Untersuchungen festgestellt werden, müssen aufgezeichnet,

analysiert und einer Prüfung unterzogen werden. Es sind Korrekturen oder Gegenmaßnahmen vorzunehmen, um die Fehler zu beseitigen. Diese Korrekturen oder Gegenmaßnahmen sind zu dokumentieren.

Laut /BEL 13/ sind die erforderlichen Leistungen (z. B. Reaktionszeit, Zykluszeit) der COTS-Software zu spezifizieren und deren Erfüllung zu überprüfen. Zudem ist nachzuweisen, dass die sicherheitstechnisch wichtigen Funktionen, die durch die COTS-Software ausgeführt werden sollen, in keiner Weise durch andere Funktionen der COTS-Komponenten oder des Systems beeinträchtigt werden können (z. B. durch Nebeneffekte von Interrupts, fehlerhafte Eingabedaten, unzureichende Nutzung oder Wartung). Es sind so viele Informationen wie möglich zu sammeln, welche Aufschluss über die Qualität der Softwareentwicklungs-, Verifikations- und Validierungsprozesse sowie der Dokumentation der Software-Anforderungsspezifikationen, des Codes und der durchgeführten Tests geben.

Eine weitere Anforderung aus /BEL 13/ ist, dass die Aufrechterhaltung der Integrität der Hard- und Softwarekonfiguration während der gesamten Lebensdauer der COTS-Komponenten zu gewährleisten ist. Dabei sind auch Fälle einzuschließen, bei denen Revisionen oder Modifikationen aufgrund von Fehlern erforderlich geworden sind. Außerdem ist die Betriebserfahrung zu dokumentieren, insbesondere die Historie von Fehlern und Software-Änderungen, frühere Betriebsprofile sowie Umgebungsbedingungen. Treten signifikante Diskrepanzen zwischen der bisherigen Nutzung der COTS-Software und der geplanten Anwendung auf, sind zumindest ergänzende Tests festzulegen, um diese zu entschärfen. Die Ergebnisse anderer Qualifizierungen oder Zertifizierungen, auch aus anderen Industriebereichen als der Kerntechnik, können bei der Qualifizierung einbezogen werden.

Weitere Anforderungen in /BEL 13/ befassen sich mit den Mindestvoraussetzungen, die erforderlich sind, um COTS-Komponenten erfolgreich zu qualifizieren. Es ist durch den Endnutzer nachzuweisen, dass die COTS-Komponenten in der Lage sind, die erforderlichen sicherheitstechnisch wichtigen Funktionen zu erfüllen. Auf Grundlage der gesammelten Informationen wird die Gültigkeit dieses Nachweises sowie die Eignung der COTS-Komponenten zur Erfüllung der sicherheitstechnisch wichtigen Funktionen von der Aufsichtsbehörde beurteilt. Ist ein Einsatz von COTS-Komponenten zur Ausführung von Funktionen der Kategorien B oder C geplant, besteht in gerechtfertigten Fällen die Möglichkeit, fehlende spezifische Nachweise durch den Rückfluss aus der Betriebserfahrung zu ersetzen.

Auf einem JRC-Meeting zum Thema „Commercial Grade Dedication“, welches im Jahr 2021 stattgefunden hat, wurde vom belgischen Vertreter im Vortrag /TRA 21/ ausgesagt, dass es beim Einsatz nicht nuklear qualifizierter Komponenten zu einem deutlich höheren Aufwand bei der Qualifizierung dieser Komponenten kommen kann und dass unter Umständen mehr Maßnahmen zur Überwachung der Komponenten implementiert werden müssen. Dies kann zur Folge haben, dass beim Einsatz von COTS-Komponenten mit der Maßgabe, ein vergleichbares Sicherheitsniveau wie bei der Nutzung nuklear qualifizierter Komponenten zu erlangen, die Gesamtkosten nicht gesenkt werden.

### 2.2.2 Finnland

In Finnland erfolgt die Qualifizierung von Komponenten zum Einsatz in elektro- und leittechnischen Systemen in kerntechnischen Anlagen nach der finnischen Norm YVL E.7 „Electrical and I&C equipment of a nuclear facility“ /STU 19/. Auch die Qualifizierung von COTS-Komponenten für den Einsatz in elektro- und leittechnischen Systemen soll anhand dieser Norm erfolgen, insbesondere wenn diese in Funktionen der finnischen Safety Classes 2 und 3 eingesetzt werden sollen, wobei die Norm nicht spezifisch für COTS-Komponenten ist. Basierend auf /STU 19/ sollte ein Plan zur Qualifizierung erstellt werden, der zumindest die bei der Qualifizierung berücksichtigten Normen, die durchgeführte Tests und Analysen während Design und Fertigung der Komponenten, die Organisationen, die bei Analysen zur Qualifizierung der Komponenten beteiligt sind, sowie den Rückfluss aus Betriebserfahrung enthält. Bei der Qualifizierung der Komponenten ist bereits zu berücksichtigen, in welcher Zielanwendung die Komponenten später eingesetzt werden sollen. Entsprechende Anforderungen, die sich aus dieser späteren Anwendung ergeben (z. B. Sicherheitsanforderungen, Umgebungsbedingungen) müssen bei der Qualifizierung berücksichtigt werden. Es ist nicht vorgesehen, eine Qualifizierung unabhängig von der späteren Anwendung durchzuführen, was aber gerade bei COTS-Komponenten, die später in diversen Anwendungen eingesetzt werden könnten, einen Vorteil hinsichtlich der Kosten der Qualifizierung liefern könnte. Einzelne Teile einer Qualifizierung können aber in Finnland bei anderen Anwendungen wiederverwendet werden. Treten bei der Qualifizierung von COTS-Komponenten Mängel in der Dokumentation oder der Umsetzung des Designprozesses auf, können diese Mängel durch zusätzliche Tests oder Analysen ausgeglichen werden.

Zur Entwicklung eines Prozesses speziell zur Qualifizierung von COTS-Komponenten zum Einsatz in sicherheitstechnisch wichtigen Systemen in nuklearen Einrichtungen

wurde in Finnland im Jahr 2018 das KELPO-Projekt aufgelegt, an dem eine Kooperation verschiedener finnischer Betreiber kerntechnischer Anlagen (Fortum, TVO, Fennovoima) mitgearbeitet hat. Die finnische Aufsichtsbehörde STUK fungierte als Beobachter in dem Projekt. Der Einsatz von COTS-Komponenten soll dabei ab der finnischen Safety Class 2 (entspricht im Prinzip der Kategorie A in Deutschland, die höchste Sicherheitsklasse wird in Finnland nur auf Betonstrukturen angewendet) erfolgen, wobei der Anteil an COTS-Komponenten in der Safety Class 2 eher gering vermutet wird. Hauptanwendungsgebiete für COTS-Komponenten werden die Safety Class 3 und nicht sicherheitstechnisch wichtige Funktionen sein. Im Rahmen des KELPO-Projektes wurden gemeinsame, generische Anforderungen entwickelt, die dann für alle Betreiber nuklearer Anlagen Gültigkeit haben. Somit sollte das Projekt ermöglichen, gemeinsame Prozeduren zwischen Betreibern, Herstellern und der Aufsichtsbehörde zu schaffen. Im Anschluss an das KELPO-Projekt wurde das Projekt unter dem Namen KELPO 2 mit dem Ziel weitergeführt, die im KELPO-Projekt begonnenen Entwicklungen weiter fortzuführen und den Informationsaustausch auf EU-Ebene auszuweiten. Im KELPO 2-Projekt wurde die Anwendung auch auf elektro- und leittechnische Komponenten ausgeweitet, während die erste Phase sich noch hauptsächlich mit mechanischen Komponenten befasst hat. Im Folgenden werden die für das Vorhaben relevanten Teile der Abschlussberichte des KELPO-Projektes /KEL 19/ und des KELPO 2-Projektes /KEL 20/ zusammengefasst.

Hintergrund der KELPO-Projekte war, dass Qualifizierungen von Systemen und Komponenten nach kerntechnischem Regelwerk oftmals aufwändig sind und daher immer weniger Hersteller diese Verfahren durchlaufen wollen, dass gleichzeitig aber die Qualitätsanforderungen in anderen Industriebereichen erheblich gestiegen sind und somit auch qualitativ hochwertige Systeme und Komponenten am Markt erhältlich sind, die nicht nach kerntechnischem Regelwerk qualifiziert wurden. Diese gestiegenen Qualitätsanforderungen anderer Industriebereiche kann sich laut /KEL 19/ die Nuklearindustrie zunutze machen, um ein umfassendes Zulieferernetz aufzubauen und so die Verfügbarkeit von Systemen und Komponenten für Modernisierungen oder Neubauten sicherzustellen.

Die Ziele der KELPO-Projekte waren laut /KEL 19/ und /KEL 20/ die Entwicklung eines vereinfachten Genehmigungs- und Qualifizierungsverfahrens für COTS-Komponenten zum Einsatz in kerntechnischen Anlagen in Finnland, die Analyse der Durchführbarkeit

des Einbringens von Komponenten in kerntechnische Anlagen, die nicht gemäß kerntechnischen Normen und Anforderungen hergestellt wurden, sowie die Analyse der Verfügbarkeit von Zuverlässigkeitsdaten zu solchen Komponenten. Mit den KELPO-Projekten sollten Wege gefunden werden, um den Nuklearsektor für Hersteller attraktiver zu machen und die Zusammenarbeit zwischen Betreibern kerntechnischer Anlagen und Komponentenherstellern zu verbessern.

Laut /KEL 19/ sollten sich behördliche Kontrollen/Inspektionen kerntechnischer Anlagen auf Bereiche konzentrieren, die für die nukleare Sicherheit wesentlich sind. Dabei sollten sich behördliche Kontrollen/Inspektionen auf Anlagen- und Systemebene und auf höhere Sicherheitsklassen konzentrieren. In den unteren Sicherheitsklassen könnten die Kontrollen/Inspektionen durch zugelassene Organisationen, interne Inspektionen des Betreibers oder andere unabhängige Bewertungen erfolgen. Hintergrund ist, dass sich der Großteil der behördlichen Kontrollen/Inspektionen auf die Komponentenebene der unteren Sicherheitsklassen konzentriert, da diese ein große Anzahl an Systemen enthalten. Allerdings sollte laut /KEL 19/ die behördliche Kontrolle dort ansetzen, wo die Grundlage für die Sicherheit geschaffen wird, also auf Anlagen- und Systemebene sowie den höheren Sicherheitsklassen. Durch die Anpassung der behördlichen Kontrollen/Inspektionen soll erreicht werden, dass Zeit und Ressourcen eingespart werden, um sich auf höhere Sicherheitsklassen konzentrieren zu können.

Ein weiterer Vorschlag aus /KEL 19/ ist, die Zusammenarbeit zwischen verschiedenen Betreibern kerntechnischer Anlagen zu verstärken, um sich überschneidende Arbeiten der Betreiber zu reduzieren sowie nationale Genehmigungen in der finnischen Nuklearindustrie einzuführen. Momentan werden bei der Einführung einer neuen Komponente, die in mehreren kerntechnischen Anlagen genutzt werden soll, von allen betroffenen Betreibern jeweils ähnliche oder sogar gleiche Dokumente zur Genehmigung an die Aufsichtsbehörde geschickt und von allen Betreibern getrennt voneinander Genehmigungen beantragt. Dies bedeutet einen Mehraufwand sowohl für die Betreiber, die getrennt voneinander identische Dokumente erstellen, als auch für die Aufsichtsbehörde, die diese identischen Dokumente einzeln bearbeitet. Durch eine Harmonisierung der Aktivitäten der Betreiber, eine verstärkte Zusammenarbeit und die Nutzung gemeinsamer Genehmigungen kann laut /KEL 19/ die mit der Genehmigung neuer Komponenten verbundene Arbeit deutlich reduziert werden. Dies könnte auf alle Sicherheitsklassen angewendet

werden und damit zu erheblichen Vorteilen in Bezug auf Kosten, Arbeits- und Zeitaufwand führen. Insbesondere gilt dies für Anwendungen, bei denen ähnliche, serienmäßig gefertigte Komponenten verwendet werden können.

In /KEL 20/ werden die Aufgaben der beteiligten Parteien (Aufsichtsbehörde, Betreiber, Hersteller) im Rahmen des Qualifizierungsprozesses von COTS-Komponenten festgelegt. Die Aufsichtsbehörde soll laut /KEL 20/ sicherstellen, dass der Betreiber über geeignete Verfahren verfügt, um eine qualitativ hochwertige Durchführung von Beschaffungen zu gewährleisten, die Kapazitäten und Prozesse der Betreiber sowie deren Umsetzung überwachen sowie bei Bedarf an Bewertungen und Inspektionen von Herstellern teilnehmen. Die Betreiber sollten laut /KEL 20/ die Beschaffung durchführen, über Verfahren und Methoden verfügen, mit denen sie sicherstellen können, dass die Hersteller ihre Aufgaben erfüllen und sicherstellen, dass die Hersteller über die erforderlichen Verfahren und Maßnahmen verfügen sowie die Hersteller zwecks Qualitätssicherung im notwendigen Umfang überwachen. Die Hersteller sollten laut /KEL 20/ über Verfahren und Maßnahmen im Rahmen eines Qualitätssicherungssystems verfügen, um einen qualitativ hochwertigen und angemessenen Betrieb zu gewährleisten, Prozesse und Maßnahmen sowie geeignete Qualitätssicherungs- und Überwachungsmaßnahmen umsetzen sowie die Unterauftragnehmer überwachen und deren Qualität und Lieferfähigkeit sicherstellen.

Hersteller sind laut /KEL 20/ zu bewerten und zu auditieren, um sie für die Lieferung von COTS-Komponenten zum Einsatz in kerntechnischen Einrichtungen zuzulassen. Bei der Bewertung, Auditierung und Zulassung von Herstellern sollte sich laut /KEL 20/ auf ihre Fähigkeit zur Lieferung und Produktion von qualitativ hochwertigen Komponenten sowie auf die Faktoren konzentriert werden, die die Qualität der Komponenten beeinflussen. Besonderes Augenmerk sollte dabei auf Qualitätskontroll- und -sicherungsprozesse des Herstellers sowie deren Umsetzung gelegt werden. Es ist Aufgabe des Betreibers, sicherzustellen, dass die Hersteller Verfahren nutzen, welche die Herstellung qualitativ hochwertiger und für den Verwendungszweck geeigneter Komponenten gewährleisten.

In /KEL 19/ und /KEL 20/ werden zudem diverse Anforderungen an ein Qualifizierungsverfahren für COTS-Komponenten aufgestellt. Hinsichtlich Beschaffung, Entwurf und Herstellung von COTS-Komponenten wird in /KEL 19/ gefordert, dass der Betreiber über detaillierte und nachvollziehbare Praktiken zur Beschaffung verfügen muss. Außerdem müssen unter Berücksichtigung der Zielanwendung und der Umgebungsbedingungen Anforderungsspezifikationen für zu beschaffende COTS-Komponenten erstellt werden,

die wenn möglich von mehreren Betreibern gemeinsam genutzte Dokumente enthalten und durch standortspezifische Anforderungen und Auslegungswerte ergänzt werden. Der Hersteller der COTS-Komponenten muss ausreichende Informationen erhalten, in denen die Anforderungen aus der Anforderungsspezifikation sowie die Beschaffungsverfahren des Betreibers klar und deutlich dargelegt werden. Zudem ist sicherzustellen, dass der Hersteller über ein Qualitätsmanagementsystem verfügt sowie seine eigene Betriebserfahrung und die Betriebserfahrung der zu liefernden Komponenten berücksichtigt. Der Betreiber kann laut /KEL 19/ während der Herstellung der COTS-Komponenten Inspektionen und Tests durchführen oder durchführen lassen, um zu prüfen, ob die Qualität der Komponenten gewährleistet wird.

Hinsichtlich der Beschaffung von COTS-Komponenten wird in /KEL 20/ gefordert, dass marktübliche Komponenten eingesetzt werden sollten, deren Erfüllung standortspezifischer Anforderungen nachzuweisen ist. Allgemeine Anforderungen z. B. an Konstruktion, Qualitätsmanagement, Werkstoffe, Herstellung und Dokumentation sind in einem allgemeinen Pflichtenheft festzulegen. Dieses Pflichtenheft ist so zu erstellen ist, dass es geltenden Anforderungen für die Industrie entspricht. Dieses allgemeine Pflichtenheft gilt dabei für alle Betreiber und für eine bestimmte Komponentengruppe, also nicht spezifisch für eine Komponente. Standortspezifische Anforderungen wie z. B. Auslegungsdruck, -temperatur, Leistung, usw. sind in einem Datenblatt festzulegen und dem allgemeinen Pflichtenheft beizufügen. Ergeben sich durch den geplanten Einsatz in kerntechnischen Anlagen zusätzliche Anforderungen, welche COTS-Komponenten nicht erfüllen oder deren Erfüllung noch nicht nachgewiesen wurde, ist der Betreiber laut /KEL 20/ verpflichtet, die Erfüllung dieser Anforderungen durch Analysen oder Tests nachzuweisen.

Die Qualifizierung von COTS-Komponenten soll laut /KEL 20/ aus zwei Teilen bestehen. Im ersten Schritt erfolgt die Qualifizierung der Komponentenfamilie, was bedeutet, dass die COTS-Komponenten oder die Komponentenfamilie allgemeine Anforderungen erfüllen müssen. Dieser Schritt soll in der Regel bei der ersten Beschaffung von Komponenten für die betreffende Komponentenfamilie durchgeführt werden und kann für alle Betreiber gemeinsam erfolgen. Im zweiten Schritt erfolgt dann eine Qualifizierung bezogen auf die geplante Zielanwendung und die Anlage, in der die COTS-Komponenten eingesetzt werden sollen. In diesem zweiten Schritt fließen also spezifische Anforderungen, die sich aus der Zielanwendung und dem spezifischen Standort ergeben, ein. Dadurch

wird die die Eignung für die spezifische Anwendung und den spezifischen Standort festgestellt. Dieser Schritt muss bei allen zukünftigen Beschaffungen erneut durchgeführt werden.

Im Rahmen des KELPO-Projekts wurde der Einfluss der Sicherheitsklasse auf die Zuverlässigkeit von Komponenten untersucht und es wurde festgestellt, dass nahezu kein Unterschied in der Ausfallhäufigkeit zwischen als sicherheitstechnisch relevant klassifizierten Komponenten und als nicht sicherheitstechnisch relevant klassifizierten Komponenten besteht. Daraus lässt sich laut /KEL 19/ schließen, dass heutige COTS-Komponenten von hoher Qualität und Zuverlässigkeit sind und das spezielle kerntechnische Zusatzanforderungen nicht zweifelsfrei zu einer besseren Qualität führen. Im Gegenteil soll die Qualität sogar sinken können, wenn Hersteller von ihrer bewährten Praxis abweichen müssen, um kerntechnisch qualifizierte Komponenten herstellen zu können. In der Regel sollen COTS-Komponenten laut /KEL 19/ diverse Entwicklungsphasen und Reproduktionen durchlaufen haben, wodurch Mängel und Schwachstellen bereits vielfach beseitigt wurden, während dies bei speziell für die Kerntechnik gefertigten Produkten häufig nicht der Fall ist. Zudem bedeutet die große Anzahl gefertigter COTS-Komponenten auch, dass viel Erfahrung und damit verbundene Verbesserungen verfügbar sind, die zu einer hohen Qualität und Zuverlässigkeit beitragen können. Laut /KEL 19/ soll die Verwendung von COTS-Komponenten ermöglichen, moderne und bewährte Technik zu nutzen, anstatt Komponenten zu beschaffen, die speziell gefertigt sind und aufgrund der Einzigartigkeit der Komponenten und des Herstellungsverfahrens ein überdurchschnittliches Risiko aufweisen.

### 2.2.3 Kanada

Nach kanadischem Regelwerk muss generell sichergestellt werden, dass ein Leittechniksystem so ausgelegt ist, dass die sich aus der Sicherheitsklassifizierung ergebenden Anforderungen erfüllt werden. Außerdem sind sicherheitskritische Merkmale, welche die Zuverlässigkeit und Integrität des Systems erhöhen, zu identifizieren und in die Auslegung des Leittechniksystems einzubeziehen. Zudem ist sicherzustellen, dass das System nicht anfällig für Fehler mit gemeinsamer Ursache (common cause failure, CCF) ist.

Hinsichtlich des Einsatzes kommerzieller Komponenten findet die kanadische Norm CSA N290.14-07 „Qualification of Pre-Developed Software for Use in Safety-Related Instrumentation and Control Applications in Nuclear Power Plants“ /CSA 07/ Anwendung. In dieser wird ein Prozess zur Qualifizierung von COTS-Software aufgestellt, die in

sicherheitstechnisch wichtigen Funktionen in kerntechnischen Anlagen verwendet werden soll. Zur Qualifizierung der COTS-Software ist dabei die spätere Anwendung in Betracht zu ziehen. Es sind alle Software-Komponenten und deren Funktionalität, die Schnittstellen zu anderen Systemen sowie Grenzen, Einschränkungen und Bedingungen für die Verwendung der Software festzulegen. Die zweite Version dieser Norm mit dem Titel CSA N290.14:15 „Qualification of digital hardware and software for use in instrumentation and control applications for nuclear power plants" /CSA 15/ enthält zusätzlich Anforderungen an die Qualifizierung der Hardware von COTS-Komponenten sowie einen erweiterten Umfang an Anforderungen zur Software-Qualifizierung. Zur Hardware-Qualifizierung werden beispielsweise Bewertungen der Umweltverträglichkeit, der elektromagnetischen Störfestigkeit und Emissionen sowie der Erdbebenfestigkeit gefordert. Zudem muss eine Bewertung des Hardware-Entwicklungsprozesses erfolgen, wobei Hardware-Prüftechniken, Hardware-Designprozesse und die Methoden des Herstellungsprozesses analysiert werden müssen.

In Kanada wird bei der Bewertung von COTS-Software hinsichtlich einer möglichen Qualifizierung zum Einsatz in sicherheitstechnisch wichtigen Funktionen in kerntechnischen Einrichtungen berücksichtigt, inwieweit man sich darauf verlassen kann, dass die Software ihre sicherheitsrelevanten Funktionen erfüllt. Dabei werden beispielsweise Aspekte wie ausfallsicheres Verhalten, sichere Fehlererkennung, deterministisches Verhalten, Leistungsfähigkeit, Instandhaltbarkeit, Sicherheit, Verlässlichkeit sowie Prüfbarkeit in Betracht gezogen.

Zur Qualifizierung von COTS-Komponenten nach dem in /CSA 07/ bzw. /CSA 15/ vorgegebenem Prozess sind zu Beginn die Funktionen der zu qualifizierenden Komponenten zu identifizieren. Zudem sind die Schnittstellen zu anderen Systemen aufzuzeigen und zu beschreiben. Daran anschließend erfolgt eine Kategorisierung der auszuführenden Sicherheitsfunktionen der Komponenten anhand der IEC 61226 /DIN 10a/. Nach der Kategorisierung der Sicherheitsfunktionen erfolgt eine Bewertung von „Problemen bei der Qualifizierung" und anschließend die eigentliche Qualifizierung, deren Ergebnisse zu dokumentieren sind.

Unter der Bewertung von „Problemen bei der Qualifizierung" erfolgt die Bewertung einer Liste mit häufig auftretenden Schwachstellen oder Problemen im Zusammenhang mit COTS-Komponenten, insbesondere wenn diese Software enthalten. Dabei handelt es sich im postulierte Fehleraspekte, die das Potential haben, sicherheitsrelevante

Funktionen der zu qualifizierenden Komponenten zu beeinträchtigen oder sicherheitsrelevante Funktionen anderer Systeme oder Komponenten zu stören. Bei der Bewertung wird analysiert, inwieweit die auf dieser Liste genannten Schwachstellen und Probleme für die zu qualifizierenden Komponenten relevant sind und ob die Schwachstelle bzw. das Problem behoben werden konnte bzw. nicht behoben werden kann, was damit eine Qualifizierung der Komponenten verhindert. Da der GRS solch eine Liste nicht vorliegt, können keine genauen Aussagen gegeben werden.

Bei der eigentlichen Qualifizierung der COTS-Komponenten kann nach einer oder mehrerer der nachfolgend vorgestellten Methoden vorgegangen werden. Bei der „recognized program method“ erfolgt die Qualifizierung der COTS-Komponenten dadurch, dass diese nach einer anderen relevanten Norm aus anderen Industriebereichen zertifiziert sind, wie beispielsweise der IEC 61508. Zusätzlich ist dann noch die tatsächliche Eignung der Komponenten für die Zielfunktion festzustellen. Die „mature product method“ stützt sich bei der Qualifizierung der COTS-Komponenten auf Daten aus der Betriebserfahrung. Eine Qualifizierung kann hierbei für Komponenten erfolgen, die sich in der Praxis bewährt haben, wobei diese Methode nicht für Komponenten, die in Sicherheitsfunktionen der Kategorie A eingesetzt werden sollen, anwendbar ist. Der für die Qualifizierung erforderliche Umfang an Daten aus der Betriebserfahrung hängt von der Komplexität der Komponenten sowie von der Kategorie der Sicherheitsfunktion ab, in der die Komponenten später eingesetzt werden soll. Bei der Methode „proof through testing“ kann die Qualifizierung der COTS-Komponenten durch ein bestimmtes Maß an Tests erfolgen, wobei die Tests im Betrieb in einer für die spätere Zielanwendung repräsentativen Konfiguration erfolgen müssen. Diese Methode ist nur für Komponenten geringer Komplexität sowie für einen späteren Einsatz in Sicherheitsfunktionen der Kategorie C zulässig. Die Methode „preponderance of evidence“ dient zur Qualifizierung der COTS-Komponenten, wenn bei den anderen drei genannten Methoden nur eine teilweise Qualifizierung erreicht werden konnte. Dazu werden Aktivitäten wie beispielsweise ergänzende Tests oder Analysen durchgeführt oder eine frühere, bereits erfolgte Qualifizierung der Komponenten berücksichtigt.

Hinsichtlich der Methode „preponderance of evidence“ sind laut /ALI 18/ diverse Aktivitäten möglich, die durchgeführt werden können, um eine Qualifizierung der COTS-Komponenten zu erreichen. Es wird dabei zwischen indirekten und direkten Aktivitäten unterschieden, wobei in der Regel eine Kombination von mehreren dieser Aktivitäten zur erfolgreichen Qualifizierung notwendig ist. Beispiele für indirekte Aktivitäten sind laut

/ALI 18/ die Bewertung des Qualitätsmanagements des Herstellers, die Berücksichtigung der Betriebserfahrung des Herstellers, die Überprüfung der Referenzstandorte des Herstellers, die Überprüfung der Möglichkeit zur Wartung der COTS-Komponenten, die Einbeziehung bereits vorhandener Zertifizierungen sowie die Berücksichtigung von Instandhaltungskapazitäten. Beispiele für direkte Aktivitäten sind die Durchführung einer Fehlermöglichkeits- und Einflussanalyse (FMEA), die Analyse der Qualität des Designs, die Analyse der Sicherheitseigenschaften, die Durchführung einer Fehlerbaumanalyse, die Überprüfung des Software-Codes, eine funktionale Prüfung sowie eine Analyse der Zuverlässigkeit der Komponenten.

Erfolgt die Qualifizierung von COTS-Komponenten anhand der in /CSA 15/ genannten Vorgehensweise, ist die Qualifizierung in der Regel anwendungsspezifisch und soll laut /XIN 18/ den Nachweis erbringen, dass die COTS-Komponenten hinsichtlich der funktionalen Sicherheit zum Einsatz in der vorgesehenen Anwendung geeignet sind. Zudem muss eine sicherheitsbezogene Benutzerdokumentation vorhanden sein, es muss der Nachweis der Korrektheit des Designs der COTS-Komponenten gegeben werden und die gesammelten Nachweise müssen überprüfbar sein. Bei der anwendungsspezifischen Qualifizierung der COTS-Komponenten sind laut /XIN 18/ die Spezifikationen der Komponenten (Hardware, Software und Werkzeuge) zu bewerten. Zudem sollte eine Bewertung der Betriebserfahrung erfolgen, wobei Daten zur Betriebserfahrung gesammelt und ausgewertet sowie Änderungen am Design der Komponenten bewertet werden sollen. Außerdem muss eine Bewertung der Instandhaltungsprozesse und -prüfungen der COTS-Komponenten erfolgen. Bei der Bewertung des Hardware-Designs der COTS-Komponenten sind Aspekte wie Umweltverträglichkeit, elektromagnetische Störfestigkeit und Emissionen, Erdbebenfestigkeit, Hardware-Zuverlässigkeit und Fehlermodi sowie die Nutzungsdauer der Hardware zu berücksichtigen. Zudem ist der Hardware-Entwicklungsprozess zu bewerten, wobei Aspekte wie Hardware-Prüftechniken, der Hardware-Designprozess und der Herstellungsprozess und die Qualitätssicherung zu betrachten sind. Laut /XIN 18/ sind bei der Bewertung des Software-Designs Aspekte wie die Auswirkungen von Softwarefehlern, Software-Diagnose und Selbsttestfähigkeit, die Qualität des Software-Designs sowie eine Software-Gefährdungsanalyse (HAZOP) relevant. Die Bewertung des Software-Entwicklungsprozesses muss Aspekte wie Software-Implementierungsprozesse, Software-Testtechniken, Software-Konfigurationsmanagementprozesse sowie den Software-Support und die Support-Lebensdauer berücksichtigen. Werden Nachweise aus Zertifizierungen Dritter herangezogen, können

beispielsweise Zertifizierungen des Qualitätsmanagementsystems Dritter, Sicherheitszertifikate Dritter, die Konformität mit Hardware-Teststandards Dritter oder Zertifizierungen des Softwareentwicklungsprozesses Dritter berücksichtigt werden. Bei Änderungen an bereits qualifizierten Komponenten sind die Auswirkungen dieser Änderungen zu ermitteln und es ist zu bewerten, ob die Qualifizierung weiterhin ihre Gültigkeit behält oder ob eine Neuqualifizierung aufgrund der Änderungen erforderlich ist.

Im Rahmen des IAEA „Technical Meeting on Justification of Commercial Industrial Instrumentation and Control Equipment for Nuclear Power Plant Applications“ wurden im Vortrag /ROG 18/ Einblicke in die Problematik des Einsatzes von softwarebasierten COTS-Komponenten in Kanada gegeben. Dabei wurde erwähnt, dass COTS-Komponenten so detailliert verstanden werden müssen, dass mit der erforderlichen Sicherheit gewährleistet werden kann, dass die COTS-Komponenten ihre sicherheitskritischen Aufgaben erfüllen. Hinsichtlich der Qualifizierung softwarebasierter COTS-Komponenten wurde erwähnt, dass der benötigte Aufwand und die benötige Zeit zur Durchführung der Qualifizierung nicht zu unterschätzen sind. Zudem ist eine Qualitätssicherung der COTS-Software durchzuführen, was es erforderlich macht, dass die dazu erforderlichen Dokumente und Informationen freigegeben werden müssen, auch wenn diese geschützt sind. Dies gilt auch für durch Informationen zu von Unterauftragnehmern entwickelten Komponenten. Laut /ROG 18/ ist nach Möglichkeit die „mature product method“ bei der Qualifizierung anzuwenden, da durch eine umfangreiche Auswertung von Daten aus der Betriebserfahrung bestehende Probleme entdeckt und behoben werden können. Zudem sind Anforderungen bezüglich Cybersicherheit zu berücksichtigen. Bezüglich des Beschaffungsprozesses von COTS-Komponenten wurde in /ROG 18/ ausgesagt, dass der Beschaffungsprozess sehr komplex sein kann. In Frage kommende Hersteller müssen einen Qualitätssicherungsprozess inklusive Auditierungen durchlaufen, um in eine Liste zugelassener Hersteller aufgenommen zu werden. In diesem Prozess sind auch alle Zulieferer des Herstellers aufzunehmen.

Hinsichtlich der Komplexität von COTS-Komponenten wurde in /ALI 18/ ausgesagt, dass diese möglichst gering sein sollte. Dies gilt insbesondere für softwarebasierte COTS-Komponenten, die für den Einsatz in kerntechnischen Einrichtungen qualifiziert werden sollen, um eine Qualifizierung erfolgreich durchführen zu können. Durch diverse Analysen wie eine Fehlermöglichkeits- und Einflussanalyse (FMEA), Fehlerbaumanalyse (FTA) oder Gefährdungsanalyse (HAZOP) mit dem Schwerpunkt der Analysen auf das Design, die Herstellung und die Prüfung kann die Komplexität der COTS-Komponenten

bestimmt werden. Um eine Qualifizierung von COTS-Komponenten erfolgreich abzuschließen, sollte, insbesondere wenn die COTS-Komponenten Software enthalten, laut /ALI 18/ bei der Auswahl der Komponenten so vorgegangen werden, dass nur Komponenten mit relevanter Betriebserfahrung, nachvollziehbarem Herstellungsprozess, bereits vorhandenen Zertifizierungen sowie einfachem Aufbau ausgewählt werden. Des Weiteren wurde darauf hingewiesen, dass die Qualifizierung vor dem endgültigen Kauf abgeschlossen sein sollte, da auch der Hersteller stark in den Qualifizierungsprozess eingebunden werden muss und dessen Anreiz, bei der Qualifizierung mitzuwirken, größer ist, wenn der Kauf noch nicht abgeschlossen wurde.

Hinsichtlich des Aufwandes für eine Qualifizierung von COTS-Komponenten wurde in /XIN 18/ erwähnt, dass dieser von verschiedenen Faktoren abhängt, wie beispielsweise der Sicherheitsklassifizierung der Zielanwendung oder dem Vorhandensein einer bereits durchgeführten Zertifizierung und dem Herstellungsprozess der Komponenten. Außerdem wurde hinsichtlich der Qualifizierung von COTS-Komponenten ausgesagt, dass diese in Kanada in der Regel anhand der beschriebenen Vorgehensweise nach der Norm CSA N290.14:15 /CSA 15/ erfolgt, dass aber auch die Möglichkeit besteht, eine Qualifizierung nach dem Verfahren der „Commercial Grade Dedication“ durchzuführen, was einer der möglichen US-amerikanischen Vorgehensweisen entspricht (siehe Abschnitt 2.2.5 dieses Berichtes).

### 2.2.4 Vereinigtes Königreich

Die Aufsichtsbehörde (ONR, Office for Nuclear Regulation) im Vereinigten Königreich (UK, United Kingdom) arbeitet in der Regel nicht mit auf Normen basierenden Regelungen, sondern mit Zielvorgaben, die von den Betreibern kerntechnischer Anlagen zu erfüllen sind. Eher übergeordnete, allgemeine Zielvorgaben hat ONR im Leitfaden für regulatorische Beurteilungen und Empfehlungen, den Safety Assessment Principles (SAP) /ONR 20/, aufgestellt. Zusätzlich wurden von ONR für diverse Themenbereiche Erwartungen und Überlegungen in den unterstützenden technischen Nuclear Safety Technical Assessment Guides (TAG) aufgestellt. Anschließend ist es Sache der Betreiber, eigene Regelungen und Verfahren z. B. für die Prüfung oder den Einsatz von Komponenten zu entwickeln, um sicherzustellen, dass die Zielvorgaben von ONR erfüllt werden und dass die Komponenten für die Anwendung und die jeweilige sicherheitstechnische Bedeutung der Funktion geeignet sind, für die sie verwendet werden sollen. Dabei ist die Verwendung spezifischer Normen und Regelwerke nicht zwingend vorge-

schrieben, aber der Nachweis einer systematischen Anwendung nationaler und internationaler Normen mit entsprechenden Begründungen bei Abweichungen von diesen wird empfohlen.

Bei COTS-Komponenten, die in der Regel auf rechnerbasierten oder programmierbaren Komponenten basieren, handelt es sich aus Sicht von ONR um „Smart Devices“, welche rechnerbasierten Systemen gleichgestellt werden. Der relevante SAP /ONR 20/ für rechnerbasierte Systeme ist ESS.27. Dieser besagt, dass für den Fall, dass die Systemzuverlässigkeit in erheblichem Maße von der Leistung der Software abhängt, die Einhaltung geeigneter Normen und Praktiken während des gesamten Lebenszyklus der Software sichergestellt werden muss, um die Sicherheit zu gewährleisten. Weiterhin wird in den SAP erwähnt, dass aufgrund der oftmals vorhandenen Komplexität von „Smart Devices“ herkömmliche Methoden zur Zuverlässigkeitsbewertung in der Regel nicht ausreichen, um die Komponenten beispielsweise hinsichtlich des Risikos systematischer Ausfälle zu bewerten. Daher sind zusätzliche, geeignete Verfahren vorzusehen, um die Zuverlässigkeit solcher Komponenten nachzuweisen, wobei die Härte des Verfahrens dem geforderten Zuverlässigkeitsniveau entsprechen muss. Für „Smart Devices“ (also auch COTS-Komponenten) wird dabei laut /ONR 20/ die Verfolgung eines zweistufigen Ansatzes, basierend auf den nachfolgend beschriebenen Säulen „Production Excellence“ und „Independent Confidence Building“, erwartet:

**„Production Excellence“:**
Hierbei soll der Nachweis hervorragender Leistungen in allen Bereichen der Produktion der Komponenten erfolgen, wobei der Lebenszyklus von der anfänglichen Spezifikation bis zur Inbetriebnahme zu betrachten ist. Die „Production Excellence“ steht somit im Zusammenhang mit der Bewertung der Qualität der Prozesse des Designs, der Entwicklung, der Herstellung und der Abnahmeprüfung (FAT, Factory Acceptance Test) der Komponenten beim Hersteller. Durch die Bewertung der „Production Excellence“ soll gezeigt werden, dass während des gesamten Entwicklungszyklus geeignete Techniken und Maßnahmen angewandt wurden, welche sich auf einschlägige Normen stützen und der Sicherheitsklasse bzw. dem SIL-Level der zu bewertenden Komponenten angemessen sind. Die Bewertung erfolgt hierbei in der Regel anhand eines Fragebogens (liegt der GRS nicht vor), der auf Grundlage der IEC 61508 entwickelt wurde und ca. 300 Fragen aus den Bereichen Qualitätssicherung und Sicherheitsmanagement, generische Aspekte bezüglich programmierbarer elektronischer Komponenten, Hardware-Entwicklungsprozess und -Verifizierung sowie Software-Entwicklungsprozess und -Verifizierung

enthält. Je nach Sicherheitsklassifizierung der zu bewertenden Komponenten werden dabei unterschiedliche Fragen verwendet. Eine Bewertung nach anderen Normen ist akzeptabel, wenn diese gleichwertige Anforderungen stellen.

Die Bewertung erfolgt dabei in der Regel unabhängig von der späteren Anwendung der Komponenten. Daher kann die Qualifizierung für nachfolgende Anwendungen ebenfalls verwendet werden, ohne diese neu durchführen zu müssen. Dabei ist allerdings nachzuweisen, dass die Komponenten für die Anwendungen geeignet sind. Dem Hersteller der Komponenten fällt dabei die Aufgabe zu, die Fragen zu beantworten und die Korrektheit der Antworten nachzuweisen. Anschließend erfolgt eine Bewertung der Antworten und Nachweise durch die Aufsichtsbehörde oder ein von der Aufsichtsbehörde beauftragtes drittes Unternehmen. Werden Lücken/Schwachstellen festgestellt, sind diese zu beheben oder durch geeignete Maßnahmen auszugleichen. Es ist zu begründen, dass die getroffene Maßnahme die Lücke/Schwachstelle so schließt, dass diese nicht mehr vorliegt. In Einzelfällen, in denen die Lücke/Schwachstelle nicht als erhebliche Beeinträchtigung angesehen wird, kann diese durch andere Nachweise geschlossen werden. Dabei ist anzugeben und zu begründen, warum die Lücke/Schwachstelle nicht als signifikant angesehen wird und wie die anderen Nachweise als angemessen beurteilt werden.

Anhand der „Production Excellence“ ist laut /ONR 20/ nachzuweisen, dass technische Praktiken während des Designprozesses der Komponenten angewendet wurden, die mit aktuell anerkannten Standards für die Entwicklung von Software für rechnerbasierte Sicherheitssysteme übereinstimmen. Es sind einschlägige, bewährte Verfahren anzuwenden, um Fehler zu vermeiden, Fehler zu erkennen und zu beseitigen und für nicht erkannte Fehler eine eingebaute Systemtoleranz zu schaffen. Dabei ist es wichtig, dass eindeutige, umfassende und überprüfte Spezifikationen der Systemanforderungen, die sowohl das Systemverhalten als auch die Anforderungen für den gesamten Lebenszyklus des Systems abdecken, bereits in den frühesten Phasen des Produktionsprozesses zur Verfügung stehen. Zudem ist nachzuweisen, dass auf Seiten des Herstellers ein Qualitätsmanagementsystem nach modernen Standards eingeführt wurde. Zudem ist ein umfassendes Testprogramm anzuwenden, mit dem alle Systemfunktionen überprüft werden. Dabei muss vor der Installation der Komponenten in der Zielanwendung die Verifizierung aller Phasen des Herstellungsprozesses und die Validierung des integrierten Systems gegenüber seiner Spezifikation erfolgen. Diese Prüfungen sind von Personen durchzuführen, die nicht an Spezifikation und Design beteiligt waren. Nach der

Installation ist zu demonstrieren, dass das Sicherheitssystem in Verbindung mit der Anlage gemäß seiner Spezifikation funktioniert. Dazu sind umfangreiche Tests vor der Inbetriebnahme erforderlich, um nachzuweisen, dass das System in der Anlage gemäß Spezifikation funktioniert. Dieser Nachweis ist von Personen zu erbringen, die nicht an der Spezifikation, dem Design und der Herstellung beteiligt waren. Zudem ist eine dynamische Prüfung des Systems durchzuführen, welche auf das gesamte System anzuwenden ist, und den Nachweis erbringt, dass das System wie vorgesehen funktioniert. Sofern Betriebsprofil und Transienten des Gesamtsystems bekannt sind, kann anstatt der dynamischen Prüfung auch eine statische Prüfung durchgeführt werden.

**„Independent Confidence Building“:**
Hierbei soll eine unabhängige und gründliche Prüfung und Bewertung der Tauglichkeit der Komponenten erfolgen. Die Bewertungen werden unabhängig vom Betreiber durchgeführt, bei Bedarf kann spezialisierte technische Unterstützung hinzugezogen werden. Die unabhängigen Prüfer müssen ihre Vorgehensweise für jede Aufgabe festlegen und begründen. Wenn praktikabel, sollten die unabhängigen Prüfer andere Prüfmethoden anwenden als der Hersteller. Es ist nicht praktikabel, Maßnahmen zur „Independent Confidence Building“ zu Beginn eines Projektes festzulegen, da Einzelheiten der Komponenten (z. B. Architektur, Technologie, angewandte Techniken während Entwicklung) zu diesem Zeitpunkt noch nicht bekannt sind. Daher sind diese Maßnahmen erst festzulegen, wenn die Einzelheiten der Komponenten bekannt sind. Die Maßnahmen zur „Independent Confidence Building“ sind auf die endgültig ausgelieferten Komponenten anzuwenden, sollten also nach Abschluss der Verifizierung und Validierung durch den Hersteller erfolgen.

Bei der „Independent Confidence Building“ ist laut /ONR 20/ zu beachten, dass eine vollständige und vorzugsweise mehrfache (diversitäre) Überprüfung der endgültig validierten Software durchgeführt wird, wobei diese Überprüfung von einem von dem Hersteller unabhängigen Team durchzuführen ist. Dabei ist zu berücksichtigen, dass eine unabhängige Überprüfung der Komponenten durchzuführen ist, die eine Analyse des endgültigen Systems ermöglicht. Zudem ist eine unabhängige Überprüfung der Design- und Produktionsprozesse durchzuführen. Außerdem ist eine unabhängige Bewertung des Testprogramms durchzuführen, wobei der gesamte Umfang der Testaktivitäten abzudecken ist.

Dieser zweistufige Ansatz soll laut /ONR 20/ dazu dienen, dass sich die Qualifizierung von Komponenten sowohl auf den Nachweis einer qualitativ hochwertigen Produktion

als auch auf eine unabhängige Prüfung der Tauglichkeit der Komponenten stützt, bei der keine signifikanten Mängel oder Fehler festgestellt werden, die die erforderliche sicherheitstechnische Bedeutung der Komponenten beeinträchtigen. Werden Schwachstellen im Produktionsprozess festgestellt, sind laut /ONR 20/ Maßnahmen zu ergreifen, um diese zu beheben, wobei die Wahl der Maßnahmen und ihre Wirksamkeit zu begründen und nachzuweisen sind. Die Art der Maßnahmen sollte dabei von den festgestellten Schwachstellen abhängen und auf diese ausgerichtet sein.

Unterstützende technische Zielvorgaben zum Einsatz rechnerbasierter Systeme liefert der Nuclear Safety Technical Assessment Guide (TAG) „Computer Based Safety Systems (NS-TAST-GD-046)“ /ONR 19/. Hierin ist auch ein Kapitel enthalten, welches sich mit der Qualifizierung und dem Einsatz kommerzieller Komponenten befasst. Hinsichtlich des zweistufigen Ansatzes wird in /ONR 19/ erwähnt, dass der Umfang der Techniken, die zum Nachweis der Tauglichkeit der Komponenten eingesetzt werden, der Sicherheitsklassifizierung und der Zielanwendung der Komponenten entsprechen sollten. Dabei ist die Eignung der verwendeten Techniken zu prüfen und zu begründen. Es werden drei Klassen berücksichtigt, wobei Klasse 3 für Funktionen der niedrigsten Sicherheit und Klasse 1 für Funktionen der höchsten Sicherheit gilt. Bei Produkten für den Einsatz in Klasse 3 kann eine nachgewiesene, gute kommerzielle Qualität der Produktion in Verbindung mit Inbetriebnahmetests ausreichen, um die Komponenten zu qualifizieren. Komponenten für den Einsatz in Klasse 1 benötigen zur Qualifizierung hingegen eine breite Palette an Herstellerunterlagen einschließlich des Quellcodes.

Hinsichtlich COTS-Komponenten im Speziellen ist in /ONR 19/ erwähnt, dass deren Eignung für den Einsatz angemessen nachzuweisen ist. Werden COTS-Komponenten in nicht sicherheitstechnisch wichtigen Funktionen eingesetzt, ist nachzuweisen, dass durch ihren Einsatz keine sicherheitstechnisch wichtigen Funktionen beeinträchtigt werden. Zum Nachweis der Eignung von COTS-Komponenten sowie zum Prozess der Qualifizierung ist der Zugang zu zahlreichen Dokumenten notwendig und vom Hersteller sind umfangreiche Informationen zur Verfügung zu stellen, damit die „Production Excellence“ nachgewiesen werden kann und erforderliche Maßnahmen zum „Independent Confidence Building“ getroffen werden können. Hierzu ist beispielsweise ein Zugang zum Quellcode notwendig, was eine enge Zusammenarbeit zwischen Betreiber und Hersteller notwendig macht. In der in /IAE 20/ beschriebenen, länderspezifischen Vorgehensweise des Vereinigten Königreichs wird daher erwähnt, dass eine frühzeitige Vereinbarung mit dem Hersteller hinsichtlich benötigter Dokumente und notwendiger

Vertraulichkeitsvereinbarungen empfehlenswert ist. Außerdem sollten Strategien hinsichtlich Wartung, Software- und Firmware-Updates sowie Obsoleszenz entwickelt werden. Die „Production Excellence“ bei COTS-Komponenten bezieht sich in der Regel auf die Entwicklung der Komponenten, bevor diese kommerziell verfügbar gemacht wurden. Die Qualifizierung zur Integration der COTS-Komponenten in die Zielanwendung wird durch die Bewertung der Eignung der Komponenten für die Anwendung und die Durchführung von Maßnahmen zum „Independent Confidence Building“ erreicht.

Im Vereinigten Königreich können laut der in /IAE 20/ beschriebenen, länderspezifischen Vorgehensweise auch bereits existierende Zertifizierungen bei der Qualifizierung von COTS-Komponenten in Betracht gezogen werden. Allerdings werden bereits existierende Zertifizierungen nur begrenzt berücksichtigt, da diese oftmals nicht verständlich sind und nicht für die spezifische Zielanwendung genutzt werden können. Eine Ausnahme bilden hierbei Zertifizierungen nach IEC 61508, die berücksichtigt werden. Insbesondere in den Sicherheitsklassen 1 und 2 bedürfen bereits existierende Zertifizierungen einer unabhängigen Überprüfung. Des Weiteren wird in der in /IAE 20/ beschriebenen, länderspezifischen Vorgehensweise erwähnt, dass bereits bestehende Betriebserfahrung von COTS-Komponenten zwar für die Qualifizierung berücksichtigt werden kann, dass dies aber nur eine schwache Qualifizierung darstellt. Die Berücksichtigung von Betriebserfahrung hängt zudem wesentlich von der Qualität der erfassten Daten (z. B. Versionsnummer, Anzahl der Anforderungen, Fehlerart) und den vertraglichen Regelungen für die Meldung von Fehlern ab. In der Regel muss zur Qualifizierung von COTS-Komponenten die Betriebserfahrung durch weitere Analysen ergänzt werden.

Da COTS-Komponenten oftmals die Möglichkeit bieten, in einem breiten Anwendungsspektrum eingesetzt werden zu können, wird im Vereinigten Königreich laut der in /IAE 20/ beschriebenen, länderspezifischen Vorgehensweise zu Beginn der Qualifizierung von COTS-Komponenten eine Identifizierung der erforderlichen Eigenschaften als notwendig angesehen. Nach dem darauffolgenden zweistufigen Ansatz mit Maßnahmen zu „Production Excellence“ und „Independent Confidence Building“ erfolgt dann laut der in /IAE 20/ beschriebenen Vorgehensweise eine Qualifizierung der Hardware der COTS-Komponenten, welche auch eine Qualifizierung hinsichtlich Umgebungsbedingungen einschließlich einer Qualifizierung hinsichtlich der elektromagnetischen Verträglichkeit umfasst. Anschließend ist es bei der Qualifizierung wichtig, dass eine Bewertung der Eignung der Komponenten für die Zielanwendung durchgeführt wird. Eine generische Qualifizierung zum Einsatz in mehreren Anwendungen kann akzeptabel sein, dabei ist

es aber wichtig, die Grenzen solcher Qualifizierungen zu verstehen und zu berücksichtigen. Insbesondere sollten alle Nutzungsbeschränkungen, welche die Funktionsfähigkeit innerhalb bestimmter Betriebsprofile einschränken können, ermittelt werden. Beim Heranziehen einer generischen Qualifizierung für eine spezifische Anwendung ist ein angemessener Nachweis zur Tauglichkeit der Komponenten zu erbringen, z. B. durch speziell auf die gewählte Anwendung ausgerichtete Maßnahmen zum „Independent Confidence Building“.

### 2.2.5 USA

In den USA müssen Komponenten, die in sicherheitstechnisch wichtigen Funktionen in Kernkraftwerken eingesetzt werden sollen, im Rahmen einer nuklearen Qualifizierung hinsichtlich ihrer Eignung für den Einsatz überprüft werden. Komponenten, die eine solche Qualifizierung durchlaufen haben, werden Basiskomponenten genannt. Ist es nicht möglich, Komponenten zu beschaffen, die eine nukleare Qualifizierung durchlaufen haben, ist der Einsatz von COTS-Komponenten möglich. Um diese in sicherheitstechnisch wichtigen Funktionen in Kernkraftwerken in den USA einsetzen zu können, ist eine Qualifizierung durchzuführen, durch welche eine hinreichende Gewähr dafür erhalten werden soll, dass COTS-Komponenten, die als Basiskomponenten verwendet werden sollen, ihre vorgesehenen Sicherheitsfunktionen erfüllen. Anschließend gelten die COTS-Komponenten als gleichwertig zu Basiskomponenten.

Der aktuelle Leitfaden der U.S. NRC RG 1.250 mit dem Titel „Dedication of Commercial-Grade Digital Instrumentation and Control Items for Use in Nuclear Power Plants” /NRC 22/ beschreibt den von der U.S. NRC verwendeten Ansatz zur Feststellung der Erfüllung der regulatorischen Anforderungen zur Zulassung von COTS-Komponenten zum Einsatz in sicherheitstechnisch wichtigen Funktionen in Kernkraftwerken. Es werden zwei mögliche Prozesse zur Qualifizierung von COTS-Komponenten für den Einsatz in sicherheitstechnisch wichtigen Funktionen in Kernkraftwerken genannt. Zum einen ist dies das Verfahren der „Commercial Grade Dedication“, zum anderen die Nutzung einer bereits vorhandenen Zertifizierung einer Komponente nach IEC 61508 (Norm zur funktionalen Sicherheit).

Das Verfahren der „Commercial Grade Dedication“ dient dazu, COTS-Komponenten in sicherheitstechnisch wichtigen Funktionen einsetzen zu können. Dabei handelt es sich um ein Verfahren, welches hinreichende Gewähr dafür bringen soll, dass die COTS-Komponenten ihre vorgesehenen Sicherheitsfunktionen erfüllen. Die im EPRI-Bericht

TR-106439 „Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications" /EPR 96/ beschriebene Methode wird von der U.S. NRC als akzeptable Methode für eine "Commercial Grade Dedication" anerkannt. In /EPR 96/ wird ausgesagt, dass die Überprüfung der Zuverlässigkeit von COTS-Komponenten z. B. die Untersuchung der Prozesse des Herstellers sowie die Einbeziehung der Betriebserfahrung der Komponenten umfassen soll. Zur Überprüfung kritischer Merkmale enthält /EPR 96/ Akzeptanzkriterien und Verifizierungsmethoden. Dabei wird in /EPR 96/ herausgestellt, dass eine vollständige Definition der Anforderungen an Hardware, Software, Mensch-Maschine-Schnittstelle, Qualität und Zuverlässigkeit eine wichtige Voraussetzung für die Qualifizierung von COTS-Komponenten ist.

Der Bericht des Nuclear Energy Institutes 17-06 mit dem Titel „Guidance on Using IEC 61508 SIL Certification to Support the Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Related Applications" /NEI 19/ besagt, dass die in /EPR 96/ beschriebenen kritischen Merkmale auch dann erfüllt sind, wenn die Komponenten mit einem angemessenen SIL-Level nach IEC 61508 hergestellt wurden. Die Erfüllung der kritischen Merkmale wird dabei durch Inspektionen, Tests oder Analysen verifiziert. Zusätzlich erfolgt ein „Commercial Grade Survey" anhand einer Zertifizierung gemäß /DIN 11/. Die dabei eingebundene Stelle zur Zertifizierung wird von der U.S. NRC durch Beobachtung der Akkreditierung dieser Stelle oder durch Beobachtung der Zertifizierung unter Verwendung einer in /NEI 19/ enthaltenen Checkliste begutachtet.

Nachfolgend werden die beiden möglichen Prozesse zur Qualifizierung von COTS-Komponenten für den Einsatz in sicherheitstechnisch wichtigen Funktionen in den USA hinsichtlich der für das Vorhaben relevanten Inhalte beschrieben.

**Commercial Grade Dedication**

Um Fragen hinsichtlich Auslegung, Beschaffung und Qualifizierung kommerzieller Komponenten zu beantworten, hat das Electric Power Research Institute (EPRI) den Leitfaden TR-106439 /EPR 96/ entwickelt, in dem ein Ansatz für die Bewertung und Akzeptanz von COTS-Komponenten zum Einsatz in sicherheitstechnisch wichtigen Funktionen in Kernkraftwerken gegeben wird. Dieser Leitfaden stützt sich auf das Verfahren der „Commercial Grade Dedication" und enthält zusätzliche Anmerkungen, um spezifische Probleme bei COTS-Komponenten zu lösen. Schwerpunkte liegen dabei auf Tests, Analysen, Bewertungen der Hersteller und einer Einbeziehung der Betriebserfahrung, um eine angemessene Sicherheit und Zuverlässigkeit der Komponenten zu gewährleisten.

Das Verfahren der „Commercial Grade Dedication“ soll die Gewährleistung erbringen, dass die COTS-Komponenten ihre vorgesehene Sicherheitsfunktionen erfüllen. Um das Verfahren durchführen zu können, sind im Vorfeld einige Schritte notwendig. Als erstes sind Informationen hinsichtlich der geplanten Zielanwendung der COTS-Komponenten zu sammeln (z. B. sicherheitstechnische Funktion, Umgebungsbedingungen, spezifische Anforderungen). Anschließend ist die Entscheidung zu treffen, ob die „Commercial Grade Dedication“ auf eine bestimmte Anwendung fokussiert sein soll oder ob sie einen breiten, generischen Fokus haben soll. Daraufhin erfolgt die Ermittlung möglicher COTS-Komponenten als Kandidaten für den Einsatz in der Zielanwendung unter Einbeziehung von beispielsweise deren Funktionalität, weiteren Merkmalen und einer Befragung der Hersteller. Anschließende Tests und Analysen sollen die generelle Eignung der COTS-Komponenten bestätigen, wobei diese in Abhängigkeit von der beabsichtigten Zielanwendung aber auch der Verfügbarkeit von Informationen stattfinden sollen.

Das anschließende Verfahren der „Commercial Grade Dedication“ soll dann dem Nachweis dienen, dass die tatsächlich gefertigten COTS-Komponenten mit dem Entwurf übereinstimmen. Für die „Commercial Grade Dedication“ ist laut /EPR 96/ ein Prozess basierend auf einer technischen Bewertung zur Definition der Anforderungen an die COTS-Komponenten, einer Definition kritischer Merkmale sowie die Anwendung mindestens einer von vier Akzeptanzmethoden notwendig. Bei der technischen Bewertung der COTS-Komponenten ist die funktionale Klassifizierung (sicherheitsrelevant oder nicht) durchzuführen, wobei die späteren Sicherheitsfunktionen, welche die COTS-Komponenten ausführen sollen, zu definieren sind. Anschließend sind im Rahmen der technischen Bewertung die Anforderungen an das Design festzulegen, die Äquivalenz der Ersatzkomponenten zu ursprünglichen Komponenten (bei einem Austausch) zu bewerten sowie die Spezifikation geeigneter technischer und qualitativer Anforderungen an die COTS-Komponenten festzulegen. Nach der technischen Bewertung erfolgt dann in der Regel eine Fehler-Möglichkeits- und Einfluss-Analyse (FMEA) auf Grundlage der später auszuführenden Sicherheitsfunktionen, um die kritischen Merkmale der COTS-Komponenten zu identifizieren. Die kritischen Merkmale sind Merkmale, die für die Ausführung der Sicherheitsfunktionen der COTS-Komponenten entscheidend sind. Jedem kritischen Merkmal werden ein spezifisches Akzeptanzkriterium und eine Akzeptanzmethode zugeordnet. Um eine hinreichende Gewähr dafür zu bieten, dass die COTS-Komponenten die Anforderungen erfüllen, erfolgt danach die Durchführung einer oder mehrerer von vier zur Verfügung stehenden Akzeptanzmethoden, um die Eigenschaften der COTS-Komponenten zu verifizieren und festzustellen, ob die kritischen Merkmale

erfüllt werden. Insbesondere für digitale COTS-Komponenten ist die Anwendung nur einer der vier Akzeptanzmethoden nicht ausreichend. Laut /EPR 96/ werden in den meisten Fällen die Akzeptanzmethoden 1, 2 und 4 benötigt. Nach der Durchführung dieser Schritte gelten die überprüften COTS-Komponenten als Basiskomponenten für die festgelegten Funktionen.

Die kritischen Merkmale sind laut /EPR 96/ die wichtigsten Merkmale von COTS-Komponenten, wobei diese in die Kategorien physikalische Merkmale, Leistungsmerkmale und Zuverlässigkeitsmerkmale unterteilt werden können. Zur Aufstellung der kritischen Merkmale ist es von besonderer Wichtigkeit, dass die Anforderungen an die COTS-Komponenten (einschließlich Anforderungen an Hardware, Software, Mensch-Maschine-Schnittstelle, Qualität und Zuverlässigkeit) vollständig definiert werden.

Zu den physikalischen Merkmalen gehören laut /EPR 96/ beispielsweise Merkmale zur Identifikation der COTS-Komponenten (z. B. Modelnummer, Firmwareversion, Softwareversion, Hardwareversion), Merkmale zu physikalischen Eigenschaften der COTS-Komponenten wie Abmessungen, Montagemöglichkeiten oder Stromverbrauch sowie Merkmale zu Schnittstellen (z. B. Signale, Kommunikation, Mensch-Maschine-Schnittstelle). Die meisten dieser Merkmale werden durch Inspektion und Messung verifiziert und die Überprüfungsmethoden sind für analoge Komponenten größtenteils identisch zu denen programmierbarer oder rechnerbasierter Komponenten. Unterschiede gibt es beispielsweise in der Notwendigkeit der Prüfung der Software- und Firmware-Revisionen bei programmierbaren oder rechnerbasierten Komponenten.

Die Leistungsmerkmale umfassen laut /EPR 96/ z. B. die von den COTS-Komponenten geforderte Funktionalität (z. B. Eingabeverarbeitung, spezifische Funktionen, Ausgangssignale, Funktionen zu Test und Diagnose) und die mit dieser Funktionalität verbundenen Leistungsmerkmale (z. B. Reaktionszeit, Genauigkeit, Stabilität, Datenrate). Zu den Leistungsmerkmalen gehören außerdem Umgebungsbedingungen (z. B. Temperatur, Feuchtigkeit, Seismik, elektromagnetische Verträglichkeit) in Bezug auf die erforderliche Leistung (z. B. Erfüllung von Anforderungen an die Genauigkeit bei bestimmten Umgebungstemperaturen). Weitere mögliche Leistungsmerkmale sind Anforderungen an ein bestimmtes Komponentenverhalten unter bestimmten (fehlerhaften) Bedingungen, die Erkennung von Fehlern oder die Einnahme ausfallsicherer Modi unter bestimmten Umständen.

Die Zuverlässigkeitsmerkmale umfassen laut /EPR 96/ Eigenschaften, die nicht allein durch Inspektionen oder Tests verifiziert werden können und die in der Regel durch den Herstellungsprozess beeinflusst werden. Zu den Zuverlässigkeitsmerkmalen gehören beispielsweise die Zuverlässigkeit selbst und die eingebaute Qualität inklusive der Qualität des Designs, der Qualität des Entwicklungsprozesses, dem Qualitätsmanagement und Konfigurationsmanagement des Herstellers, den Testprogrammen des Herstellers, der Fehleranalyse (z. B. potentielle Fehlermodi der Hard- und Software), der Qualifikation und Erfahrung des Personals beim Hersteller, die Berücksichtigung der Betriebserfahrung der Komponenten, die Herstellerunterstützung und die Rückverfolgbarkeit der Komponenten. Diese werden stark von dem Verfahren und dem Personal beeinflusst, welches der Hersteller für Konzeption, Entwicklung, Verifizierung und Validierung einsetzt. Insbesondere bei rechnerbasierten Komponenten sind diese Merkmale wichtig. Hohe Qualität lässt sich beispielsweise durch einen systematischen Lebenszyklus erreichen, der von den Anforderungen bis zur Implementierung reicht und diverse Verifizierungs- und Validierungsschritte enthält sowie eine angemessene Dokumentation umfasst.

Zur Überprüfung der kritischen Merkmale stehen vier Akzeptanzmethoden zur Verfügung. Die erste Methode „Spezielle Tests und Inspektionen“ (Special Tests and Inspections) umfasst Aktivitäten in Form spezieller Tests und Inspektionen, die nach dem Erhalt der COTS-Komponenten durchgeführt werden. Es handelt sich um Prüfungen und Tests der COTS-Komponenten, wobei diese bereits als Teil des Lieferprozesses stattfinden können. Es sind aber auch Tests eingeschlossen, die nach der Installation der Komponenten in der vorgesehenen Zielanwendung durchgeführt werden. Die zweite Methode „Überprüfung des Herstellers“ (Commercial Grade Survey of Supplier) beschreibt eine leistungsbasierte Bewertung des Herstellers der COTS-Komponenten. Sie wird durchgeführt, um die Angemessenheit der Qualitätskontrollen des Herstellers zu bestimmen, die in direktem Zusammenhang mit der Erfüllung der kritischen Merkmale der COTS-Komponenten stehen. Die dritte Methode „Überprüfung der Herkunft“ (Source Verification) beschreibt eine Prüfung der COTS-Komponenten im Werk des Herstellers, die vor dem Versand stattfindet. Dies kann z. B. dazu dienen, den Herstellungsprozess an verschiedenen Stellen zu überwachen, beim Hersteller durchgeführte Tests zu bezeugen oder technische Arbeiten zu prüfen. Die vierte Methode „Leistungsnachweis für Hersteller/Komponenten“ (Acceptable Supplier/Item Performance Record) beinhaltet die Verwendung dokumentierter Aufzeichnungen der Betriebserfahrung der COTS-Komponenten. Dadurch sollen Informationen als Grundlage für die Qualifizierung der

COTS-Komponenten erhalten werden. In der Regel wird diese Methode nicht allein verwendet, sondern in Kombination mit einer oder mehrerer der anderen Methoden.

Laut /EPR 96/ ist zu beachten, dass alle kritischen Merkmale verifiziert werden müssen, d. h. jedes dieser Merkmale sollte eine Anforderung darstellen, die erfüllt werden muss, um zu gewährleisten, dass die Komponenten ihre Sicherheitsfunktionen erfüllen. Außerdem muss der Satz kritischer Merkmale, der letztendlich abgeleitet wird, alle Anforderungen abdecken, die erforderlich sind, um hinreichend zu gewährleisten, dass die COTS-Komponenten ihre Sicherheitsfunktionen erfüllen. Die Tiefe der Bewertung von COTS-Komponenten hängt von verschiedenen Faktoren ab und ist für die zu bewertenden COTS-Komponenten in Abhängigkeit von der sicherheitstechnischen Bedeutung der späteren Zielanwendung und der Komplexität der COTS-Komponenten zu bestimmen. Ebenfalls beitragender Faktor zur Tiefe der Bewertung und der Notwendigkeit weiterer Tests und Prüfungen ist die Verfügbarkeit von und der Zugang zu (oft geschützten) Informationen des Herstellers.

**Nutzung einer bereits vorhandenen Zertifizierung**

Im Regulatory Guide RG 1.250 /NRC 22/ wird ausgesagt, dass der im Bericht NEI 17-06 des Nuclear Energy Institutes beschriebene Prozess zur Nutzung einer bereits vorhandenen Zertifizierung nach IEC 61508 zur Qualifizierung von COTS-Komponenten genutzt werden kann. Der Bericht des Nuclear Energy Institutes (NEI) 17-06 „Guidance on Using IEC 61508 SIL Certification to Support the Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Related Applications“ /NEI 19/ bietet einen Ansatz zur Beschaffung und Qualifizierung von COTS-Komponenten mit einer SIL-Zertifizierung, um diese in sicherheitstechnisch wichtigen Funktionen in Kernkraftwerken einsetzen zu können. Ziele der Verwendung SIL-zertifizierter COTS-Komponenten sind laut /NEI 19/ eine verbesserte Standardisierung bei der Bewertung der Komponentenqualität, geringere Kosten bei der Beschaffung von Komponenten sowie eine größere Auswahl an geeigneten Herstellern, ohne dabei die Sicherheit zu beeinträchtigen.

/NEI 19/ legt Kriterien fest, bei deren Vorhandensein sich auf den SIL-Zertifizierungsprozess verlassen werden kann, um COTS-Komponenten, die einen SIL-Zertifizierungsprozess durchlaufen haben, in sicherheitstechnisch wichtigen Funktionen in Kernkraftwerken verwenden zu können. Unter Verwendung der in /NEI 19/ beschriebenen Methode ist dann keine weitere Untersuchung der COTS-Komponenten (Commercial

Grade Dedication) mehr notwendig. Bei den Stellen, welche die SIL-Zertifizierung durchführen, muss es sich um akkreditierte Stellen handeln. Laut U.S. NRC /NRC 22/ reicht die Inanspruchnahme einer Zertifizierungsstelle und die Verifizierung der Zertifizierung nach entsprechender SIL-Klassifikation aus, um die kritischen Merkmale zur Verwendung der in EPRI TR-106439 /EPR 96/ beschriebenen Methode zu verifizieren.

Laut /NEI 19/ muss der Hersteller zur Akzeptanz der SIL-Zertifizierung die COTS-Komponenten konform zu den Anforderungen der IEC 61508 produzieren. Die IEC 61508 bietet einen generischen, risikobasierten Ansatz zur Qualifizierung elektrischer, elektronischer oder programmierbarer elektronischer Komponenten, die zur Ausführung von Sicherheitsfunktionen verwendet werden sollen, wobei der gesamte Lebenszyklus berücksichtigt wird. In der IEC 61508 wird beispielsweise die Anwendung strenger Entwicklungsprozesse gefordert, wie z. B. die Definition der Anforderungen an die Komponenten, die Dokumentation des Hardware- und Softwareentwurfs sowie die Verifizierung und Validierung. Außerdem fordert die IEC 61508 den Einsatz von Fehleranalysen, um Funktionen wie Selbstdiagnose, Fehlertoleranz, Fehlerbehebung, Fail-Safe-Verhalten und Toleranz gegen Umwelteinflüsse einzubeziehen. Zur Erreichung eines bestimmten Maßes an Zuverlässigkeit ist bei der Herstellung von Komponenten in Konformität zur IEC 61508 darauf zu achten, bewährte Teilkomponenten zu verwenden, Sicherheitsspielräume einzubauen und fehlertolerante Architekturen zu verwenden.

Die nach IEC 61508 hergestellten Komponenten sind laut /NEI 19/ dann durch eine Third-Party-Organisation (Zertifizierungsstelle) daraufhin zu überprüfen, ob bei der Herstellung der Komponenten die Anforderungen der IEC 61508 tatsächlich eingehalten wurden. Durch die Zertifizierungsstelle sind die Dokumentation, der Hersteller und die Komponenten hinsichtlich der Erfüllung der Anforderungen der IEC 61508 zu bewerten. Der dabei verwendete Prozess hat laut /NEI 19/ Besuche und Audits der Fertigungsstätten des Herstellers, die Überprüfung der Konstruktionsunterlagen sowie eine Verifizierung der Berechnungen und technischen Bewertungen zu umfassen. Zudem werden von der Zertifizierungsstelle Daten aus der Betriebserfahrung, wie z. B. tatsächliche Ausfallraten, ausgewertet. Anschließend wird durch die Zertifizierungsstelle das SIL-Zertifikat ausgestellt oder es werden zu behebende Lücken aufgezeigt, um ein solches ausstellen zu können. Je nach sicherheitstechnischer Bedeutung der Funktion, in welcher die Komponente später eingesetzt werden soll, sind unterschiedliche Sicherheitsniveaus der SIL-Zertifizierung (SIL 1 bis SIL 4) möglich.

Um sicherzustellen, dass die Zertifizierungsstelle glaubwürdig ist, ist diese durch eine nationale Akkreditierungsstelle zu akkreditieren. Dazu werden von der Akkreditierungsstelle Audits durchgeführt und die Tätigkeiten der Zertifizierungsstelle überwacht. Damit wird sichergestellt, dass die Prozesse und Verfahren der Akkreditierungsstelle sowie die entsprechende Umsetzung der ISO 17065 entsprechen. /NEI 19/

Des Weiteren wird in /NEI 19/ auf eine Untersuchung von EPRI eingegangen, in deren Rahmen Informationen und Daten von Personen und Organisationen gesammelt wurden, die Kenntnisse hinsichtlich der SIL-Zertifizierung von Komponenten und der Akkreditierung von Zertifizierungsstellen hatten. Außerdem wurde die tatsächliche Betriebserfahrung von SIL-zertifizierten Komponenten ins Verhältnis mit der im Zertifizierungsprozess behaupteten Zuverlässigkeit gesetzt, um zu bestimmen, ob die Angaben übereinstimmen. Laut dieser EPRI-Untersuchung zeigen SIL-zertifizierte Komponenten ein hohes Maß an Zuverlässigkeit von Hardware und Software. Als grundlegende Norm für die funktionale Sicherheit und die SIL-Zertifizierung wurde die IEC 61508 herausgestellt. In /NEI 19/ wird ausgesagt, dass der Einsatz von nach IEC 61508 SIL-zertifizierten Komponenten in Verbindung mit einer anwendungsspezifischen Funktions- und Umgebungsqualifizierung eine erhebliche Verbesserung der Zuverlässigkeit und Senkung der Kosten bewirkt. Auf Basis der EPRI-Untersuchung wird in /NEI 19/ der Schluss gezogen, dass der SIL-Zertifizierungsprozess nach IEC 61508 die Bewertung der in /EPR 96/ festgelegten kritischen Merkmale umfasst. SIL-Zertifizierungen können somit als Nachweis für die Erfüllung der in /EPR 96/ definierten kritischen Merkmale verwendet werden. Die Begründung hierfür ist, dass die Ziele sowohl bei der Vorgehensweise nach /EPR 96/ als auch bei der SIL-Zertifizierung darin bestehen, dass die Komponenten ihre Sicherheitsfunktionen immer korrekt erfüllen und das sowohl Endnutzer als auch Aufsichtsbehörde Vertrauen in die korrekte Funktion der Komponenten haben. Durch diese Gemeinsamkeit gibt es laut /NEI 19/ für die Nuklearindustrie ein großes Potenzial, COTS-Komponenten zu verwenden, die gemäß IEC 61508 entwickelt und hergestellt wurden.

# 3 Entwicklung eines Ansatzes zur Bewertung des Einsatzes von COTS-Komponenten

In diesem Kapitel werden die Ergebnisse der Arbeiten zu Arbeitspaket 2 dargestellt. Die Zielsetzung der Arbeiten im Arbeitspaket 2 war die Entwicklung eines Ansatzes zur Bewertung des Einsatzes von COTS-Komponenten in sicherheitstechnisch wichtigen elektro- und leittechnischen Einrichtungen in kerntechnischen Anlagen. Dazu wurden die in Arbeitspaket 1 ermittelten Erkenntnisse und Anforderungen hinsichtlich des Einsatzes und der Qualifizierung von COTS-Komponenten bezüglich verschiedener Aspekte zusammengefasst und mit Anforderungen aus dem nationalen kerntechnischen Regelwerk hinsichtlich dieser Aspekte verglichen. Darauf aufbauend wurde ein Ansatz zur Bewertung des Einsatzes von COTS-Komponenten entwickelt, dessen Grundlage ebenfalls die folgenden Aspekte sind:

- Auswahl und Beschaffung von COTS-Komponenten
- Qualitätsmanagement des Herstellers und dessen Zulieferer
- Design- und Entwicklungsprozess der COTS-Komponenten
- Komplexität der COTS-Komponenten
- Technische Eigenschaften und Einsatzort bzw. -art der COTS-Komponenten
- Qualifizierung von COTS-Komponenten
- Möglichkeiten zur Fehlererkennung und Fehlervermeidung
- Änderungsmanagement
- Wartung und Instandhaltung
- Dokumentation

Da die Anforderungen für elektro- und leittechnische Einrichtungen in Abhängigkeit von ihrer sicherheitstechnischen Bedeutung (Kategorie A, B oder C nach DIN EN 61226 /DIN 10a/) unterschiedlich sind, wurden in dem Bewertungsansatz die drei Kategorien A, B und C berücksichtigt. Pro betrachteten Aspekt wurden für den Bewertungsansatz fünf Anforderungen formuliert. In Abschnitt 3.1 werden die Anforderungen an elektro- und leittechnische Komponenten zu den betrachteten Aspekten aus dem natio-

nalen kerntechnischen Regelwerk zusammengefasst. Der entwickelte Bewertungsansatz hinsichtlich des Einsatzes von COTS-Komponenten in elektro- und leittechnischen Einrichtungen in kerntechnischen Anlagen findet sich in Abschnitt 3.2.

## 3.1 Anforderungen an elektro- und leittechnische Komponenten aus dem nationalen kerntechnischen Regelwerk

Zur Sammlung der Anforderungen an elektro- und leittechnische Komponenten aus dem nationalen kerntechnischen Regelwerk wurden diverse nationale kerntechnische Regelwerke hinsichtlich der genannten Aspekte ausgewertet. Folgende Regelwerke wurden betrachtet:

- „Sicherheitsanforderungen an Kernkraftwerke“ /BMU 22/
- „Interpretationen zu den Sicherheitsanforderungen an Kernkraftwerke“ /BMU 15/
- KTA 3501 „Reaktorschutzsystem und Überwachungseinrichtungen des Sicherheitssystems“ /KTA 15a/
- KTA 3503 „Typprüfung von elektrischen Baugruppen der Sicherheitsleittechnik“ /KTA 15b/
- KTA 3507 „Werksprüfungen, Prüfungen nach Instandsetzung und Nachweis der Betriebsbewährung der Baugruppen und Geräte der Sicherheitsleittechnik“ /KTA 14a/
- KTA 3701 „Übergeordnete Anforderungen an die elektrische Energieversorgung in Kernkraftwerken“ /KTA 14b/
- KTA 3901 „Kommunikationseinrichtungen für Kernkraftwerke“ /KTA 17/
- KTA 3903 „Prüfung und Betrieb von Hebezeugen in Kernkraftwerken“ /KTA 20/
- DIN EN 60880 „Kernkraftwerke, Leittechnik für Systeme mit sicherheitstechnischer Bedeutung, Softwarefunktionen für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie A“ /DIN 10b/
- DIN EN 61513 „Kernkraftwerke, Leittechnik für Systeme mit sicherheitstechnischer Bedeutung, Allgemeine Systemanforderungen“ /DIN 13/

Diese Regelwerke wurden hinsichtlich der genannten Aspekte ausgewertet. In den nachfolgenden Abschnitten wird kurz auf die Inhalte der ausgewerteten nationalen kerntechnischen Regelwerke bezüglich der betrachteten Aspekte eingegangen.

### 3.1.1 Sicherheitsanforderungen an Kernkraftwerke

Die „Sicherheitsanforderungen an Kernkraftwerke“ /BMU 22/ enthalten grundsätzliche und übergeordnete sicherheitstechnische Anforderungen im Rahmen des untergesetzlichen Regelwerks, die die nach dem Stand von Wissenschaft und Technik erforderliche Vorsorge gegen Schäden durch die Errichtung und den Betrieb von Kernkraftwerken konkretisieren. Um den Einschluss radioaktiver Stoffe im Kernkraftwerk und die Abschirmung der von diesen Stoffen ausgehenden Strahlung sicherzustellen, wird ein Sicherheitskonzept umgesetzt, bei dem Maßnahmen und Einrichtungen gestaffelten Sicherheitsebenen zugeordnet sind.

In /BMU 22/ werden allgemeine, übergeordnete Anforderungen definiert, die auch auf elektro- und leittechnische Komponenten übertragen werden können. Laut /BMU 22/ sind Tests bzw. Prüfungen der Komponenten unter Einsatzbedingungen und für alle relevanten Betriebsphasen durchzuführen. Dabei sind geeignete und bewährte Prüfverfahren anzuwenden. Es ist sicherzustellen, dass die Komponenten für die geplanten Einsatzbedingungen und die vorgesehene Betriebszeit keine inakzeptable Ausfallrate zeigen. Eine gewisse Ausfallrate lässt sich jedoch aufgrund von Alterungsprozessen und zufälligen, statistisch verteilten Ausfällen von Komponenten nicht vermeiden. Um zu gewährleisten, dass diese Ausfallrate beherrschbar ist und keine Gefährdung für die Erfüllung der Sicherheitsanforderungen darstellt, sind laut /BMU 22/ diverse Maßnahmen zu treffen. Beispielsweise sind für die geplanten Einsatzbedingungen und die vorgesehene Betriebszeit bereits bewährte Komponenten gegenüber anderen Komponenten vorzuziehen. Außerdem sind geeignete Sicherheitszuschläge bei der Auslegung von Komponenten in Abhängigkeit von ihrer sicherheitstechnischen Bedeutung umzusetzen und inhärent sicher wirkende Mechanismen bei der Auslegung von Komponenten zu bevorzugen. Zudem sind passive Sicherheitseinrichtungen gegenüber aktiven Sicherheitseinrichtungen vorzuziehen. Sicherheitsrelevante Systeme sind redundant, also in mehrfacher Ausführung, zu realisieren. Bei Ausfall einer oder mehrerer Redundanzen wird auf diese Weise die Sicherheitsfunktion über die verbliebenen, funktionsfähigen Redundanzen sichergestellt. Für die einzelnen Redundanzen ist das Prinzip der Diversität anzuwenden. Das bedeutet, dass in den zueinander redundanten Systemen sich in ihrer

Arbeitsweise voneinander unterscheidende Komponenten für die Realisierung der gleichen Funktionen einzusetzen sind (z. B. unterschiedliche Messverfahren, Auswertung von verschiedenen Parametern). Auf diese Weise wird dem potenziellen Ausfall mehrerer Redundanzen eines sicherheitsrelevanten Systems infolge gemeinsamer Fehlerursache entgegengewirkt. Des Weiteren sind redundante Teilsysteme zu entmaschen, soweit dieser Entmaschung keine sicherheitstechnischen Nachteile entgegenstehen und darüber hinaus sind die redundanten Teilsysteme entsprechend dem Wirkungsbereich möglicher versagensauslösender Ereignisse räumlich zu trennen. Teilsysteme oder Anlagenteile sollten außerdem ein sicherheitsgerichtetes Systemverhalten bei Fehlfunktion aufweisen.

Um betriebs- und alterungsbedingte Ausfälle zu vermeiden, wird in /BMU 22/ die Durchführung von wiederkehrenden Prüfungen in einem Umfang gefordert, der den Sicherheitsanforderungen gerecht wird. Zudem müssen die relevanten Betriebszustände in den jeweiligen Betriebsphasen überwacht werden. Die Entwicklung und Anwendung eines Überwachungskonzepts zur Erkennung und Beherrschung von betriebs- und alterungsbedingten Schädigungen sowie die Aufzeichnung und Auswertung von Betriebserfahrungen wird ebenfalls gefordert.

In /BMU 22/ sind zudem allgemeine Anforderungen an die Leittechnik enthalten. Es wird gefordert, dass die Anforderungen an Auslegung, Fertigung, Errichtung und Betrieb der Hardware sowie an Entwurf, Implementierung, Qualifizierung, Inbetriebsetzung, Betrieb und Modifizierung der Software entsprechend der sicherheitstechnischen Klassifizierung der von ihnen ausgeführten Funktionen festzulegen sind. Komponenten, die betriebliche Steuer- und Regelungsfunktionen in der Leittechnik der Sicherheitsebene 1 (bestimmungsgemäßer und ungestörter Normalbetrieb) wahrnehmen, sind so auszulegen und zu betreiben, dass auch ohne Inanspruchnahme von leittechnischen Einrichtungen der Sicherheitsebene 2 (Anomaler Betrieb) ein möglichst störungsfreier Betrieb der Anlage gewährleistet ist. Komponenten in der Leittechnik der Sicherheitsebene 2 müssen geeignet sein, bei Ereignissen der Sicherheitsebene 2 eine Anforderung der Schutzaktionen der Sicherheitsebene 3 (Störfälle) zu vermeiden.

Komponenten in der Leittechnik der Sicherheitsebene 3 müssen so ausgelegt sein, dass ihre Leittechnikfunktionen bei Erreichen festgelegter Ansprechwerte Schutzaktionen auslösen. Zusätzlich zu den übergeordneten technischen Anforderungen müssen Komponenten in der Leittechnik der Sicherheitsebene 3 laut /BMU 22/ eine selbsttätige Über-

wachung auf einen möglichen Ausfall hin besitzen. Außerdem müssen sie für die möglichen Umgebungsbedingungen ausgelegt sein und eine eventuell vorhandene Software muss einfach strukturiert sein. Zudem ist der Funktionsumfang von Hard- und Software auf das sicherheitstechnisch notwendige Maß zu reduzieren. Der Einsatz fehlervermeidender, fehlerentdeckender und fehlerbeherrschender Maßnahmen und Einrichtungen ist umzusetzen und auch beim Eintreten eines zu unterstellenden Einzelfehlers dürfen keine Aktionen ausgelöst werden, die zu einem Störfall führen können oder die Störfallbeherrschung verhindern. Laut /BMU 22/ ist unter Berücksichtigung der verfahrenstechnischen Vorgaben zu analysieren, welche Potentiale für das systematische Versagen der leittechnischen Einrichtungen auf die Ereignisabläufe in der Sicherheitsebene 3 bestehen und welche Auswirkungen sich daraus ergeben. Anhand dieser Analysen sind entsprechende Vorkehrungen gegen systematisches Versagen zur Minderung von dessen Eintrittswahrscheinlichkeit zu treffen, und zwar derart, dass es auf der Sicherheitsebene 3 nicht mehr unterstellt werden muss.

In /BMU 22/ werden außerdem übergeordnete Anforderungen an die elektrische Energieversorgung gestellt, die auch für elektro- und leittechnische Komponenten zu erfüllen sind. Beispielweise sind Komponenten, die elektrische, elektromechanische oder elektromagnetische Bauteile sowie einfach aufgebaute analoge, elektronische Baugruppen enthalten, auf mögliche systematische Ausfälle dieser Komponenten zu analysieren. Dabei müssen Vorkehrungen zur Verminderung der Eintrittswahrscheinlichkeit systematischer Ausfälle getroffen werden, die gewährleisten, dass ein systematischer Ausfall nicht mehr unterstellt werden muss oder aber die Auswirkungen systematischer Ausfälle beherrschbar sind. Für den Fall, dass die Komponenten programmierbare oder nicht programmierbare komplexe elektronische Baugruppen enthalten, müssen fehlervermeidende und fehlerbeherrschende Maßnahmen auf Komponentenebene sowie gegebenenfalls fehlerbeherrschende Vorkehrungen auf Systemebene getroffen werden, damit redundanzübergreifende systematische Ausfälle auf Systemebene der jeweils betroffenen Sicherheitsebene verhindert werden.

### 3.1.2 Interpretationen zu den Sicherheitsanforderungen an Kernkraftwerke

Da die „Sicherheitsanforderungen an Kernkraftwerke“ /BMU 22/ Interpretationsspielräume offenlassen, die zu Schwierigkeiten bezüglich der Auslegung und Anwendung führen können, wurden die „Interpretationen zu den Sicherheitsanforderungen an Kernkraftwerke“ /BMU 15/ verfasst. Diese sollen die Spielräume durch erläuternde und konkretisierende Interpretationen schließen. In /BMU 15/ werden allgemeine, übergeordnete

Anforderungen definiert, die auch auf elektro- und leittechnische Komponenten übertragen werden können. Dabei werden Leittechnik-Funktionen gemäß ihrer sicherheitstechnischen Bedeutung unterschiedlichen Sicherheitskategorien zugeordnet, für die abgestufte Anforderungen gelten. Leittechnik-Funktionen der Kategorie A sind alle Funktionen, die erforderlich sind, um Ereignisse der Sicherheitsebene 3 zu beherrschen. Leittechnik-Funktionen der Kategorie B sind alle Funktionen, die erforderlich sind, um Ereignisse der Sicherheitsebene 2 zu beherrschen und um den Eintritt von Ereignissen der Sicherheitsebene 3 zu vermeiden. Alle übrigen sicherheitstechnisch wichtigen Leittechnik-Funktionen werden der Kategorie C zugeschrieben.

Hinsichtlich Anforderungen an die Auslegung leittechnischer Komponenten der Kategorien A bis C wird in /BMU 15/ ausgesagt, dass grundsätzlich auf ihre Eignung geprüfte oder für den Einsatzfall und für die unterstellten Einsatzbedingungen betriebsbewährte Hardware und Software zu verwenden ist. Die Hardware soll während des Leistungsbetriebs wartungsfrei sein. Wenn Komponenten ihre auslegungsgemäßen Funktionen auch unter Störfallbedingungen ausführen müssen, dann ist die Störfallfestigkeit der betreffenden Komponenten nachzuweisen. Werden gleiche Komponenten für Leittechnik-Funktionen verwendet, die zu unterschiedlichen Sicherheitskategorien gehören, dann müssen die Komponenten nach den Anforderungen ausgelegt werden, die sich durch die Kategorie mit der höchsten sicherheitstechnischen Bedeutung ergeben. Zudem sind die Komponenten vor unzulässiger Beeinflussung der Signale durch anlageninterne und externe Störquellen zu schützen. Die Anforderungen an Unabhängigkeit und Beherrschung von Fehlerkombinationen darf nicht unzulässig beeinträchtigt werden. Es müssen Maßnahmen getroffen werden und Einrichtungen vorhanden sein, um die Funktionsfähigkeit der Komponenten zu überprüfen und ihren Zustand zu überwachen.

Hinsichtlich Komponenten, die Leittechnik-Funktionen der Kategorie A ausführen, wird in /BMU 15/ gefordert, dass diese grundsätzlich so auszulegen sind, dass sie ihre Aufgaben im Anforderungsfall während eines Zufallsausfalls durch einen Einzelfehler und einem systematischen Ausfall und Folgeausfällen und einem Instandhaltungsfall erfüllen. Bei der Auslegung von Komponenten sind versagensauslösende Ereignisse innerhalb und außerhalb des Sicherheitssystems zu berücksichtigen und die Komponenten sind vor unzulässigen Eingriffen zu schützen. Komponenten, die Leittechnik-Funktionen der Kategorie A übernehmen, sind laut /BMU 15/ stets selbstüberwachend auszulegen. Die Funktionen, die nicht von der Selbstüberwachung erfasst werden, sind regelmäßig

und lückenlos zu überprüfen. Grundsätzlich sind diversitäre rechnerbasierte oder programmierbare Komponenten zu verwenden, wobei es keine Vorgaben bezüglich des Einsatzes diversitärer Komponenten gibt, wenn für die auszuführende Leittechnik-Funktion ein aktiver systematischer Ausfall sicherheitsgerichtet ist. Erfüllen die Komponenten Schutzfunktionen, die nicht für jeden Anlagenzustand sicherheitsgerichtet sind, ist in Abhängigkeit von den Auswirkungen von passiven oder aktiven systematischen Ausfällen der Komponenten eine zweifach oder dreifach diversitäre Ausführung umzusetzen. Sind Komponenten für die Funktionsfähigkeit des Sicherheitssystems nach Eintritt von Ereignissen der Sicherheitsebene 3 vorgesehen, dann sind diese laut /BMU 15/ so auszulegen, dass sie den jeweils ungünstigsten Umgebungs- und Störfallbedingungen widerstehen, die im zugehörigen Aufstellungs- und Installationsbereich auftreten können.

Hinsichtlich Komponenten, die Leittechnik-Funktionen der Kategorie B ausführen, wird in /BMU 15/ gefordert, dass diese so auszulegen sind, dass sie ihre Aufgaben auch dann erfüllen, wenn im Anforderungsfall zusätzlich ein Zufallsausfall und daraus resultierende Folgeausfälle eintreten. Komponenten zur Ausführung von Leittechnik-Funktionen bei Notstandsfällen und auf den Sicherheitsebenen 4b (Ereignisse mit Mehrfachversagen von Sicherheitseinrichtungen) oder 4c (Unfälle mit schweren Brennelementschäden) müssen laut /BMU 15/ so ausgelegt werden, dass sie unter den für die jeweilige Aufgabe zu unterstellenden Umgebungsbedingungen ihre Aufgaben mit der für diese Sicherheitsebenen jeweils ausreichenden Zuverlässigkeit erfüllen.

Hinsichtlich der Qualifizierung der für Leittechnik-Funktionen eingesetzten Hard- und Software wird in /BMU 15/ für allen Phasen der Entwicklung, Herstellung, Inbetriebnahme und während des Betriebs gefordert, dass analytische Maßnahmen, inklusive praktischer Prüfungen, zur Qualitätssicherung hinsichtlich der zu erfüllenden leittechnischen Anforderungen durchzuführen sind. Die dabei durchgeführten Tests und Prüfungen sind unter möglichst realistischen Einsatzbedingungen durchzuführen und es muss sichergestellt werden, dass alle zu unterstellenden Ereignisabläufe beherrscht werden. Speziell hinsichtlich der Qualifizierung der für Leittechnik-Funktionen eingesetzten Hardware wird in /BMU 15/ gefordert, dass für die erforderlichen Leittechnik-Funktionen der Kategorien A und B zuverlässige, typgeprüfte oder für die unterstellten Einsatzbedingungen betriebsbewährte Hardware zu verwenden ist. Diese Hardware sollte während des Leistungsbetriebs wartungsfrei sein. Bezüglich der Leittechnik-Funktionen der Kategorie C ist zuverlässige und für die unterstellten Einsatzbedingungen geeignete Hardware

einzusetzen. Speziell hinsichtlich der Qualifizierung der für Leittechnik-Funktionen eingesetzten Software wird in /BMU 15/ gefordert, dass Software, die für leittechnische Funktionen eingesetzt werden soll, in verifizierbaren Schritten nach einem Phasenmodell entwickelt werden muss. Die Software ist so zu gestalten, dass ihr anforderungsgerechter Ablauf unabhängig von Art und Umfang der zeitlichen Änderung ihrer Eingangssignale ist. Eine Rückwirkung von leittechnischen Einrichtungen, die Leittechnik-Funktionen einer sicherheitstechnisch niederwertigen Kategorie ausführen, auf leittechnische Einrichtungen, die Leittechnik-Funktionen einer sicherheitstechnisch höherwertigen Kategorie realisieren, ist auszuschließen.

In /BMU 15/ werden Anforderungen an die für Leittechnik-Funktionen der Kategorie A eingesetzte Software gestellt. Beispielsweise wird ein einfacher und robuster Aufbau der Software mit klar abgegrenzten Einheiten in einer übersichtlichen Programmstruktur und Reduktion des Funktionsumfangs auf das für den Einsatzfall erforderliche Maß gefordert. Zudem wird der Entwurf nach einem Phasenmodell und die Implementierung der Software mit formalisierten und rechnergestützten Konstruktions-, Analyse- und Prüfmethoden gemäß dem aktuellen Stand von Wissenschaft und Technik verlangt. Das anforderungsgerechte Verhalten des Hard- und Softwaresystems nach Installation der Software muss validiert werden und eine durchgängige Nachweisführung der korrekten Arbeitsweise der Software ist zu realisieren.

Für in Leittechnik-Funktionen der Kategorie B eingesetzte Software wird in /BMU 15/ gefordert, dass diese einfach und robust in einer übersichtlichen Programmstruktur aufgebaut und dass der Funktionsumfang auf das für den Einsatzfall erforderliche Maß reduziert sein muss. Die Entwicklung der Software muss nach einem Phasenmodell und weitgehend mit rechnergestützten Werkzeugen erfolgen. Zur Entwicklung und Qualifizierung der Software sind Beschreibungen sowie rechnergestützte Testverfahren anzuwenden, die die korrekte Arbeitsweise sicherstellen. Zudem muss das anforderungsgerechte Verhalten des Hard- und Softwaresystems nach Installation der Software validiert werden.

Hinsichtlich der für Leittechnik-Funktionen der Kategorie C eingesetzten Software wird in /BMU 15/ gefordert, dass bei der Entwicklung der Software die einzelnen Entwicklungsschritte ausgewiesen werden müssen und, wenn möglich, bei wesentlichen Entwicklungsschritten Softwarewerkzeuge verwendet werden sollen. Das Erreichen der Entwicklungsziele ist nach jedem Schritt durch Prüfungen nachzuweisen und zu doku-

mentieren. Die Software muss nach dem anerkannten Stand der Technik qualifiziert werden. Zudem muss die Software nach einem Qualitätssicherungsplan gemäß den anerkannten Regeln der Technik erstellt werden.

### 3.1.3 KTA 3501

Die Regeln des Kerntechnischen Ausschusses KTA legen sicherheitstechnische Anforderungen fest, bei deren Einhaltung nach dem aktuellen Stand von Wissenschaft und Technik die Vorsorge gegen Schäden durch die Errichtung und den Betrieb von kerntechnischen Anlagen sichergestellt ist. Damit sollen die im Atomgesetz und in der Strahlenschutzverordnung festgelegten sowie in den „Sicherheitsanforderungen an Kernkraftwerke“ /BMU 22/ und den „Interpretationen zu den Sicherheitsanforderungen an Kernkraftwerke“ /BMU 15/ weiter konkretisierten Schutzziele erreicht werden. In der Regel KTA 3501 /KTA 15a/ werden die Anforderungen an das Reaktorschutzsystem, die Schutzbegrenzungen, die Zustandsbegrenzungen und an die Überwachungseinrichtungen des Sicherheitssystems beschrieben. Dabei werden unter anderem Anforderungen bezüglich fehlervermeidender Maßnahmen und der Auslegung leittechnischer Einrichtungen der Kategorien A und B definiert.

Hinsichtlich fehlervermeidender Maßnahmen für rechnerbasierte Funktionseinrichtungen der Kategorie A wird in /KTA 15a/ gefordert, dass die rechnerbezogene Bearbeitung der Anwenderfunktionen und die Datenübertragung in festen Zeitzyklen erfolgen muss. Bei der Datenübertragung über einen Datenbus müssen alle Daten zyklisch übertragen werden, unabhängig davon, ob sie sich geändert haben. Zudem dürfen alle Rechner und Datenbusse im Auslösepfad lediglich indirekte Datenbusverbindungen nach außen über einen Schnittstellenrechner haben, der eine leittechnische Einrichtung der Kategorie A ist und keine direkten Datenbusverbindungen nach außen hat. Alle Rechner im Auslösepfad sind mit einem Schnittstellenrechner in der gleichen leittechnischen Redundanz verbunden, der die Datenverbindung nach außen ermöglicht. Mit „außen“ sind damit Wartungsrechner, Prozessrechneranlage des Kraftwerks und gegebenenfalls weitere funktionsbezogene Rechner gemeint. Außerdem darf die Programmierung von Rechnern im Auslösepfad im Betriebsmodus nicht ermöglicht werden. Der Funktionsumfang von Einrichtungen der Kategorie A ist zudem auf die notwendigen Aufgaben zu beschränken.

In /KTA 15a/ werden Anforderungen an elektro- und leittechnische Komponenten festgelegt, die leittechnische Funktionen der Kategorien A und B ausführen. Die Komponenten müssen bezüglich ihrer statischen und dynamischen Eigenschaften den Anforderungen der umzusetzenden Leittechnikfunktion der Kategorie A bzw. B genügen. Zudem müssen die Komponenten für die geplante Einsatzumgebung ausgelegt sein. Es müssen bewährte und zuverlässige Bauteile und Schaltungen verwendet werden, wobei deren Betriebserfahrungen zu beachten sind. Außerdem müssen die Komponenten so ausgelegt sein, dass eine Prüfung ihrer Funktion ohne einen Eingriff in die Signalführung/Verdrahtung möglich ist. Insbesondere für Komponenten zur Ausführung von leittechnischen Funktionen der Kategorie A gilt, dass das Schaltungskonzept einfach und übersichtlich sein sowie dem gewünschten Einsatzzweck entsprechen muss.

### 3.1.4 KTA 3503

In der Regel KTA 3503 /KTA 15b/ werden die Anforderungen an die Typprüfung von elektrischen Baugruppen der Sicherheitsleittechnik beschrieben. Dabei werden allgemeine Anforderungen bezüglich der erforderlichen Typprüfungen von Komponenten, die in der Sicherheitsleittechnik eingesetzt werden, definiert. Hinsichtlich des Prüfverfahrens wird in /KTA 15b/ beschrieben, dass eine Typprüfung die Prüfung der im Datenblatt und in der Funktionsbeschreibung einer Komponente spezifizierten Eigenschaften an für die Typenreihe der Komponente repräsentativen Mustern ist. Sie dient dazu, die Eignung der bei der Herstellung der Komponente umgesetzten Qualitätssicherungsmaßnahmen zu bewerten. Die Qualitätssicherungsmaßnahmen sind anhand von Auditberichten zu durchgeführten Qualitätsaudits nachvollziehbar zu bewerten. Reichen die Auditberichte nicht aus, dann müssen die Qualitätsnachweise im Rahmen der Typprüfung erbracht werden. Die Typprüfung ist in theoretische und praktische Prüfungen zu unterteilen. Liegen Betriebserfahrungen und die Ergebnisse bereits durchgeführter Prüfungen vor, dann dürfen diese bei der Typprüfung unter der Voraussetzung berücksichtigt werden, dass die sicherheitstechnischen Anforderungen erfüllt werden. Bei rechnerbasierten Komponenten sind theoretische Prüfungen der Software und ihrer Qualitätsmerkmale sowie praktische Prüfungen der Funktion durchzuführen. An die Schnittstellen der Prüflinge sind die gleichen Anforderungen zu stellen wie an die Prüflinge selbst.

Bei theoretischen Prüfungen handelt es sich laut /KTA 15b/ um die Prüfung der Unterlagen, der vorzulegenden Nachweise sowie der Prüfanweisungen und des Prüfprogramms, die die zu prüfende Komponente betreffen. Die Unterlagen müssen Angaben über Hersteller, Typ und Änderungszustand der betreffenden Komponente enthalten.

Benötigte Unterlagen sind z. B. die Funktionsbeschreibung, das Datenblatt (muss alle Daten einschließlich der zulässigen Bereiche und Toleranzen enthalten) sowie die Gebrauchsanweisung bzw. das Handbuch mit Angaben zu Einbau, Inbetriebsetzung, Einstellung, Sonderzubehör, Wartung, Verpackung, Transport und Lagerung. Zudem werden Hardwareunterlagen mit Stromlaufplänen, Stücklisten, Datenblättern der verbauten Bauelemente, Lagepläne der Bauelemente und Bestückungsvarianten sowie Software-Unterlagen zum Software-Entwicklungsprozess, Funktionsablauf, Zeitverhalten, Konfigurierungs- und Parametrisierungsmöglichkeiten bzw. Konfigurierungs- und Parametrisierungsbedingungen inklusive dafür vorhandener Software-Werkzeuge, Schnittstellenspezifikationen, Qualifizierungs- oder Eignungsnachweisverfahren bei vorgefertigter Software, Möglichkeiten zum Schutz gegen Eingriffe in die Software inklusive der Erfassung, Meldung und Protokollierung von Eingriffen benötigt. Zudem werden Unterlagen zu den Selbstüberwachungsmechanismen der Hard- und Software benötigt, die mindestens deren Spezifikation, die Spezifikation des Verhaltens der Komponente bei einem Ansprechen der Überwachung sowie eine Analyse der implementierten Selbstüberwachungsfunktionen hinsichtlich ihres Abdeckungsgrades bei der Überwachung der sicherheitstechnisch wichtigen Funktionen beinhalten. Alle Unterlagen müssen für die Verifizierung der Wirksamkeit der Mechanismen geeignet sein. Die Ermittlung der Zuverlässigkeitsangaben ist auf Grundlage der vorgelegten Unterlagen durchzuführen und die dabei eingesetzten Verfahren sind anzugeben.

Zur Durchführung praktischer Prüfungen ist laut /KTA 15b/ ein Prüfprogramm bestehend aus Prüfplan und Prüfanweisungen zu entwickeln. Dabei muss der Prüfplan die während der Prüfung anzuwendenden Verfahren und Geräte festlegen. Die Prüfanweisungen geben die Art der Prüfungen, die Prüfbedingungen, die Prüfparameter und ihre Werte, die Prüfeinrichtungen, die Durchführung der Prüfungen und die Akzeptanzkriterien für ein erfolgreiches Bestehen der Prüfung an. Als Prüflinge sind werksgeprüfte Komponenten eines Typs oder einer Typenreihe auszuwählen, die das gesamte Spektrum der nachzuweisenden Eigenschaften des Typs oder der Typenreihe abdecken müssen. Es muss eine Identitätsprüfung durchgeführt werden, um sicherzustellen, dass der Prüfling mit den Herstellerunterlagen übereinstimmt. Nach erfolgreich abgeschlossener Typprüfung müssen die Prüflinge mindestens drei Jahre für Nachprüfungen zur Verfügung stehen.

Durchzuführende praktische Prüfungen sind laut /KTA 15b/ Funktionsprüfungen, um die im Datenblatt festgelegten Funktionen und die in den Unterlagen spezifizierten Eigen-

schaften der Komponente nachzuweisen. Dabei sind die im Datenblatt festgelegten Bereichsgrenzen und Signalformen für Eingangsgröße, Ausgangsbelastung, Umgebungsbedingungen, Hilfsenergie und elektrische Eigenschaften zu kombinieren. Zudem sind Funktionszwischenprüfungen während der praktischen Prüfungen an bestimmten Haltepunkten durchzuführen. Prüfungen der elektromagnetischen Verträglichkeit müssen nachweisen, dass die laut Datenblatt zulässigen leistungsgebundenen und feldgebundenen elektromagnetischen Beanspruchungen die Funktion der Komponente nicht beeinträchtigen. Zudem sind Klimaprüfungen (konstante Kälte, konstante trockene Wärme, konstante feuchte Wärme, zyklische feuchte Wärme, zyklische trockene Wärme) durchzuführen, um zu zeigen, dass die nach Datenblatt zulässigen klimatischen Beanspruchungen, denen die Komponente wahrend Transport, Lagerung und im Betrieb ausgesetzt werden darf, nicht die Funktionen der Komponente beeinträchtigen. Prüfungen bei mechanischen Beanspruchungen (Schwingungsfestigkeit in verschiedenen Frequenzbereichen, Stoßprüfungen) sind durchzuführen, um zu zeigen, dass die nach Datenblatt zulässigen mechanischen Beanspruchungen, denen die Komponente wahrend Transport und im Betrieb ausgesetzt werden darf, nicht die Funktionen der Komponente beeinträchtigen.

### 3.1.5 KTA 3507

In der Regel KTA 3507 /KTA 14a/ werden die Anforderungen an Vorbereitung, Umfang und Durchführung der Werksprüfungen, Prüfungen nach Instandsetzung und an die Nachweise der Betriebsbewährung der Baugruppen und Komponenten der Sicherheitsleittechnik festgelegt, die auch für elektro- und leittechnische Komponenten Gültigkeit haben. Hinsichtlich Qualitätsaudits wird in /KTA 14a/ beschrieben, dass ein Qualitätsaudit die Überprüfung eines Qualitätssicherungssystems oder seiner Teile ist. Hersteller oder eine zertifizierte Instandsetzungsstelle dürfen die Prüfungen durchführen, wenn sie dem Genehmigungsinhaber oder dessen Auftragnehmer in Qualitätsaudits die Durchführung der Qualitätssicherung und die produkt- und verfahrensspezifischen Qualitätssicherungsmaßnahmen nachweisen und der Genehmigungsinhaber oder dessen Auftragnehmer diese anerkennen. Die mit der Qualitätssicherung beauftragten Stellen sind bei einem Qualitätsaudit anhand von Checklisten stichprobenartig zu überprüfen, wobei geprüft werden muss, dass die beschriebenen Qualitätssicherungsmaßnahmen angewendet werden, die dazu erforderlichen, gültigen Vorschriften, Regeln, Richtlinien und Anweisungen den ausführenden Stellen vorliegen und bekannt sind sowie alle Anweisungen ausreichend und zweckmäßig sind. Die Ergebnisse des Qualitätsaudits sind zu

dokumentieren, wobei die Bewertung des Qualitätssicherungssystems und der Produktqualität sowie alle festgestellten, unzulässigen Abweichungen von den geforderten Qualitätssicherungsmaßnahmen enthalten sein müssen.

Hinsichtlich Werksprüfungen bei der Herstellung wird in /KTA 14a/ gefordert, dass die Qualitätsmerkmale, die geprüft werden sollen, aufzulisten und vom Hersteller eigenverantwortlich festzulegen sind. Dazu sind Unterlagen wie z. B. technische Datenblätter, Fertigungspläne, werksinterne Prüfungen, Ergebnisse der Typprüfungen, Ergebnisse des Nachweises der Betriebsbewährung, werksinterne Instandsetzungsberichte, Fehlermeldungen der Produktion, vorhandene Betriebserfahrungen, Fertigungsverfahren sowie Konfigurations- und Versionsmanagement zu verwenden. Es sind Prüfanweisungen auf Basis der zu prüfenden Qualitätsmerkmale zu erstellen, in denen z. B. Prüfeinrichtungen, Prüfhilfsmittel, Prüfmethode, Prüfparameter, Prüfumfang, Sollwerte mit zulässigen Abweichungen sowie Versions- und Revisionsidentifikation anzugeben sind. Zudem sind Pläne für die Fertigungs- und Werksprüfung zu erstellen, die alle Fertigungs- und Prüfgänge mit den erforderlichen Fertigungs- und Prüfanweisungen und deren Reihenfolge enthalten. Bezüglich Prüfungen werden Pläne für die Eingangsprüfung, Fertigungsprüfung und die Endprüfung benötigt. Bei der Eingangsprüfung hat der Hersteller zu prüfen, ob die von seinem Auftragnehmer gelieferten Bauelemente den in den Beschaffungsunterlagen festgelegten Qualitätsmerkmalen genügen. Die Fertigungsprüfung ist eine stichprobenartige Prüfung der Komponente unter Grenzbelastungsbedingungen. Bei der Endprüfung müssen alle in den Prüfanweisungen festgelegten Qualitätsmerkmale geprüft werden, wobei im Rahmen der Endprüfung eine Identitätsprüfung durchzuführen ist. Wurden Änderungen an der Komponente oder deren Herstellungsprozess vorgenommen, sind alle vorgenannten Schritte entsprechend zu überarbeiten.

Prüfungen von Komponenten nach deren Instandsetzung dürfen von einer Instandsetzungsstelle durchgeführt werden, wenn sie einer organisatorisch unabhängigen Stelle in Qualitätsaudits nachweist, dass sie über die geeigneten technischen Einrichtungen, über qualifiziertes Personal und über die Verantwortlichen für die Prüfung sowie die produkt- und verfahrensspezifischen Qualitätssicherungsmaßnahmen verfügt. Bei jeder Instandsetzungsmaßnahme an einer Komponente sind die festgestellten Ausfälle und ihre Ursachen sowie die daraus abgeleiteten Reparaturmaßnahmen zu dokumentieren. Für die Prüfung nach Instandsetzung müssen diverse Unterlagen wie z. B. Funktionsbeschreibung, Datenblatt, Stromlaufplan, Stückliste, Lageplan der Bauelemente, Prüfanweisungen und Prüffolgeplan vorhanden sein. Die zu prüfenden Qualitätsmerkmale müssen

von der Instandsetzungsstelle anhand der Unterlagen, der Ergebnisse der anlagenspezifischen Eignungsprüfungen und der Typprüfungen sowie der Betriebserfahrungen festgelegt werden. Anschließend sind entsprechende Prüfanweisungen und Prüffolgepläne zu erstellen.

Die Betriebsbewährung einer Komponente ist durch die Auswertung von Aufzeichnungen über die Betrachtungszeit für die spezifizierten Komponenteneigenschaften und Umgebungsbedingungen nachzuweisen. Die im Zuge der Betriebsbewährung nicht nachgewiesenen Eigenschaften sind durch eine ergänzende Typprüfung nachzuweisen. Liegt kein Typprüfnachweis für die Hardware der Komponente vor, dann sind zum Nachweis der Betriebsbewährung die Aufzeichnungen über die Betrachtungszeit für eine Betrachtungseinheit nach statistischen Methoden auszuwerten. Alternativ können dazu vergleichbare Betrachtungseinheiten verwendet werden, wenn diese über vergleichbare elektrische Bauteiltypen, Konstruktionselemente und Auslegungsgrundsätze verfügen und sie für die gleichen Umgebungs- und Betriebsbedingungen spezifiziert wurden.

### 3.1.6 KTA 3701

In der Regel KTA 3701 /KTA 14b/ werden die übergeordneten Anforderungen an die elektrische Energieversorgung von Kernkraftwerken festgelegt, die auch für elektro- und leittechnische Komponenten Gültigkeit haben, die in den Einrichtungen der elektrischen Energieversorgung von Kernkraftwerken eingesetzt werden.

Laut /KTA 14b/ dürfen nur Komponenten in der Energieversorgung sicherheitstechnisch wichtiger Verbraucher verwendet werden, die so zuverlässig sind, dass sie die Nichtverfügbarkeit der zu versorgenden Systeme nicht bestimmen. Die elektromagnetische Verträglichkeit dieser Komponenten in Abhängigkeit von der sicherheitstechnischen Bedeutung sowie die Zuverlässigkeit der elektrischen Energieversorgung der sicherheitstechnisch wichtigen Verbraucher sind nachzuweisen. Dabei müssen sämtliche Komponenten und Hilfssysteme der elektrischen Energieversorgung berücksichtigt werden. Komponenten, die in den Einrichtungen der Netzanschlüsse und der Eigenbedarfsversorgung sowie im Notstromnetz eingesetzt werden, müssen überwachbar, prüfbar, gut zugänglich und austauschbar sein. Durch die Qualitätssicherung ist nachzuweisen, dass die Anforderungshäufigkeit der Notstromerzeugungsanlage minimiert ist.

### 3.1.7 KTA 3901

In der Regel KTA 3901 /KTA 17/ werden die Anforderungen an die Kommunikationseinrichtungen von Kernkraftwerken festgelegt, die auch für elektro- und leittechnische Komponenten Gültigkeit haben, die in Alarmanlagen, Personensuchanlagen, Sprechanlagen und Kommunikationseinrichtungen von Kernkraftwerken eingesetzt werden. In /KTA 17/ wird gefordert, dass Alarmanlagen redundant auszuführen sind. Sie müssen so ausgeführt werden, dass die Alarmabgabe durch den zufälligen Ausfall einer ihrer Komponenten oder durch ein örtlich begrenztes versagensauslösendes Ereignis (z. B. Brand) nicht verhindert wird. Zudem werden in /KTA 17/ Anforderungen bezüglich des Schallpegels von Alarmsignalen und zusätzlich zum akustischen Alarmsignal blinkenden optischen Aufmerksamkeitszeichen aufgestellt.

Hinsichtlich der Auslegung von Komponenten wird in /KTA 17/ gefordert, dass deren Umgebungsbedingungen in Abhängigkeit vom Einbauort und den Anforderungsfällen zu spezifizieren sind und die Komponente den Umgebungsbedingungen entsprechend ausgelegt werden müssen. Außerdem dürfen nur Komponenten eingesetzt werden, die für die Einsatzbedingungen geeignet sind. Die Qualität der Komponenten kann z. B. durch einen Nachweis der Betriebsbewährung, eine Eignungsüberprüfung oder einen Zuverlässigkeitsnachweis nachgewiesen werden. Zudem ist nachzuweisen, dass Einrichtungen des Sicherheitssystems nicht unzulässig durch elektromagnetische Störaussendungen der Komponenten beeinflusst werden. Werden rechnerbasierte Komponenten verwendet, sind zum Schutz ihrer Vertraulichkeit, Integrität und Verfügbarkeit entsprechende Maßnahmen festzulegen.

Komponenten von Kommunikationseinrichtungen sind laut /KTA 17/ dahingehend zu prüfen, dass die spezifizierten Anforderungen eingehalten werden. Zudem sind nach der Installation oder nach Änderungen Abnahme- und Funktionsprüfungen durchzuführen.

### 3.1.8 KTA 3903

In der Regel KTA 3903 /KTA 20/ werden die Anforderungen an die Prüfung und den Betrieb von Hebezeugen festgelegt. Dabei werden auch allgemeine Anforderungen an elektro- und leittechnische Komponenten gestellt, die in Hebezeugen in Kernkraftwerken eingesetzt werden. Hinsichtlich Prüfungen für elektro- und leittechnische Komponenten wird in /KTA 20/ gefordert, dass im Rahmen von Abnahmeprüfungen elektrische Komponenten beispielsweise hinsichtlich elektrischer Versorgung, Schutzeinrichtungen,

elektromagnetischer Verträglichkeit, Steuer- und Meldefunktionen, Kennzeichnung sowie Funktion zu prüfen sind. Im Rahmen wiederkehrender Prüfungen an elektrischen Komponenten sind Befehlseinrichtungen, Leitungen, Verbraucher, Schutzmaßnahmen sowie Mess-, Regel-, Überwachungs- und Sicherheitseinrichtungen zu prüfen. Für die Funktionsprüfungen sind entsprechende Prüfanweisungen zu erstellen.

Für elektro- und leittechnische Komponenten müssen laut /KTA 20/ diverse Unterlagen vorhanden sein. Dies sind z. B. Übersichtsschaltpläne, Stromlaufpläne, Dispositionspläne für Schaltschränke, Schalttafeln und Steuergeräte, Stücklisten, die technische Daten enthalten sowie Datenblätter. Außerdem sind Beschreibungen vorzuhalten, die die Arbeitsweise der Mess-, Regel-, Überwachungs- und Sicherheitseinrichtungen beschreiben. Werden programmierbare elektro- und leittechnische Komponenten eingesetzt, sind alle Verriegelungen sowie das Anwenderprogramm zu beschreiben und das Anwenderprogramm sowie zugehörige Systemhandbücher müssen zur Prüfung vorgelegt werden. Beim Einsatz rechnerbasierter Komponenten ist die Unabhängigkeit der Sicherheitsfunktionen von den betrieblichen Funktionen nachzuweisen. Dies kann beispielsweise durch systematische Methoden zur Identifikation von Fehlermöglichkeiten und Analyse der Auswirkungen dieser Fehler (z. B. FMEA) oder durch eine einsatzunabhängige Typprüfung erfolgen. Für Hard- und Softwarekomponenten sind Konfigurations- und Identifikationsdokumentationen vorzulegen.

Zudem werden in /KTA 20/ direkte Anforderungen an kommerzielle Komponenten gestellt. Dabei wird gefordert, dass Hersteller von COTS-Komponenten nach DIN EN ISO 9001 zertifiziert sein müssen und ein entsprechendes Qualitätsmanagement nachweisen können. Für die Durchführung von Vorprüfungen an COTS-Komponenten ist zu beachten, dass die für die Bemessung maßgeblichen Unterlagen mit den entsprechenden Auslegungsdaten vorzulegen sind. Der Hersteller muss bestätigen, dass die COTS-Komponenten die vorgegebenen Auslegungsdaten erfüllen. Die bei Versuchen ermittelten Messdaten und die Unterlagen mit den Auslegungsdaten sind zu prüfen. Zudem muss der Hersteller eine gleichbleibende Qualität bei der Herstellung der COTS-Komponenten garantieren.

Zur Vorprüfung von COTS-Komponenten sind laut /KTA 20/ diverse Unterlagen vorzulegen, wie z. B. Übersichtszeichnungen, Ausführungszeichnungen, Stücklisten mit Werkstoffangaben, Festigkeitsberechnungen, Schweißangaben, Schweißzulassung, elektrische Einrichtungen, Betriebs- und Wartungsanleitungen, Prüfplan für die Bauprüfung,

Prüfplan für die Abnahmeprüfung und Prüfplan für wiederkehrende Prüfungen. Die Unterlagen sind beispielsweise auf Richtigkeit der Lastannahmen, Vollständigkeit und Richtigkeit der Berechnungen, Einhaltung der zulässigen Spannungen und der Sicherheiten, Einhaltung der Verriegelungen, Bemessung der Leistungskabel und Zuordnung der Überstromschutzeinrichtungen, Auslegung der Sicherheits- und Überwachungseinrichtungen, Vollständigkeit der Funktionsbeschreibung und des Funktionsablaufplans sowie Zugänglichkeit der Hebezeuge für Wartungs- und Reparaturarbeiten zu prüfen. Endprüfungen sind im Herstellerwerk auf einem Lastprüfstand durchzuführen.

Hinsichtlich der Wartung und Instandsetzung wird in /KTA 20/ gefordert, dass für alle umgesetzten Wartungs- und Instandsetzungsmaßnahmen diverse Angaben aufgezeichnet werden müssen. Dies sind die eindeutige Bezeichnung des Hebezeugs, der Anlass und die Begründung für die Wartungs- und Instandsetzungsarbeiten, die Art und Anzahl der ausgewechselten Teile inklusive Begründung, das Datum und die Bezeichnung der Zeugnisse oder Bescheinigungen der neu eingesetzten Teile sowie das Datum der Wartung oder Instandsetzung.

### 3.1.9 DIN EN 60880

Die Norm DIN EN 60880 /DIN 10b/ legt die Anforderungen für die Software rechnerbasierter leittechnischer Systeme in Kernkraftwerken für Funktionen der Kategorie A fest. Diese Anforderungen bieten die Grundlage für die Entwicklung hochzuverlässiger Software. Es wird auf jede Stufe der Softwareentwicklung und der Dokumentation eingegangen, einschließlich Anforderungsspezifikation, Auslegung, Realisierung, Verifizierung, Validierung und Betrieb. /DIN 10b/ enthält übergeordnete Informationen zum Software-Projektmanagement, Software-Qualitätssicherungsplan, Konfigurationsmanagement, Zugriffsschutz, zur Selbstüberwachung sowie zur Auslegung und Implementierung von Software rechnerbasierter leittechnischer Systeme die Funktionen der Kategorie A ausführen. Zudem wird in /DIN 10b/ in einzelnen Teilen auf COTS-Software eingegangen.

Hinsichtlich des Software-Projektmanagements wird in /DIN 10b/ gefordert, dass jedes Softwareprojekt in mehrere Phasen der Softwareentwicklung strukturiert werden muss. Dabei ist zu berücksichtigen, dass die Tätigkeiten in den jeweiligen Phasen der Softwareentwicklung unter Einbeziehung des gesamten Software-Sicherheitslebenszyklus festzulegen sind. Jede Phase muss formalisiert sein und keine der Phasen darf ausgelassen werden. Die Ein- und Ausgänge jeder Phase sind zu definieren und zu dokumen-

tieren. Werden Tätigkeiten zur Softwareentwicklung automatisiert, müssen die automatisierten Vorgänge dokumentiert werden. Das Ergebnis jeder Phase ist systematisch zu überprüfen und für jede Phase hat eine hinreichende Dokumentation zu erfolgen.

Zudem wird in /DIN 10b/ ein Software-Qualitätssicherungsplan gefordert, in dem alle technischen Prozeduren, die in den verschiedenen Phasen des Software-Sicherheitslebenszyklus benötigt werden, beschrieben sind. Im Qualitätssicherungsplan müssen die Aktivitäten während der verschiedenen Phasen des Lebenszyklus kompetenten Personen mit geeigneten Ressourcen zugeordnet werden. Modifizierungen sind zu prüfen und von autorisierten Personen zu genehmigen sowie zu dokumentieren. Die verwendeten Methoden, Sprachen, Werkzeuge, Regeln und Normen müssen festgelegt, dokumentiert und beherrscht werden, sowie den jeweiligen Aktivitäten eindeutig zugeordnet werden können. Alle Qualitätsanforderungen müssen angesprochen, verfolgt und gelöst werden.

Im Rahmen des Konfigurationsmanagements der Software ist laut /DIN 10b/ ein Versionsmanagement umzusetzen, so dass alle Versionen der Softwareeinheiten eindeutig identifizierbar sind. Dabei muss in Entwicklung befindliche Software deutlich von fertiggestellter und verifizierter Software getrennt werden. Die Integrität der Software muss verifizierbar sein und es muss möglich sein, die Software-Version des Zielsystems sowie die von einer Modifizierung betroffenen Softwareeinheiten und die dabei eingesetzten Werkzeuge festzustellen. Die Software darf nur von autorisierten Personen modifiziert werden, so dass der Zugriff auf die Software entsprechend zu schützen ist. Der Zugriffsschutz dient dazu, zu verhindern, dass nicht autorisierte Personen und Systeme die Software lesen oder ändern können. Dabei ist laut /DIN 10b/ eine Analyse der möglichen Bedrohungen unter Berücksichtigung der relevanten Phasen des System- und Software-Sicherheitslebenszyklus durchzuführen. Wenn sich bei der Analyse herausstellt, dass die Gegenmaßnahmen auf Systemebene unzureichend sind, dann sind entsprechende Gegenmaßnahmen bei der Softwareauslegung zu realisieren. Zudem ist der Zugriffsschutz so auszulegen, dass die Verwundbarkeit des Systems minimiert wird, z. B. durch Reduzierung der Funktionalität auf den notwendigen Umfang. Das Bedienpersonal darf keine Änderungen an der Software durchführen können. Müssen für bestimmte leittechnische Funktionen Daten geändert werden, ist der Zugriff über die Mensch-Maschine-Schnittstelle auf das Nötige zu beschränken. Für den Benutzerzugang ist laut /DIN 10b/ falls erforderlich ein Authentifizierungsprozess umzusetzen. Der Benutzerzugang ist entsprechend zu schützen und muss auf ein geeignetes Maß reduziert werden. Ein Zugang

von außerhalb des technischen Umfelds der Anlage, durch den Softwarefunktionen oder Daten manipuliert werden können, darf nicht ermöglicht werden.

Hinsichtlich der Selbstüberwachung wird in /DIN 10b/ gefordert, dass während des Betriebs in spezifizierten Zeitabständen die Hardware sowie das Verhalten der Software überwacht werden muss. Der Programmcode und unveränderliche Daten müssen im Hinblick auf unbeabsichtigte Änderungen überwacht werden. Dabei können Selbsttestfunktionen wie z. B. eine Daten-Plausibilitätsprüfung, eine Überprüfung der Parameterbereiche oder auch die zeitliche Begrenzung von Schleifendurchläufen zum Einsatz kommen. Durch die Selbstüberwachung müssen Zufallsausfälle von Hardwarekomponenten, fehlerhaftes Verhalten der Software sowie fehlerhafte Datenübertragung zwischen verschiedenen Prozessoren erkannt werden. Wird ein Fehler entdeckt, muss die Software in geeigneter Weise zeitgerecht reagieren und diagnostische Informationen sammeln. Die Systemfunktionen dürfen durch die Selbstüberwachung nicht beeinträchtigt werden. Hinsichtlich der Auslegung und Implementierung der Software wird in /DIN 10b/ ausgesagt, dass die Programmstruktur modular, übersichtlich und leicht verständlich aufgebaut sein sollte. Um die Auswirkung menschlicher Fehler einzuschränken, sollte bei der Konfiguration der Software eine werkzeugbasierte Vorgehensweise vorgezogen werden.

Hinsichtlich der Qualifizierung von COTS-Software wird in /DIN 10b/ ausgesagt, dass COTS-Software zunächst hinsichtlich ihrer Fähigkeiten, die funktionalen sowie die Leistungs- und Architekturanforderungen der System-Anforderungsspezifikation zu erfüllen, und der sich daraus ergebenden Eignung für die vorgesehene Anwendung bewertet werden muss. Zudem sind die Qualität und die Betriebserfahrung der COTS-Software zu bewerten und falls Korrekturen oder Anpassungen der COTS-Software erforderlich sind, sind diese festzulegen. Der Bewertungs- und Beurteilungsprozess muss eine Bewertung der Funktions- und Leistungsmerkmale der Software und der vorhandenen Dokumentation über ihre Qualifizierung, Bewertung der Qualität des Softwareentwurfs- und Entwicklungsprozesses, Bewertung der Betriebserfahrung sowie eine Dokumentation der Beurteilung der aus den Bewertungen gewonnenen Erkenntnisse und der erforderlichen Maßnahmen zur Ertüchtigung für die vorgesehene Anwendung der Software einschließen. Bei einer Entscheidung für die Verwendung von COTS-Software, muss diese in das Konfigurationsmanagement des Systems einbezogen werden und nur die in der Qualifizierung beschriebene Fassung der Software mit den erforderlichen Anpassungen darf verwendet werden. Für den Fall, dass eine andere Softwareversion verwendet werden

soll, muss der Qualitätssicherungsplan des Systems ein Verfahren für die Anpassung der COTS-Software vorsehen. Fehler und Ausfälle der Software im Zuge deren Nutzung in anderen Anlagen und die entsprechend dort durchgeführten Softwareänderungen sollten kontinuierlich aufgenommen und ausgewertet werden.

### 3.1.10 DIN EN 61513

Die Norm DIN EN 61513 /DIN 13/ legt Anforderungen für die gesamte leittechnische Architektur in Kernkraftwerken fest. Dabei wird berücksichtigt, dass entweder fest verdrahtete oder rechnerbasierte Komponenten eingesetzt werden können sowie eine Kombination aus beiden Technologien. /DIN 13/ enthält übergeordnete Anforderungen zu in der Leittechnik eingesetzten Komponenten bezüglich ihrer Selbstüberwachung und Ausfalltoleranz, ihrer Qualifizierung und der Benutzerschnittstellen. Darüber hinaus wird auf Vorkehrungen gegen schädigende Beeinflussungen eingegangen. Zudem wird in /DIN 13/ auf die Auswahl und Beschaffung von COTS-Komponenten eingegangen.

Hinsichtlich Selbstüberwachung und Ausfalltoleranz wird in /DIN 13/ gefordert, dass Komponenten Abweichungen und Ausfälle rechtzeitig über eine Selbstüberwachung erkennen müssen, damit das leittechnische System, in dem sie eingebaut sind, verfügbar bleibt. Dabei ist ein geeigneter Kompromiss zwischen der Erkennung von Ausfällen durch die Selbstüberwachung und der dafür erforderlichen Komplexität zu finden. Für die benötigten korrigierenden Eingriffe sind angemessene, zeitgerechte und geeignet aufbereitete diagnostische Informationen zu sammeln. Bei der Entdeckung von Ausfällen ist ein angemessener Backup-Betrieb zu ermöglichen (z. B. kontrollierte Verminderung der Funktionalität, Fail-Safe-Eigenschaften, Ausgänge auf AUS).

Bei der Mensch-Maschine-Kommunikation muss laut /DIN 13/ sichergestellt werden, dass die Wahrscheinlichkeit menschlicher Fehler (z. B. versehentliche Fehler, Versäumnisse, Auslegungsfehler) minimiert wird. Für rechnerbasierte Systeme muss die Hardware unter Berücksichtigung der Umgebungsbedingungen sowie die in die Hardware integrierte System- und Anwendungssoftware qualifiziert werden.

Hinsichtlich der Auswahl von COTS-Komponenten wird in /DIN 13/ empfohlen, dass zu prüfen ist, ob die verfügbaren Dokumente die Funktionalität und die Eigenschaften aller Komponenten explizit beschreiben. Typischerweise werden dabei Informationen über Laufzeit und Speicherbedarf der Softwarekomponenten, Ausfallraten der Komponenten,

Fail-Safe-Eigenschaften bezüglich Hardware- und Softwarefehlern, Umgebungsbedingungen für die Systemkonfiguration, Anforderungen an die Montage, Energieversorgung, Energieverbrauch und Wartungswerkzeuge benötigt. Nicht explizit vorgegebene Eigenschaften müssen durch Prüfungen bestimmt werden. Es ist nachzuweisen, dass in der konkreten Anwendung nicht genutzte Komponentenfunktionen die geforderte Funktionalität nicht beeinträchtigen können.

## 3.2 Bewertungsansatz hinsichtlich des Einsatzes von COTS-Komponenten

Aufbauend auf den Anforderungen an kommerzielle Komponenten zum Einsatz in sicherheitstechnisch wichtigen Systemen, die aus den ausgewerteten Dokumenten (siehe Abschnitt 2.1) und internationalen Vorgehensweisen (siehe Abschnitt 2.2) gewonnen wurden, und den Anforderungen an elektro- und leittechnische Komponenten aus dem nationalen kerntechnischen Regelwerk (siehe Abschnitt 3.1) wurde ein Ansatz zur Bewertung des Einsatzes von COTS-Komponenten entwickelt. Da die Nachweistiefen und Anforderungen an elektro- und leittechnische Einrichtungen in Abhängigkeit von ihrer sicherheitstechnischen Bedeutung unterschiedlich sind, wurden bei der Entwicklung des Bewertungsansatzes die Kategorien A, B und C nach DIN EN 61226 /DIN 10a/ berücksichtigt. Bei der Entwicklung des Bewertungsansatzes wurden die zehn Aspekte betrachtet, die bereits bei der Ermittlung der Anforderungen berücksichtigt wurden.

Die betrachteten Aspekte sind:

- Auswahl und Beschaffung von COTS-Komponenten
- Qualitätsmanagement des Herstellers und dessen Zulieferer
- Design- und Entwicklungsprozess der COTS-Komponenten
- Komplexität der COTS-Komponenten
- Technische Eigenschaften und Einsatzort bzw. -art der COTS-Komponenten
- Qualifizierung von COTS-Komponenten
- Möglichkeiten zur Fehlererkennung und Fehlervermeidung
- Änderungsmanagement
- Wartung und Instandhaltung
- Dokumentation

Für jeden dieser Aspekte wurden für den Bewertungsansatz fünf Anforderungen entwickelt.

Die jeweilige sicherheitstechnische Bedeutung der leittechnischen Funktionen und die damit in Verbindung stehenden Anforderungen an die in diesen Funktionen eingesetzten Komponenten unterscheiden sich je nach Funktion, weshalb nach DIN EN 61226 /DIN 10a/ eine Einstufung der leittechnischen Funktionen in die Kategorien A, B und C erfolgt. Dabei werden in Kategorie A Funktionen eingestuft, die eine grundsätzliche Rolle für die Erreichung und Beibehaltung der Sicherheit der Anlage spielen. Typische leittechnische Systeme, die Kategorie A zugeordnet werden, sind z. B. das Reaktorschutzsystem oder das Sicherheits-Auslösesystem. In Kategorie B werden Funktionen eingestuft, die für die Erreichung und Beibehaltung der Sicherheit der Anlage eine ergänzende Rolle spielen. Typische leittechnische Systeme, die Kategorie B zugeordnet werden, sind z. B. das automatische Steuerungs-/Regelungssystem oder präventive Schutzsysteme. In Kategorie C werden Funktionen eingestuft, die eine unterstützende oder indirekte Rolle bei der Erreichung und Erhaltung der Sicherheit der Anlage spielen. Typische leittechnische Systeme, die Kategorie C zugeordnet werden, sind beispielsweise die Meldeanlage, Zugangskontrollsysteme oder Überwachungssysteme zur Verfolgung radioaktiver Abgaben. Da die Anforderungen an Systeme, die Funktionen der Kategorie A ausführen, höher sind als die Anforderungen an Systeme, die Funktionen der Kategorie B ausführen und da die Anforderungen an Systeme, die Funktionen der Kategorie B ausführen wiederum höher sind als die Anforderungen an Systeme, die Funktionen der Kategorie C ausführen, erfolgt eine abgestufte Formulierung der Anforderungen. Daher erfolgte in dem entwickelten Bewertungsansatz für den Einsatz von COTS-Komponenten, falls notwendig, ebenfalls eine abgestufte Formulierung der Anforderungen für den Einsatz der COTS-Komponenten in Systemen, die Funktionen der Kategorien A, B oder C ausführen. Dabei sind in der Regel die Anforderungen für die niedrigeren Sicherheitskategorien geringer als die Anforderungen für die höheren Sicherheitskategorien.

Der entwickelte Bewertungsansatz kann als Grundlage genutzt werden, um COTS-Komponenten hinsichtlich der Möglichkeit des Einsatzes in sicherheitstechnisch wichtigen elektro- und leittechnischen Einrichtungen in kerntechnischen Anlagen zu bewerten. Zudem gibt der Bewertungsansatz Hinweise bezüglich zu berücksichtigender Aspekte und Anforderungen bei der Qualifizierung von COTS-Komponenten.

Der entwickelte Bewertungsansatz wurde in erster Linie auf der Basis von Anforderungen entwickelt, die für Kernkraftwerke aufgestellt wurden. Da der Bewertungsansatz Anforderungen hinsichtlich allgemein gültiger Aspekte aufstellt und nach den Kategorien der Sicherheitsfunktionen aufgebaut ist, ergibt sich aber prinzipiell auch die Möglichkeit, diesen auf andere kerntechnische Anlagen (z. B. Forschungsreaktoren, Zwischenlager) anzuwenden, wenn in diesen die sicherheitstechnisch wichtigen Funktionen entsprechend den Kategorien nach DIN EN 61226 /DIN 10a/ kategorisiert worden sind.

Bei der Anwendung des entwickelten Bewertungsansatzes ist zu bewerten, inwieweit die aufgestellten Anforderungen von den in Betracht gezogenen COTS-Komponenten erfüllt werden. Es ist zu erwähnen, dass die Anwendung des Bewertungsansatzes keine Qualifizierung von COTS-Komponenten ersetzt. Der Bewertungsansatz soll lediglich dazu dienen, die grundsätzliche Möglichkeit des Einsatzes von COTS-Komponenten in sicherheitstechnisch wichtigen elektro- und leittechnischen Einrichtungen in kerntechnischen Anlagen zu bewerten. Zudem soll der Bewertungsansatz Hinweise geben, welche Aspekte und Anforderungen bei einer Qualifizierung von COTS-Komponenten zu berücksichtigen sind. Eine Qualifizierung der COTS-Komponenten (z. B. durch den Betreiber der kerntechnischen Anlage, Third-Party-Organisation, etc.) ist also auch dann durchzuführen, wenn die COTS-Komponenten alle Anforderungen aus dem Bewertungsansatz erfüllen.

In den nachfolgenden Abschnitten wird der Bewertungsansatz hinsichtlich der zehn betrachteten Aspekte dargestellt.

### 3.2.1 Auswahl und Beschaffung von COTS-Komponenten

Hinsichtlich des Aspektes der Auswahl und Beschaffung von COTS-Komponenten wurden folgende Anforderungen entwickelt, die nachfolgend für die Kategorien A, B und C vorgestellt werden:

- Anforderungsspezifikation an COTS-Komponenten
- Eignung der COTS-Komponenten für die Zielanwendung
- Auswahl des Herstellers der COTS-Komponenten
- Dokumentation im Rahmen der Auswahl von COTS-Komponenten
- Vorhandensein einer bereits durchgeführten Qualifizierung/Zertifizierung

**Anforderungsspezifikation an COTS-Komponenten**

Kategorie A

Vor der Auswahl und Beschaffung von COTS-Komponenten ist festzulegen, welche Anforderungen die Komponenten erfüllen müssen und welche Funktionen von den Komponenten ausgeführt werden sollen. Die Anforderungsspezifikation muss dabei Punkte umfassen wie beispielsweise die auszuführenden Funktionen der Komponenten, potentielle Einschränkungen bei der Auswahl der Komponenten (z. B. CCF-Vorgaben, Sicherheitsfragen), regulatorische Anforderungen, Funktions- und Leistungsanforderungen (z. B. Genauigkeit, Reaktionszeit), Zuverlässigkeitsmerkmale (z. B. Verhalten bei Fehlern, Verhalten bei anormalen Umgebungsbedingungen) oder Maßnahmen bezüglich der Cybersicherheit (z. B. Schutz der Funktion vor unbeabsichtigten Änderungen, Deaktivierung nicht verwendeter Kommunikationskanäle). Zudem muss die Anforderungsspezifikation Voraussetzungen zur Erfüllung der Anforderungen wie beispielsweise erforderliche Ressourcen (z. B. Energieversorgung, Kommunikationsbandbreite), Umgebungsbedingungen (z. B. Temperatur, Feuchtigkeit, Vibration, elektromagnetische Verträglichkeit) sowie Betriebs- und Wartungsanforderungen umfassen. Die Anforderungen sind in einem Pflichtenheft festzulegen und dem Hersteller klar verständlich vorzulegen, so dass der Hersteller nur die für die Lieferung relevanten Anforderungen in einem klaren Format erhält.

Grundsätzlich sollte die Möglichkeit bestehen, bei der Erstellung der Anforderungsspezifikation mit anderen Betreibern zusammenzuarbeiten und dabei eine generische, gemeinsam erstellte und gemeinsam genutzte Anforderungsspezifikation zu erstellen, um Überlappungen zu vermeiden. Dies kann auch die Zusammenarbeit mit den Herstellern der COTS-Komponenten erleichtern. Falls erforderlich sind standortspezifische Anforderungen zusätzlich zur generischen Anforderungsspezifikation festzulegen.

Kategorie B

Hinsichtlich der Anforderungsspezifikation an COTS-Komponenten ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

Kategorie C

Hinsichtlich der Anforderungsspezifikation an COTS-Komponenten ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie C gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

**Eignung der COTS-Komponenten für die Zielanwendung**

Kategorie A

Die prinzipielle Eignung der COTS-Komponenten für den Einsatz in der Zielanwendung muss eingeschätzt und untersucht werden. Dazu sind deren Funktionalität, die Betriebsumgebung, für die diese Komponenten konzipiert wurden sowie weitere Merkmale zur Bestimmung der Anpassungsfähigkeit dieser COTS-Komponenten an die Zielanwendung (z. B. physische Architektur, Softwarearchitektur, funktionale Architektur, Schnittstellen) zu untersuchen. Durch diese Untersuchungen ist festzustellen, ob die COTS-Komponenten die vorgesehenen Funktionen unter den vorgesehenen Betriebsbedingungen in den Systemen, in denen sie eingesetzt werden sollen, erfüllen können.

Es kann bereits die für die Zielanwendung relevante Betriebshistorie der COTS-Komponenten berücksichtigt werden, um Aufschluss darüber zu erhalten, ob die COTS-Komponenten beispielsweise Anforderungen hinsichtlich Sicherheit, Zuverlässigkeit und Wartbarkeit erfüllen können.

Ergeben sich Unterschiede zwischen der Anforderungsspezifikation und den Eigenschaften der COTS-Komponenten, aufgrund derer die COTS-Komponenten nicht für einen Einsatz in der Zielanwendung geeignet sind, müssen die COTS-Komponenten zurückgewiesen werden.

Kategorie B

Hinsichtlich der Eignung der COTS-Komponenten für die Zielanwendung ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

Kategorie C

Hinsichtlich der Eignung der COTS-Komponenten für die Zielanwendung ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie C gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

**Auswahl des Herstellers der COTS-Komponenten**

Kategorie A

Hersteller von COTS-Komponenten, die zum Einsatz in der Zielanwendung geeignet sein könnten, sollten einen Qualitätssicherungsprozess inklusive Auditierungen durchlaufen, um zur Lieferung von COTS-Komponenten zugelassen zu werden. In diesen Prozess ist auch die vollständige Lieferkette des Herstellers mit allen Zulieferern sowie auch deren Zulieferern aufzunehmen. In diesem Prozess sollte geprüft werden, dass die Reputation der Hersteller und der COTS-Komponenten positiv ist.

Zudem müssen die Hersteller bereit sein, sowohl am Prozess der Qualifizierung der COTS-Komponenten teilzunehmen als auch die dafür erforderlichen Informationen und Unterlagen (z. B. Entwicklungsunterlagen, Schaltpläne, Quellcode, usw.) bereitzustellen. Dies ist notwendig, da nur die Hersteller über die benötigten Detailinformationen verfügen. Es ist mit den Herstellern zu vereinbaren, welche Informationen und Ressourcen zur Verfügung gestellt werden müssen. Stellen die Hersteller erforderliche Unterlagen nicht außerhalb des Firmengeländes zur Verfügung, muss die Möglichkeit bestehen, Prüfungen und Bewertungen vor Ort bei den Herstellern durchzuführen. Außer für die Hersteller gelten diese Anforderungen auch für die gesamte Lieferkette, die in Verbindung mit der Herstellung der COTS-Komponenten steht.

Die in Frage kommenden Hersteller müssen dahingehend überprüft werden, dass sie in der Lage sind, langfristige Unterstützung bereitzustellen. Dabei ist auch zu prüfen, dass eine zuverlässige Ersatzteilstrategie und eine langfristige Ersatzteilversorgung sichergestellt sind.

Außerdem sollten in Frage kommende Hersteller in der Lage sein, Informationen hinsichtlich der Betriebserfahrung der COTS-Komponenten liefern zu können, die im Rahmen des Qualifizierungsprozesses berücksichtigt werden können. Dabei ist es sinnvoll, dass jede Komponente auf einen vom Hersteller zugewiesenen Rückverfolgungscode,

der in der gesamten Lieferkette unverändert beibehalten werden muss, zurückverfolgt werden kann.

Kategorie B

Hinsichtlich der Auswahl des Herstellers der COTS-Komponenten ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

Kategorie C

Hinsichtlich der Auswahl des Herstellers der COTS-Komponenten ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie C gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

**Dokumentation im Rahmen der Auswahl von COTS-Komponenten**

Kategorie A

Bereits bei der Auswahl von COTS-Komponenten ist deren vorhandene Dokumentation zu überprüfen, um die Wahrscheinlichkeit einer erfolgreichen Qualifizierung abzuschätzen. Die Dokumentation muss Informationen zu bereitgestellten Funktionen der COTS-Komponenten, Schnittstellen (sowohl Hardware als auch Software), Typen, Formaten und Einschränkungen von Eingängen, Ausgängen, Signalen, Parametern und Konfigurationsdaten, verschiedenen möglichen Betriebsarten sowie Einschränkungen, die bei der Verwendung der Komponenten zu beachten sind, beinhalten. Zudem müssen Konstruktionsstandards und -anleitungen, Konstruktionszeichnungen und Spezifikationen, Funktionalität und Eigenschaften verwendeter Verfahren und Werkzeuge, bereits durchgeführte Sicherheitsanalysen, Testverfahren bereits durchgeführter Tests und zugehörige Testergebnisse sowie Berichte über Ausfälle und Anomalien vorliegen.

Außerdem müssen in der Dokumentation Informationen bezüglich Selbstüberwachungsmechanismen, Fehlertoleranzfähigkeit, Fehlermöglichkeiten, sowie bei rechnerbasierten Komponenten Anforderungen an die Laufzeitumgebung der Software vorhanden sein. Anhand der Dokumentation müssen Informationen bereitgestellt werden, um über wichtige sicherheitsrelevante Elemente der Systemleistung (z. B. maximale Antwortzeiten, maximale Ressourcennutzung) korrekte Vorhersagen zu ermöglichen.

Es ist zu analysieren, ob in der zur Verfügung stehenden Dokumentation der COTS-Komponenten deren Funktionalität und Eigenschaften explizit erläutert werden. Die Verfügbarkeit und die Qualität der vorliegenden Dokumentation muss es ermöglichen, alle Aspekte der Funktionen, der Betriebsmodi und des Verhaltens der COTS-Komponenten zu verstehen. Anhand der vorliegenden Dokumentation muss es möglich sein, die Zuverlässigkeit und Leistungsfähigkeit der Komponenten unter der vorgesehenen Konfiguration in der späteren Zielfunktion zu bestimmen.

Kategorie B

Hinsichtlich der vorhandenen Dokumentation im Rahmen der Auswahl von COTS-Komponenten ergeben sich keine Unterschiede zwischen den Sicherheitskategorien A und B. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

Kategorie C

Bereits bei der Auswahl von COTS-Komponenten ist deren vorhandene Dokumentation zu überprüfen, um die Wahrscheinlichkeit einer erfolgreichen Qualifizierung abzuschätzen. Die Dokumentation muss Informationen zu bereitgestellten Funktionen der COTS-Komponenten, Schnittstellen (sowohl Hardware als auch Software), Funktionen, Typen, Formaten und Einschränkungen von Eingängen, Ausgängen, Signalen, Parametern und Konfigurationsdaten, verschiedenen möglichen Betriebsarten sowie Einschränkungen, die bei der Verwendung der Komponenten zu beachten sind, beinhalten. Zudem müssen Konstruktionsstandards und -anleitungen, Konstruktionszeichnungen und Spezifikationen, Funktionalität und Eigenschaften verwendeter Verfahren und Werkzeuge, bereits durchgeführte Sicherheitsanalysen, Testverfahren bereits durchgeführter Tests und zugehörige Testergebnisse sowie Berichte über Ausfälle und Anomalien vorliegen.

Es ist zu analysieren, ob in der zur Verfügung stehenden Dokumentation der COTS-Komponenten deren Funktionalität und Eigenschaften explizit erläutert werden. Die Verfügbarkeit und die Qualität der vorliegenden Dokumentation sollte es ermöglichen, alle Aspekte der Funktionen, der Betriebsmodi und des Verhaltens der COTS-Komponenten zu verstehen. Anhand der vorliegenden Dokumentation sollte es möglich sein, die Zuverlässigkeit und Leistungsfähigkeit der Komponenten unter der vorgesehenen Konfiguration in den späteren Zielfunktionen zu bestimmen.

**Vorhandensein einer bereits durchgeführten Qualifizierung/Zertifizierung**

Kategorie A

Bereits bei der Auswahl von COTS-Komponenten ist zu überprüfen, ob diese unter Berücksichtigung kommerzieller Normen hergestellt wurden und eine diesen Normen entsprechende Qualifizierung/Zertifizierung besitzen.

Zum Einsatz in Funktionen der Kategorie A müssen die COTS-Komponenten speziell für den Einsatz in Sicherheitsanwendungen entwickelt und nach einer entsprechenden Norm, insbesondere DIN EN 61508 /DIN 11/, qualifiziert worden sein. Solch eine Qualifizierung alleine reicht allerdings nicht aus, damit die COTS-Komponenten eingesetzt werden können. Je nach Zielfunktion und sicherheitstechnischer Aufgabenstellung sind weitere Qualifizierungen erforderlich. Hinsichtlich eingesetzter Software sind insbesondere die Anforderungen von DIN EN 60880 /DIN 10b/ sowie DIN EN 60987 /DIN 10c/ einzuhalten.

Zur Verwendung der Ergebnisse einer bereits vorhandenen Qualifizierung/Zertifizierung müssen die dort betrachteten Eigenschaften explizit festgestellt werden und es müssen entsprechende Dokumentationen vorliegen. Notwendige zusätzliche Arbeiten und Einschränkungen für eine anlagenspezifische Qualifizierung müssen ausgewiesen werden.

Es ist zu beachten, dass sich eine bereits vorhandene Qualifizierung/Zertifizierung immer auf eine spezielle Version der COTS-Komponenten bezieht. Nur für diese Version darf eine bereits vorhandene Qualifizierung/Zertifizierung berücksichtigt werden. Für jede Versionsänderung hat eine neue Beurteilung zu erfolgen. Zudem muss die bereits vorhandene Qualifizierung/Zertifizierung unter den Umgebungsbedingungen erfolgt sein, in denen die COTS-Komponenten eingesetzt werden sollen.

Kategorie B

Bereits bei der Auswahl von COTS-Komponenten sollte überprüft werden, ob diese unter Berücksichtigung kommerzieller Normen hergestellt wurden und eine diesen Normen entsprechende Qualifizierung/Zertifizierung besitzen. Zum Einsatz in Funktionen der Kategorie B sollten die COTS-Komponenten nach einer entsprechenden Norm, insbesondere DIN EN 61508 /DIN 11/, qualifiziert worden sein.

Zur Verwendung der Ergebnisse einer bereits vorhandenen Qualifizierung/Zertifizierung müssen die dort betrachteten Eigenschaften explizit festgestellt werden und es müssen entsprechende Dokumentationen vorliegen. Notwendige zusätzliche Arbeiten und Einschränkungen für eine anlagenspezifische Qualifizierung müssen ausgewiesen werden.

Es ist zu beachten, dass sich eine bereits vorhandene Qualifizierung/Zertifizierung immer auf eine spezielle Version der COTS-Komponenten bezieht. Nur für diese Version oder eine sich von dieser Version nur geringfügig unterscheidenden Version darf eine bereits vorhandene Qualifizierung/Zertifizierung berücksichtigt werden. Die Änderungen müssen dabei gut dokumentiert und validiert sein und dürfen die beabsichtigten Funktionen der COTS-Komponenten nicht beeinträchtigen. Zudem sollte die bereits vorhandene Qualifizierung/Zertifizierung unter den Umgebungsbedingungen erfolgt sein, in denen die COTS-Komponenten eingesetzt werden sollen.

Kategorie C

Bereits bei der Auswahl von COTS-Komponenten kann überprüft werden, ob diese unter Berücksichtigung kommerzieller Normen hergestellt wurden und eine diesen Normen entsprechende Qualifizierung/Zertifizierung besitzen. Sollen Ergebnisse einer bereits vorhandenen Qualifizierung/Zertifizierung berücksichtigt werden, müssen die dort betrachteten Eigenschaften explizit festgestellt werden und es müssen entsprechende Dokumentationen vorliegen. Notwendige zusätzliche Arbeiten und Einschränkungen für eine anlagenspezifische Qualifizierung müssen ausgewiesen werden.

Es ist zu beachten, dass sich eine bereits vorhandene Qualifizierung/Zertifizierung immer auf eine spezielle Version der COTS-Komponenten bezieht. Nur für diese Version oder eine sich von dieser Version nur geringfügig unterscheidenden Version darf eine bereits vorhandene Qualifizierung/Zertifizierung berücksichtigt werden. Die Änderungen müssen dabei gut dokumentiert und validiert sein. Zudem sollte die bereits vorhandene Qualifizierung/Zertifizierung unter den Umgebungsbedingungen erfolgt sein, in denen die COTS-Komponenten eingesetzt werden sollen.

### 3.2.2 Qualitätsmanagement des Herstellers und dessen Zulieferer

Hinsichtlich des Aspektes des Qualitätsmanagements des Herstellers und dessen Zulieferer wurden folgende Anforderungen entwickelt, die nachfolgend für die Kategorien A, B und C vorgestellt werden:

- Qualitätsmanagementsystem des Herstellers
- Qualitätssicherung während des Design- und Entwicklungsprozesses
- Qualitätssicherung bei Verwendung von Werkzeugen
- Umgang mit Problemen oder Mängeln
- Qualitätsmanagement und Qualitätssicherung der Zulieferer

**Qualitätsmanagementsystem des Herstellers**

Kategorie A

Vor dem Abschluss einer Vereinbarung zur Beschaffung von COTS-Komponenten ist sicherzustellen, dass die Hersteller der Komponenten über ein dokumentiertes Qualitätsmanagementsystem nach ISO 9001 (oder gleichwertig) verfügen, welches durch ein unabhängiges Zertifikat zu bestätigen ist.

Jeder zur Lieferung von COTS-Komponenten ausgewählte Hersteller sollte im Rahmen eines Audits begutachtet werden, um sicherzustellen, dass dessen Qualitätsmanagementsystem eingehalten wird. Nach positiver Durchführung des Audits kann der Hersteller auf eine Liste zugelassener Hersteller gesetzt werden. Zur Aufrechterhaltung der Qualifizierung des Herstellers sind in regelmäßigen Abständen Re-Auditierungen durchzuführen. Wird bei dem Audit auch die Produktionsstätte der COTS-Komponenten überprüft und hat der Hersteller mehrere Produktionsstätten, ist sicherzustellen, dass die Produktionsstätte überprüft wird, in der die Komponenten hergestellt werden.

Den Teams zur Durchführung von Audits und Besichtigungen beim Hersteller sollte Personal angehören, welches sowohl aus technischer Sicht als auch aus Sicht des Qualitätsmanagements über die notwendigen Kenntnisse verfügt. Zudem sollte das Personal mit den Verfahren zur Herstellung der Komponente vertraut sein.

Kategorie B

Hinsichtlich des Qualitätsmanagementsystems des Herstellers ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

Kategorie C

Hinsichtlich des Qualitätsmanagementsystems des Herstellers ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie C gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

**Qualitätssicherung während des Design- und Entwicklungsprozesses**

Kategorie A

Von Herstellern, die COTS-Komponenten zum Einsatz in Funktionen der Kategorie A herstellen, ist ein dokumentiertes Qualitätssicherungsprogramm zu unterhalten, dass während des gesamten Design- und Entwicklungsprozesses angewendet werden muss.

In diesem Qualitätssicherungsprogramm ist vorzusehen, dass Personen, die mit der Durchführung von Arbeiten im Rahmen des Design- und Entwicklungsprozesses beauftragt werden, die ihnen zugewiesenen Arbeiten kompetent durchführen können. Die Kompetenz der beteiligten Personen ist durch Kompetenz- und Schulungsnachweise zu belegen.

Im Rahmen des Qualitätssicherungsprogramms ist für jede Phase des Design- und Entwicklungsprozesses durch eine Überprüfung zu bestätigen, dass die Anforderungen der jeweiligen Phase erfüllt wurden.

Zudem müssen im Qualitätssicherungsprogramm des Herstellers ein System zum Konfigurationsmanagement, eine Kontrolle im Falle von Änderungen am Design sowie ein Verfahren zur Dokumentation vorhanden sein.

Kategorie B

Hinsichtlich der Qualitätssicherung während des Design- und Entwicklungsprozesses beim Hersteller ergeben sich keine Unterschiede zwischen den Sicherheitskategorien A und B. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

Kategorie C

Von Herstellern, die COTS-Komponenten zum Einsatz in Funktionen der Kategorie C herstellen, ist ein Qualitätssicherungsprogramm zu entwickeln, dass während des gesamten Design- und Entwicklungsprozesses angewendet werden muss.

In diesem Qualitätssicherungsprogramm ist vorzusehen, dass Personen, die mit der Durchführung von Arbeiten im Rahmen des Design- und Entwicklungsprozesses beauftragt werden, die ihnen zugewiesenen Arbeiten kompetent durchführen können.

Zudem müssen im Qualitätssicherungsprogramm des Herstellers ein System zum Konfigurationsmanagement, eine Kontrolle im Falle von Änderungen am Design sowie ein Verfahren zur Dokumentation vorhanden sein.

**Qualitätssicherung bei Verwendung von Werkzeugen**

Kategorie A

Wenn während des Design- und Entwicklungsprozesses von COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, vom Hersteller Werkzeuge (sowohl Software- als auch Hardwarewerkzeuge) verwendet werden, ist vom Hersteller sicherzustellen, dass diese Werkzeuge für ihren Einsatz qualifiziert sind.

Ist eine Qualifizierung der verwendeten Werkzeuge nicht möglich oder unzureichend, muss anhand von Informationen über die Verwendungsgeschichte der Werkzeuge, ihrer Stabilität, ihrer Benutzerdokumentation und bereits aufgetretener Fehler sowie ihrem Potenzial, Fehler in die COTS-Komponenten einzubringen oder vorhandene Fehler nicht zu erkennen, eine Bewertung der Werkzeuge hinsichtlich der Möglichkeit ihres Einsatzes erfolgen.

Kategorie B

Hinsichtlich der Qualitätssicherung bei Verwendung von Werkzeugen beim Hersteller ergeben sich keine Unterschiede zwischen den Sicherheitskategorien A und B. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

Kategorie C

Hinsichtlich der Qualitätssicherung bei Verwendung von Werkzeugen beim Hersteller ergeben sich für COTS-Komponenten, die in Funktionen der Kategorie C eingesetzt werden sollen, keine Anforderungen.

**Umgang mit Problemen oder Mängeln**

Kategorie A

Im Falle des Auftretens von Problemen oder Mängeln (z. B. bei bereits ausgelieferten, identischen COTS-Komponenten, Problemen beim Herstellungsprozess, usw.), welche die Qualität der COTS-Komponenten mindern könnten oder die Qualifizierung des Herstellers beeinflussen, muss der Hersteller über diese Probleme oder Mängel informieren. Beim Hersteller muss eine entsprechende Vorgehensweise zur Identifizierung solcher Probleme oder Mängel vorhanden sein. Außerdem muss der Hersteller über ein Programm verfügen, um bei aufgetretenen Problemen oder Mängeln wirkungsvolle Korrekturmaßnahmen durchführen zu können.

Treten Fehler an COTS-Komponenten auf, ist vom Hersteller sicherzustellen, dass alle Käufer dieser Komponenten über die aufgetretenen Fehler informiert werden.

Kategorie B

Hinsichtlich des Umgangs mit Problemen oder Mängeln ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

Kategorie C

Hinsichtlich des Umgangs mit Problemen oder Mängeln ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie C gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

**Qualitätsmanagement und Qualitätssicherung der Zulieferer**

Kategorie A

Werden vom Hersteller Zulieferer beauftragt, müssen die Zulieferer selbst sowie auch deren Zulieferer auf allen Ebenen der Lieferkette ebenfalls über ein dokumentiertes Qualitätsmanagementsystem nach ISO 9001 (oder gleichwertig) verfügen, welches durch ein unabhängiges Zertifikat zu bestätigen ist. Jeder vom Hersteller ausgewählte Zulieferer sollte im Rahmen eines Audits begutachtet werden, um sicherzustellen, dass das Qualitätsmanagementsystem eingehalten wird. Das Audit kann vom Hersteller durchgeführt werden, wenn die entsprechende Kompetenz hierfür beim Hersteller vorhanden ist.

Zudem sollten die vorab genannten Anforderungen hinsichtlich der Qualitätssicherung während des Design- und Entwicklungsprozesses, der Qualitätssicherung bei der Verwendung von Werkzeugen sowie dem Umgang mit Problemen oder Mängeln auf allen Ebenen der Lieferkette befolgt werden.

Kategorie B

Hinsichtlich des Qualitätsmanagements und der Qualitätssicherung der Zulieferer ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

Kategorie C

Hinsichtlich des Qualitätsmanagements und der Qualitätssicherung der Zulieferer ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie C gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

### 3.2.3 Design- und Entwicklungsprozess der COTS-Komponenten

Hinsichtlich des Aspektes des Design- und Entwicklungsprozesses der COTS-Komponenten wurden folgende Anforderungen entwickelt, die nachfolgend für die Kategorien A, B und C vorgestellt werden:

- Designprozess der COTS-Komponenten
- Lebenszyklus des Design- und Entwicklungsprozesses
- Konfigurationsmanagement für die Entwicklung von COTS-Komponenten
- Entwicklungssicherheitskonzept für COTS-Komponenten
- Softwareentwicklungsprozess für COTS-Komponenten

**Designprozess der COTS-Komponenten**

Kategorie A

Der Designprozess der COTS-Komponenten muss systematisch sein. Um den Designprozess beurteilen zu können, sind Nachweise über die Anwendung eines qualitätsorientierten Designprozesses beim Hersteller einzuholen. Diese Nachweise sind mit Anforderungen aus anderen Normen zu vergleichen, wobei Abweichungen festzustellen sind. Anschließend ist zu bewerten, ob diese Abweichungen akzeptabel sind oder nicht und ob kompensierende Maßnahmen ergriffen werden können.

Kategorie B

Hinsichtlich des Designprozesses der COTS-Komponenten ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

Kategorie C

Hinsichtlich des Designprozesses der COTS-Komponenten ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie C gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

**Lebenszyklus des Design- und Entwicklungsprozesses**

Kategorie A

Für COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, muss der Design- und Entwicklungsprozess der Hard- und Software einem Lebenszyklus folgen. Dabei sind Design und Entwicklung der Komponenten in Phasen zu unterteilen. Für jede dieser Phasen ist festzulegen, welche Zielsetzung in der Phase verfolgt wird und welche Eingangsinformationen für die jeweilige Phase vorliegen sowie welche Ausgangsinformationen erwartet werden. Zudem ist für jede Phase festzulegen, welche Organisation die erforderlichen Arbeiten durchführt, wer die Ergebnisse der jeweiligen Phase verifiziert sowie welche Werkzeuge für die durchzuführenden Arbeiten verwendet werden. Für alle durchgeführten Arbeiten in jeder Phase sind entsprechende Nachweise zu erbringen und zu dokumentieren.

Werden eingesetzte COTS-Komponenten aktualisiert, müssen die Änderungen im Lebenszyklus entsprechend implementiert werden und es ist gegebenenfalls eine Re-Qualifizierung der COTS-Komponenten vorzunehmen.

Kategorie B

Hinsichtlich des Lebenszyklus des Design- und Entwicklungsprozesses ergeben sich keine Unterschiede zwischen den Sicherheitskategorien A und B. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

Kategorie C

Für COTS-Komponenten, die Funktionen der Kategorie C ausführen sollen, sollte der Design- und Entwicklungsprozess der Hard- und Software einem Lebenszyklus folgen, wobei Design und Entwicklung der Komponenten in Phasen zu unterteilen sind. Für jede dieser Phasen sollte festgelegt werden, welche Zielsetzung in der Phase verfolgt wird und welche Eingangsinformationen für die jeweilige Phase vorliegen sowie welche Ausgangsinformationen erwartet werden. Zudem sollte für jede Phase festgelegt werden, welche Organisation die erforderlichen Arbeiten durchführt, wer die Ergebnisse der jeweiligen Phase verifiziert sowie welche Werkzeuge für die durchzuführenden Arbeiten verwendet werden. Für alle durchgeführten Arbeiten in jeder Phase sollten entsprechende Nachweise erbracht und dokumentiert werden.

Werden eingesetzte COTS-Komponenten aktualisiert, müssen die Änderungen im Lebenszyklus entsprechend implementiert werden und es ist gegebenenfalls eine Re-Qualifizierung der COTS-Komponenten vorzunehmen.

**Konfigurationsmanagement für die Entwicklung von COTS-Komponenten**

Kategorie A

Bereits ab Beginn der Entwicklung der COTS-Komponenten ist der Einsatz eines Konfigurationsmanagementsystems nachzuweisen. In diesem muss die gesamte Dokumentation zum Design der Komponenten, zu genutzten Prüfverfahren bei der Validierung sowie die Prüfberichte enthalten sein, wobei diese Informationen mit den vorliegenden Versionen der Hard- und Software der COTS-Komponenten zu verknüpfen sind.

Zudem muss das Konfigurationsmanagementsystem jede genehmigte Änderung an den COTS-Komponenten und zugehörige Analysen der Auswirkungen der Änderungen enthalten, wobei auch diese mit den vorliegenden Versionen der Hard- und Software zu verknüpfen sind.

Kategorie B

Ab Beginn der Validierung der COTS-Komponenten ist der Einsatz eines Konfigurationsmanagementsystems nachzuweisen. In diesem muss die gesamte Dokumentation zum Design der Komponenten, zu genutzten Prüfverfahren bei der Validierung sowie die Prüfberichte enthalten sein, wobei diese Informationen mit den vorliegenden Versionen der Hard- und Software der COTS-Komponenten zu verknüpfen sind.

Zudem muss das Konfigurationsmanagementsystem jede genehmigte Änderung an den COTS-Komponenten und zugehörige Analysen der Auswirkungen der Änderungen enthalten, wobei auch diese mit den vorliegenden Versionen der Hard- und Software zu verknüpfen sind.

Kategorie C

Hinsichtlich des Konfigurationsmanagements für die Entwicklung von COTS-Komponenten ergeben sich keine Unterschiede zwischen den Sicherheitskategorien B

und C. Für Kategorie C gelten somit die Anforderungen, die für Kategorie B aufgestellt wurden.

**Entwicklungssicherheitskonzept für COTS-Komponenten**

Kategorie A

Es ist ein Entwicklungssicherheitskonzept für COTS-Komponenten festzulegen, um dem Risiko von Fehlern bei der Entwicklung der COTS-Komponenten zu begegnen. Ein solches Konzept kann auf ermittelten Ausfallrisiken basieren und sollte die Ausgereiftheit der COTS-Komponenten berücksichtigen. Ist eine Verwendung der COTS-Komponenten außerhalb der in ihrem Datenblatt angegebenen Kennwerte erforderlich, ist die Zuverlässigkeit und technische Eignung der COTS-Komponenten im Rahmen des Entwicklungssicherheitskonzeptes nachzuweisen.

Zudem sind im Rahmen des Entwicklungssicherheitskonzeptes Überlegungen bei der Verwendung von COTS-Komponenten mit eingebettetem Mikrocode anzustellen, insbesondere, wenn dieser nicht vom Hersteller validiert wurde oder vom Endnutzer geändert werden soll. In diesem Fall ist sicherzustellen, dass für diesen Mikrocode ein Konformitätsnachweis gegeben wird, der der Verwendung der COTS-Komponenten angemessen ist. Das Vorhandensein eines solchen Mikrocodes ist zu dokumentieren.

Kategorie B

Hinsichtlich des Entwicklungssicherheitskonzeptes für COTS-Komponenten ergeben sich keine Unterschiede zwischen den Sicherheitskategorien A und B. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

Kategorie C

Es sollte ein Entwicklungssicherheitskonzept für COTS-Komponenten festgelegt werden, welches auf ermittelten Ausfallrisiken basieren kann und die Ausgereiftheit der COTS-Komponenten berücksichtigen sollte. Ist eine Verwendung der COTS-Komponenten außerhalb der in ihrem Datenblatt angegebenen Kennwerte erforderlich, sollte die Zuverlässigkeit und technische Eignung der COTS-Komponenten im Rahmen des Entwicklungssicherheitskonzeptes nachgewiesen werden.

**Softwareentwicklungsprozess für COTS-Komponenten**

Kategorie A

Die Entwicklung der Software für COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, muss in verifizierbaren Schritten nach einem Phasenmodell erfolgen. Die Implementierung der Software muss mit formalisierten, rechnergestützten Konstruktions-, Analyse- und Prüfmethoden gemäß dem aktuellen Stand von Wissenschaft und Technik erfolgen. Bei der Softwareentwicklung sind Anwendersoftware und Systemsoftware auch bezüglich ihrer Funktionen voneinander zu trennen. Der anforderungsgerechte Ablauf der Software muss unabhängig von Art und Umfang der zeitlichen Änderung der Eingangssignale sein.

Die Software für COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, muss einen einfachen und robusten Aufbau mit klar abgegrenzten Einheiten in einer übersichtlichen Programmstruktur haben. Der Funktionsumfang der Software ist dabei auf das für die Zielanwendung erforderliche Maß zu reduzieren.

Die Software für COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, muss nach vollständigen Entwicklungs-, Prüf-, Wartungs- und Qualitätssicherungsplänen erstellt und eingesetzt werden. Eine vollständige Entwicklungs-, Qualitätssicherungs- und Benutzerdokumentation muss vorhanden sein.

Es ist eine durchgängige Nachweisführung der korrekten Arbeitsweise der Software für COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, zu realisieren, wobei nach Möglichkeit zusätzlich eine Selbstüberwachung umzusetzen ist. Zudem ist eine konsistente Konfigurierung der Software sicherzustellen.

Kategorie B

Die Entwicklung der Software für COTS-Komponenten, die Funktionen der Kategorie B ausführen sollen, muss in verifizierbaren Schritten nach einem Phasenmodell und weitgehend mit rechnergestützten Werkzeugen erfolgen. Zur Sicherstellung der korrekten Arbeitsweise der Software sind bei der Softwareentwicklung rechnergestützte Testverfahren anzuwenden.

Die Software für COTS-Komponenten, die Funktionen der Kategorie B ausführen sollen, muss einen einfachen und robusten Aufbau mit klar abgegrenzten Einheiten in einer übersichtlichen Programmstruktur haben. Der Funktionsumfang der Software ist dabei auf das für die Zielanwendung erforderliche Maß zu reduzieren.

Die Software für COTS-Komponenten, die Funktionen der Kategorie B ausführen sollen, muss nach vollständigen Entwicklungs-, Prüf-, Wartungs- und Qualitätssicherungsplänen erstellt und eingesetzt werden. Eine vollständige Entwicklungs-, Qualitätssicherungs- und Benutzerdokumentation muss vorhanden sein.

Für die Arbeitsweise der Software für COTS-Komponenten, die Funktionen der Kategorie B ausführen sollen, ist eine Selbstüberwachung vorzusehen. Zudem ist eine konsistente Konfigurierung der Software sicherzustellen.

Kategorie C

Bei der Entwicklung der Software für COTS-Komponenten, die Funktionen der Kategorie C ausführen sollen, sind die einzelnen Entwicklungsschritte auszuweisen und das Erreichen der Entwicklungsziele nach jedem Schritt durch Prüfungen nachzuweisen und zu dokumentieren. Wenn möglich, sind bei den wesentlichen Entwicklungsschritten Softwarewerkzeuge zu verwenden.

Die Software für COTS-Komponenten, die Funktionen der Kategorie C ausführen sollen, muss nach einem Qualitätssicherungsplan gemäß den anerkannten Regeln der Technik erstellt werden. Eine vollständige Entwicklungs-, Qualitätssicherungs- und Benutzerdokumentation muss vorhanden sein.

### 3.2.4 Komplexität der COTS-Komponenten

Hinsichtlich des Aspektes der Komplexität der COTS-Komponenten wurden folgende Anforderungen entwickelt, die nachfolgend für die Kategorien A, B und C vorgestellt werden:

- Beitragende Attribute zur Komplexität von COTS-Komponenten
- Bewertung der Komplexität der COTS-Komponenten
- Möglichkeiten zur Konfiguration der COTS-Komponenten

- Vorhandensein nicht genutzter/nicht benötigter Funktionen
- Einfachheit der Software von COTS-Komponenten

**Beitragende Attribute zur Komplexität von COTS-Komponenten**

Kategorie A

Um die Komplexität von COTS-Komponenten zu beurteilen, sind nachfolgende Attribute zu berücksichtigen. Bei rechnerbasierten COTS-Komponenten sind dies beispielsweise die Anzahl der Software-Codezeilen, die Anzahl der möglichen Pfade durch die Software sowie die Häufigkeit von Verschachtelungen in der Software. Ebenfalls zu berücksichtigen sind die Verwendung einer fortgeschrittenen Datenverarbeitung, fortgeschrittene Schaltungen oder mehrere Verarbeitungselemente (z. B. Mehrkernprozessoren, Grafikverarbeitung, Vernetzung, komplexe Busumschaltung).

Weitere Attribute zur Beurteilung der Komplexität von COTS-Komponenten ist die Anzahl der Funktionen, die von den Komponenten ausgeführt werden können, die Anzahl und die Komplexität der funktionalen und physischen Schnittstellen (z. B. zwischen Hardware, Software, Mensch), die Möglichkeit der Konfigurierbarkeit der Funktionen sowie die Modularität der Software-/Hardwarearchitektur.

Kategorie B

Hinsichtlich der beitragenden Attribute zur Komplexität von COTS-Komponenten ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

Kategorie C

Hinsichtlich der beitragenden Attribute zur Komplexität von COTS-Komponenten ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie C gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

**Bewertung der Komplexität der COTS-Komponenten**

Kategorie A

Die Komplexität der COTS-Komponenten ist zu bewerten. COTS-Komponenten haben oftmals mehr Funktionalitäten als erforderlich, sind also komplexer als sie sein müssten. Alle Funktionalitäten der COTS-Komponenten müssen bei der Integration in das Zielsystem bekannt sein und berücksichtigt werden. Daher ist die Wahrscheinlichkeit, dass die Qualifizierung erfolgreich abgeschlossen werden kann, umso größer, je geringer die Komplexität der COTS-Komponenten ist. Es müssen also COTS-Komponenten ausgewählt werden, die zwar die Anforderungsspezifikation erfüllen, aber eine möglichst geringe Komplexität und einfache Funktionalität aufweisen.

Die Bewertung der Komplexität kann beispielsweise durch die Durchführung diverser Analysen, wie eine Fehlermöglichkeits- und Einflussanalyse (FMEA), Fehlerbaumanalyse (FTA) oder Gefährdungsanalyse (HAZOP) mit dem Schwerpunkt der Analysen auf das Design, die Herstellung und die Prüfung erfolgen.

Kategorie B

Hinsichtlich der Bewertung der Komplexität der COTS-Komponenten ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

Kategorie C

Hinsichtlich der Bewertung der Komplexität der COTS-Komponenten ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

**Möglichkeiten zur Konfiguration der COTS-Komponenten**

Kategorie A

Komplexe COTS-Komponenten können mehrere Funktionen und viele Konfigurationen dieser Funktionen aufweisen. Die möglichen Konfigurationen der Funktionen sind so zu

verwalten, dass die erforderlichen Einstellungen zur Ausführung der Zielfunktion konsistent angewendet werden können. Zudem muss die Konfiguration auf einer anderen Komponente repliziert werden können und eine kontrollierte Änderung der Konfiguration muss möglich sein, wenn diese erforderlich ist. Die Konfiguration der COTS-Komponenten kann beispielsweise die verwendeten Funktionen, Konfigurationen beim Einschalten, Mittel zur Verwaltung von Geräte-Resets sowie Konfigurationen der Betriebsbedingungen (z. B. Taktfrequenz, Stromversorgung, Temperatur) umfassen.

Es ist sicherzustellen, dass die Verwendung der COTS-Komponenten in der gewählten Konfiguration entsprechend der vorgesehenen Funktion definiert und überprüft wurde. Die COTS-Komponenten dürfen nur in den Konfigurationen betrieben werden, für die sie auch qualifiziert worden sind. Dazu sind bei der Qualifizierung die Konditionen und Annahmen festzulegen und zu dokumentieren, für welche die Qualifizierung gültig ist.

Werden die COTS-Komponenten zur Ausführung von Funktionen der Kategorie A in mehreren Redundanten betrieben, muss sichergestellt werden, dass notwendige Änderungen der Konfiguration in nur einer Redundante und nicht in mehreren Redundanten gleichzeitig durchgeführt werden.

Die Möglichkeiten zur Konfiguration der COTS-Komponenten sind so zu gestalten, dass eine versehentliche, unbeabsichtigte oder unbefugte Einstellung nicht möglich ist. Es ist sicherzustellen, dass mehr als ein Fehler notwendig ist, bevor ein Fehler bei der Einstellung eines Konfigurationsparameters begangen werden kann.

Besteht die Möglichkeit kritischer Konfigurationseinstellungen, also Einstellungen, welche für die ordnungsgemäße Nutzung der COTS-Komponenten notwendig sind und bei deren Änderung das Verhalten der COTS-Komponenten so beeinflusst werden kann, dass die vorgesehene Funktion nicht mehr erfüllt wird, sind geeignete Abhilfemaßnahmen für den Fall einer Änderung festzulegen.

Kategorie B

Hinsichtlich der Möglichkeiten zur Konfiguration der COTS-Komponenten ergeben sich keine Unterschiede zwischen den Sicherheitskategorien A und B. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

Kategorie C

Die möglichen Konfigurationen der Funktionen sollten so verwaltet werden, dass die erforderlichen Einstellungen zur Ausführung der Zielfunktion konsistent angewendet werden können. Zudem sollte die Konfiguration auf einer anderen Komponente repliziert werden können und eine kontrollierte Änderung der Konfiguration sollte, wenn erforderlich, möglich sein.

Es ist sicherzustellen, dass die Verwendung der COTS-Komponenten in der gewählten Konfiguration entsprechend der vorgesehenen Funktion definiert und überprüft wurde. Die COTS-Komponenten dürfen nur in den Konfigurationen betrieben werden, für die sie auch qualifiziert worden sind. Dazu sind bei der Qualifizierung die Konditionen und Annahmen festzulegen und zu dokumentieren, für welche die Qualifizierung gültig ist.

Die Möglichkeiten zur Konfiguration der COTS-Komponenten sollten so gestaltet sein, dass eine versehentliche, unbeabsichtigte oder unbefugte Einstellung nicht möglich ist.

Besteht die Möglichkeit kritischer Konfigurationseinstellungen, also Einstellungen, welche für die ordnungsgemäße Nutzung der COTS-Komponenten notwendig sind und bei deren Änderung das Verhalten der COTS-Komponenten so beeinflusst werden kann, dass die vorgesehene Funktion nicht mehr erfüllt wird, sollten geeignete Abhilfemaßnahmen für den Fall einer Änderung festgelegt werden.

**Vorhandensein nicht genutzter/nicht benötigter Funktionen**

Kategorie A

In der Zielanwendung nicht genutzte/nicht benötigte Funktionen von COTS-Komponenten sind offenzulegen. COTS-Komponenten, die in Funktionen der Kategorie A eingesetzt werden sollen, dürfen keine Funktionen enthalten, die in der Zielanwendung nicht genutzt/nicht benötigt werden. Lässt sich ein Vorhandensein solcher Funktionen nicht verhindern, sind geeignete Mittel zur Deaktivierung dieser Funktionen zu wählen. Zudem ist sicherzustellen, dass diese deaktivierten Funktionen nicht versehentlich wieder aktiviert werden können. Es ist nachzuweisen, dass die nicht genutzten/nicht benötigten Funktionen der COTS-Komponenten die Integrität und Verfügbarkeit der genutzten Funktionen nicht beeinträchtigen.

Kategorie B

In der Zielanwendung nicht genutzte/nicht benötigte Funktionen von COTS-Komponenten sind offenzulegen. COTS-Komponenten, die in Funktionen der Kategorie B eingesetzt werden sollen, sollten keine Funktionen enthalten, die in der Zielanwendung nicht genutzt/nicht benötigt werden. Sind solche Funktionen in den COTS-Komponenten enthalten, sollten diese durch Einsatz geeigneter Mittel deaktiviert werden und es sollte sichergestellt werden, dass die deaktivierten Funktionen nicht versehentlich wieder aktiviert werden können. Es ist nachzuweisen, dass die nicht genutzten/nicht benötigten Funktionen der COTS-Komponenten die Integrität und Verfügbarkeit der genutzten Funktionen nicht beeinträchtigen.

Kategorie C

In der Zielanwendung nicht genutzte/nicht benötigte Funktionen von COTS-Komponenten sind offenzulegen. Es ist nachzuweisen, dass die nicht genutzten/nicht benötigten Funktionen der COTS-Komponenten die Integrität und Verfügbarkeit der genutzten Funktionen nicht beeinträchtigen.

**Einfachheit der Software von COTS-Komponenten**

Kategorie A

Die in COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, eingesetzte Software muss eine einfache und begrenzte Funktionalität besitzen. Die Funktionen müssen eindeutig umschrieben und spezifiziert sein. Zudem müssen die Funktionen für eine Verifikation und/oder einen Test unter allen möglichen Betriebsarten geeignet sein.

Die Software-Programmstruktur sollte modular, übersichtlich und leicht verständlich aufgebaut sein. Rekursive Strukturen und Code-Kompaktierung sollten vermieden werden. Entsprechend ist bei der Softwareauslegung eine top-down-Vorgehensweise der bottom-up-Vorgehensweise vorzuziehen und anwendungsorientierte Sprachen sollten gegenüber maschinenorientierten Sprachen bevorzugt verwendet werden.

Kategorie B

Die in COTS-Komponenten, die Funktionen der Kategorie B ausführen sollen, eingesetzte Software sollte eine einfache und begrenzte Funktionalität besitzen. Die Funktionen sollten eindeutig umschrieben und spezifiziert sein. Zudem sollten die Funktionen für eine Verifikation und/oder einen Test unter allen möglichen Betriebsarten geeignet sein.

Kategorie C

Es ist von Vorteil, wenn die in COTS-Komponenten, die Funktionen der Kategorie C ausführen sollen, eingesetzte Software eine einfache und begrenzte Funktionalität besitzt. Die Funktionen sollten eindeutig umschrieben und spezifiziert sein.

### 3.2.5 Technische Eigenschaften und Einsatzort bzw. -art der COTS-Komponenten

Hinsichtlich des Aspektes der technischen Eigenschaften und dem Einsatzort bzw. der Einsatzart der COTS-Komponenten wurden folgende Anforderungen entwickelt, die nachfolgend für die Kategorien A, B und C vorgestellt werden:

- Funktionale Eignung der COTS-Komponenten für die Zielanwendung
- Qualitätssicherung der COTS-Komponenten für die Zielanwendung
- Integration der COTS-Komponenten in die Zielanwendung
- Einsatz der COTS-Komponenten in der Zielanwendung
- Umgebungsbedingungen am Einsatzort der COTS-Komponenten

**Funktionale Eignung der COTS-Komponenten für die Zielanwendung**

Kategorie A

Für COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, ist die funktionale Eignung der Komponenten zur Ausführung der geforderten Funktionen zu betrachten. Dabei sind die Hauptfunktionen der COTS-Komponenten zu bewerten, welche die funktionalen Anforderungen erfüllen oder übertreffen müssen. Die COTS-

Komponenten müssen in der Lage sein, über den gesamten Anwendungsbereich betrieben zu werden und die geforderte Genauigkeit und Wiederholbarkeit zu erbringen. Alle Hardware-Fehlerarten sowie möglichst alle systematische Fehlermöglichkeiten der COTS-Komponenten sind zu definieren und ihr Auftreten muss erkannt und gemeldet werden und eine akzeptabel niedrige Wahrscheinlichkeit für ihr Auftreten aufweisen.

COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, sollten möglichst keine Funktionen beinhalten, die nicht Teil der Hauptfunktionen sind, aber erforderlich sind, um Parameter der Hauptfunktionen anzupassen oder die Zuverlässigkeit der COTS-Komponenten zu erhöhen. Ist der Einsatz solcher Funktionen unumgänglich, ist nachzuweisen, dass der Betrieb oder der Ausfall dieser Funktionen die Hauptfunktionen nicht unzulässig beeinträchtigt.

COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, sollten keine zusätzlichen Funktionen, die nicht Teil der erforderlichen Sicherheitsfunktion sind, aufweisen. Kann das Vorhandensein solcher Funktionen nicht ausgeschlossen werden, ist nachzuweisen, dass die Funktionen unter allen Betriebsbedingungen so konfiguriert werden können, dass die Hauptfunktionen nicht beeinträchtigt werden.

Die Beurteilung der funktionalen Eignung von COTS-Komponenten kann von mehreren Betreibern gemeinsam durchgeführt werden. Orts- und anlagenspezifische Anforderungen sind bei dieser Vorgehensweise gesondert zu betrachten. Bereits für den Einsatz zugelassene COTS-Komponenten können bei Vorliegen einer funktionalen Eignung auch in anderen Anlagen verwendet werden, wobei die standortspezifische Eignung separat zu analysieren ist.

Es kann wirtschaftlich sinnvoll sein, COTS-Komponenten in mehreren Funktionen einzusetzen. Beispielsweise können die Kosten für die Qualifizierung der COTS-Komponenten gesenkt werden, wenn eine Qualifizierung durchgeführt wird, um mehrere Zielanwendungen mit einer COTS-Komponente zu betreiben. Bei einer solchen Vorgehensweise sind spezifische Anforderungen, die sich aus der Zielanwendung ergeben, sorgfältig zu prüfen und zu berücksichtigen. Zudem sind die sicherheitstechnischen Bedeutungen der verschiedenen Anwendungen zu vergleichen und Fehleranalysen zu überarbeiten, um sicherzustellen, dass alle Zielanwendungen angemessen abgedeckt werden.

Kategorie B

Für COTS-Komponenten, die Funktionen der Kategorie B ausführen sollen, ist die funktionale Eignung der Komponenten zur Ausführung der geforderten Funktionen zu betrachten. Dabei sind die Hauptfunktionen der COTS-Komponenten zu bewerten, welche die funktionalen Anforderungen erfüllen oder übertreffen müssen. Die COTS-Komponenten müssen in der Lage sein, über den gesamten Anwendungsbereich betrieben zu werden und die geforderte Genauigkeit und Wiederholbarkeit zu erbringen.

COTS-Komponenten, die Funktionen der Kategorie B ausführen sollen, sollten möglichst keine Funktionen beinhalten, die nicht Teil der Hauptfunktionen sind, aber erforderlich sind, um Parameter der Hauptfunktionen anzupassen oder die Zuverlässigkeit der COTS-Komponenten zu erhöhen. Ist der Einsatz solcher Funktionen unumgänglich, ist nachzuweisen, dass der Betrieb oder der Ausfall dieser Funktionen die Hauptfunktionen nicht unzulässig beeinträchtigt.

Für COTS-Komponenten, die Funktionen der Kategorie B ausführen sollen und die zusätzliche Funktionen aufweisen, die nicht Teil der erforderlichen Sicherheitsfunktion sind, ist nachzuweisen, dass diese Funktionen unter allen Betriebsbedingungen so konfiguriert werden können, dass die Hauptfunktionen nicht beeinträchtigt werden.

Die Beurteilung der funktionalen Eignung von COTS-Komponenten kann von mehreren Betreibern gemeinsam durchgeführt werden. Orts- und anlagenspezifische Anforderungen sind bei dieser Vorgehensweise gesondert zu betrachten. Bereits für den Einsatz zugelassene COTS-Komponenten können bei Vorliegen einer funktionalen Eignung auch in anderen Anlagen verwendet werden, wobei die standortspezifische Eignung separat zu analysieren ist.

Es kann wirtschaftlich sinnvoll sein, COTS-Komponenten in mehreren Funktionen einzusetzen. Beispielsweise können die Kosten für die Qualifizierung der COTS-Komponenten gesenkt werden, wenn eine Qualifizierung durchgeführt wird, um mehrere Zielanwendungen mit einer COTS-Komponente zu betreiben. Bei einer solchen Vorgehensweise sind spezifische Anforderungen, die sich aus der Zielanwendung ergeben, sorgfältig zu prüfen und zu berücksichtigen. Zudem sind die sicherheitstechnischen Bedeutungen der verschiedenen Anwendungen zu vergleichen und Fehleranalysen zu überarbeiten, um sicherzustellen, dass alle Zielanwendungen angemessen abgedeckt werden.

Kategorie C

Für COTS-Komponenten, die Funktionen der Kategorie C ausführen sollen, ist die funktionale Eignung der Komponenten zur Ausführung der geforderten Funktionen zu betrachten. Dabei sind die Hauptfunktionen der COTS-Komponenten zu bewerten, welche die funktionalen Anforderungen erfüllen oder übertreffen müssen. Die COTS-Komponenten müssen in der Lage sein, über den gesamten Anwendungsbereich betrieben zu werden und die geforderte Genauigkeit und Wiederholbarkeit zu erbringen.

Die Beurteilung der funktionalen Eignung von COTS-Komponenten kann von mehreren Betreibern gemeinsam durchgeführt werden. Orts- und anlagenspezifische Anforderungen sind bei dieser Vorgehensweise gesondert zu betrachten. Bereits für den Einsatz zugelassene COTS-Komponenten können bei Vorliegen einer funktionalen Eignung auch in anderen Anlagen verwendet werden, wobei die standortspezifische Eignung separat zu analysieren ist.

Es kann wirtschaftlich sinnvoll sein, COTS-Komponenten in mehreren Funktionen einzusetzen. Beispielsweise können die Kosten für die Qualifizierung der COTS-Komponenten gesenkt werden, wenn eine Qualifizierung durchgeführt wird, um mehrere Zielanwendungen mit einer COTS-Komponente zu betreiben. Bei einer solchen Vorgehensweise sind spezifische Anforderungen, die sich aus der Zielanwendung ergeben, sorgfältig zu prüfen und zu berücksichtigen. Zudem sind die sicherheitstechnischen Bedeutungen der verschiedenen Anwendungen zu vergleichen und Fehleranalysen zu überarbeiten, um sicherzustellen, dass alle Zielanwendungen angemessen abgedeckt werden.

**Qualitätssicherung der COTS-Komponenten für die Zielanwendung**

Kategorie A

Für COTS-Komponenten, die zur Ausführung von Funktionen der Kategorie A eingesetzt werden sollen, ist eine Verifikations- und Validationsplanung zu erstellen. Durch diese ist sicherzustellen, dass alle sicherheitstechnisch geforderten Systemfunktionen vollständig getestet werden und das bestimmungsgemäße Verhalten des Systems nachgewiesen wird. Zudem sind Nachweise zu erbringen über die Instandhaltbarkeit des Systems bei Einzelfehlern sowie zum Ausschluss eines nicht tolerierbaren Verhaltens des Systems.

Zur Eingrenzung des Aufwands für Verifikation und Validierung können bereits zertifizierte Eigenschaften der COTS-Komponenten einbezogen werden. Werden Eigenschaften der COTS-Komponenten benötigt, die zusätzlich zu den bereits zertifizierten Eigenschaften erforderlich sind, sind diese vor dem Einsatz der Komponenten zu verifizieren.

Für COTS-Komponenten zur Ausführung von Funktionen der Kategorie A ist außerdem ein effektives Konfigurationsmanagement sowie Prinzipien zur Identifizierung der relevanten Hard- und Softwarekomponenten einzuführen.

Kategorie B

Hinsichtlich der Qualitätssicherung der COTS-Komponenten für die Zielanwendung ergeben sich keine Unterschiede zwischen den Sicherheitskategorien A und B. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

Kategorie C

Für COTS-Komponenten, die zur Ausführung von Funktionen der Kategorie C eingesetzt werden sollen, ist eine Verifikations- und Validationsplanung zu erstellen. Durch diese ist sicherzustellen, dass alle sicherheitstechnisch geforderten Systemfunktionen vollständig getestet werden und das bestimmungsgemäße Verhalten des Systems nachgewiesen wird.

Vom Hersteller zugesicherte und noch nicht zertifizierte oder anderweitig geprüfte Eigenschaften der COTS-Komponenten müssen vor dem Einsatz der Komponenten von einer vom Hersteller unabhängigen Organisation verifiziert werden.

Für COTS-Komponenten zur Ausführung von Funktionen der Kategorie C ist außerdem ein Konfigurationsmanagement sowie Prinzipien zur Identifizierung der relevanten Hard- und Softwarekomponenten einzuführen.

**Integration der COTS-Komponenten in die Zielanwendung**

Kategorie A

Sollen COTS-Komponenten in Anwendungen integriert werden, die Funktionen der Kategorie A ausführen, ist zu bewerten, ob das Verhalten, die Einschränkungen sowie weitere zu treffende Annahmen und Bedingungen für die COTS-Komponenten für den Einsatz in der spezifischen Zielanwendung geeignet sind. Zudem sind die Auswirkungen systematischer Ausfälle mehrerer identischer COTS-Komponenten zu berücksichtigen und es ist nachzuweisen, dass Maßnahmen zum Schutz vor systematischen Ausfällen implementiert wurden und wirksam sind.

Da sich die Versionen der COTS-Komponenten schnell ändern können, ist sicherzustellen, dass die durchgeführte Bewertung zur Integration der COTS-Komponenten in die Zielanwendung für die aktuelle Version der einzubauenden Komponenten anwendbar ist. Dazu ist zu überprüfen, dass der Hersteller ein konsistentes Produkt während des Herstellungsprozesses gewährleistet und dass Informationen zu Änderungen an Komponenten durch den Hersteller weitergegeben werden. Zudem ist zu prüfen, dass die bewertete Komponente mit der verwendeten übereinstimmt und dass die Komponenten während der Auslieferung nicht verändert wurden.

COTS-Komponenten, die in Anwendungen zur Ausführung von Funktionen der Kategorie A eingesetzt werden, dürfen ausschließlich in einer Weise eingesetzt werden, die nicht das Risiko eines vollständigen Ausfalls einer Sicherheitsfunktion birgt.

Kategorie B

Sollen COTS-Komponenten in Anwendungen integriert werden, die Funktionen der Kategorie B ausführen, ist zu bewerten, ob das Verhalten, die Einschränkungen sowie weitere zu treffende Annahmen und Bedingungen für die COTS-Komponenten für den Einsatz in der spezifischen Zielanwendung geeignet sind. Zudem sind die Auswirkungen systematischer Ausfälle mehrerer identischer COTS-Komponenten zu berücksichtigen und es ist nachzuweisen, dass Maßnahmen zum Schutz vor systematischen Ausfällen implementiert wurden und wirksam sind.

Da sich die Versionen der COTS-Komponenten schnell ändern können, ist sicherzustellen, dass die durchgeführte Bewertung zur Integration der COTS-Komponenten in die

Zielanwendung für die aktuelle Version der einzubauenden Komponenten anwendbar ist. Dazu ist zu überprüfen, dass der Hersteller ein konsistentes Produkt während des Herstellungsprozesses gewährleistet und dass Informationen zu Änderungen an den Komponenten durch den Hersteller weitergegeben werden. Zudem ist zu prüfen, dass die bewertete Komponente mit der verwendeten übereinstimmt und dass die Komponenten während der Auslieferung nicht verändert wurden.

Ist eine Änderung der COTS-Komponenten unbedingt erforderlich, können die COTS-Komponenten bei bestimmten Änderungen an der Hardware oder sehr geringfügigen Änderungen an der Software weiterhin als geeignet für die Verwendung in der Zielanwendung bewertet werden, sofern diese Änderungen erforderlich waren und nicht dazu führen, dass sich die Hauptfunktion der Komponenten konzeptionell ändert. Die Änderungen müssen dabei von geringem Umfang und einfach zu überprüfen sein.

COTS-Komponenten, die in Anwendungen zur Ausführung von Funktionen der Kategorie B eingesetzt werden, sollten ausschließlich in einer Weise eingesetzt werden, die nicht das Risiko eines vollständigen Ausfalls einer Sicherheitsfunktion birgt. Für den Fall der geplanten Verwendung von COTS-Komponenten in allen Redundanten eines Systems mit der Gefahr, dass der Ausfall dieser Komponenten den vollständigen Ausfall einer Sicherheitsfunktion bewirken würde, ist ausschließlich eine schrittweise Einführung der COTS-Komponenten in das System unter Berücksichtigung einer anfänglichen Verifizierungsphase, in welcher die Komponenten nur in einer Redundanz in Betrieb genommen werden, erlaubt. Zudem ist zu prüfen und sicherzustellen, dass in allen eingesetzten Komponenten die korrekten Parametereinstellungen vorliegen. Außerdem sind Testfälle für die Inbetriebnahme der COTS-Komponenten zu definieren, bei denen auch die dynamischen Aspekte des Systems (z. B. Reaktionszeiten der Komponenten, Reihenfolge und Priorität der Schutzmaßnahmen) berücksichtigt werden müssen.

Kategorie C

Sollen COTS-Komponenten in Anwendungen integriert werden, die Funktionen der Kategorie C ausführen, ist zu bewerten, ob das Verhalten, die Einschränkungen sowie weitere zu treffende Annahmen und Bedingungen für die COTS-Komponenten für den Einsatz in der spezifischen Zielanwendung geeignet sind.

Da sich die Versionen der COTS-Komponenten schnell ändern können, ist sicherzustellen, dass die durchgeführte Bewertung zur Integration der COTS-Komponenten in die

Zielanwendung für die aktuelle Version der einzubauenden Komponenten anwendbar ist. Dazu sollte überprüft werden, ob der Hersteller ein konsistentes Produkt während des Herstellungsprozesses gewährleistet und dass Informationen zu Änderungen an Komponenten durch den Hersteller weitergegeben werden. Zudem sollte geprüft werden, dass die bewertete Komponente mit der verwendeten übereinstimmt. Bei Änderungen an COTS-Komponenten (bestimmte Änderungen an der Hardware oder sehr geringfügigen Änderungen an der Software) können die Komponenten weiterhin als geeignet für die Verwendung in der Zielanwendung bewertet werden, sofern diese Änderungen erforderlich waren und nicht dazu führen, dass sich die Hauptfunktion der Komponenten konzeptionell ändert.

Ist der Einsatz von COTS-Komponenten, die in Anwendungen zur Ausführung von Funktionen der Kategorie C eingesetzt werden sollen, in allen Redundanten eines Systems geplant und besteht die Gefahr, dass der Ausfall dieser Komponenten den vollständigen Ausfall einer Sicherheitsfunktion bewirken würde, darf ausschließlich eine schrittweise Einführung der COTS-Komponenten in das System erfolgen.

**Einsatz der COTS-Komponenten in der Zielanwendung**

Kategorie A

Sollen COTS-Komponenten zur Ausführung von Funktionen der Kategorie A eingesetzt werden, dürfen nur Komponenten verwendet werden, die entweder eine kerntechnische Typprüfung durchlaufen haben oder die speziell für den Einsatz in industriellen Sicherheitsanwendungen entwickelt und entsprechend zertifiziert worden sind (z. B. nach DIN EN 61508 /DIN 11/).

Zudem müssen die COTS-Komponenten zum Einsatz in Funktionen der Kategorie A mit für die Zielanwendung geeigneten Eigenschaften zum Erhalt der erforderlichen Zuverlässigkeit (z. B. Fehlertoleranz, Unabhängigkeit, Funktionsverteilung, Funktionsparallelität) ausgestattet sein. Die Eignung der COTS-Komponenten für die spezifische Zielanwendung ist nachzuweisen.

Werden diversitäre Sicherheitsfunktionen der Kategorie A zur Aufrechterhaltung eines Schutzziels gefordert, sind diese durch mindestens zwei voneinander unabhängige leittechnische Systeme zu erbringen. Der Ausfall eines dieser beiden Systeme darf nicht zu

untolerierbaren Auswirkungen führen und es muss nachgewiesen werden, dass der Ausfall eines der Systeme die Weiterfunktion der anderen Systeme nicht beeinträchtigt.

Kategorie B

Sollen COTS-Komponenten zur Ausführung von Funktionen der Kategorie B eingesetzt werden, dürfen Komponenten verwendet werden, die entweder eine kerntechnische Typprüfung durchlaufen haben oder die speziell für den Einsatz in industriellen Sicherheitsanwendungen entwickelt und entsprechend zertifiziert worden sind (z. B. nach DIN EN 61508 /DIN 11/). Außerdem können Komponenten eingesetzt werden, die aus technischer Sicht für den Aufbau hochzuverlässiger Systeme geeignet sind und zudem unter Einhaltung der einsatzspezifischen Randbedingungen weitere ergänzende Prüfungen durchlaufen haben müssen. Die Nutzung von COTS-Komponenten, die bereits mit hohen Stückzahlen und in vielfältigen Anwendungen eingesetzt werden, kann dabei den Vorteil bringen, dass belastbare Angaben zur Betriebserfahrung der Komponenten beim Hersteller vorliegen.

COTS-Komponenten zum Einsatz in Funktionen der Kategorie B müssen zudem diverse Voraussetzungen erfüllen, wie beispielsweise ausreichende Mechanismen zur Selbstüberwachung, gerichtetes Ausfallverhalten sowie Eigenschaften zur Protokollierung von Fehlerzuständen. Außerdem dürfen nur Funktionen realisiert werden, die sicherheitsgerichtet sind und bei aktivem Versagen nicht zur Anforderung von Funktionen der Kategorie A führen.

Die Funktionen der Kategorie B sind den einzelnen leittechnischen Systemen so zuzuordnen, dass es beim Ausfall eines Systems nicht zu untolerierbaren Auswirkungen kommt und keine unzulässigen Betriebszustände auftreten.

Kategorie C

Sollen COTS-Komponenten zur Ausführung von Funktionen der Kategorie C eingesetzt werden, dürfen Komponenten verwendet werden, die entweder eine kerntechnische Typprüfung durchlaufen haben oder die speziell für den Einsatz in industriellen Sicherheitsanwendungen entwickelt und entsprechend zertifiziert worden sind (z. B. nach DIN EN 61508 /DIN 11/). Außerdem dürfen Komponenten eingesetzt werden, die aus technischer Sicht für den Aufbau hochzuverlässiger Systeme geeignet sind und zudem

unter Einhaltung der einsatzspezifischen Randbedingungen weitere ergänzende Prüfungen durchlaufen haben. Die Nutzung von COTS-Komponenten, die bereits mit hohen Stückzahlen und in vielfältigen Anwendungen eingesetzt werden, kann dabei den Vorteil bringen, dass belastbare Angaben zur Betriebserfahrung der Komponenten beim Hersteller vorliegen.

COTS-Komponenten zum Einsatz in Funktionen der Kategorie C sollten zudem diverse Voraussetzungen erfüllen, wie beispielsweise ausreichende Mechanismen zur Selbstüberwachung, gerichtetes Ausfallverhalten sowie Eigenschaften zur Protokollierung von Fehlerzuständen.

**Umgebungsbedingungen am Einsatzort der COTS-Komponenten**

Kategorie A

Für COTS-Komponenten, die zur Ausführung von Funktionen der Kategorie A eingesetzt werden sollen, sind die Umgebungsbedingungen, unter denen die Komponenten ihre Funktion ausführen müssen, festzulegen. Es ist durch eine Qualifizierung der COTS-Komponenten nachzuweisen, dass die Komponenten für den Einsatz unter den festgelegten Umgebungsbedingungen geeignet sind. Zur Durchführung der Qualifizierung ist die Bestimmung geeigneter Merkmale erforderlich, deren Erfüllung im Rahmen der Qualifizierung nachzuweisen ist. Für Software ist in der Regel keine Qualifizierung hinsichtlich der Umgebungsbedingungen erforderlich.

Kategorie B

Hinsichtlich der Umgebungsbedingungen am Einsatzort der COTS-Komponenten ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

Kategorie C

Hinsichtlich der Umgebungsbedingungen am Einsatzort der COTS-Komponenten ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie C gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

### 3.2.6 Qualifizierung von COTS-Komponenten

Hinsichtlich des Aspektes der Qualifizierung von COTS-Komponenten wurden folgende Anforderungen entwickelt, die nachfolgend für die Kategorien A, B und C vorgestellt werden:

- Umfang der Qualifizierung von COTS-Komponenten
- Vorgehensweise bei der Qualifizierung von COTS-Komponenten
- Einbeziehung der Betriebserfahrung bei der Qualifizierung
- Analyse der Fehlermöglichkeiten von COTS-Komponenten
- Cybersicherheit von COTS-Komponenten

**Umfang der Qualifizierung von COTS-Komponenten**

Kategorie A

Für COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, ist festzulegen, welchen Umfang eine Qualifizierung haben soll. Der Umfang kann dabei davon abhängen, ob die Komponenten nur zum Einsatz in einer Zielanwendung vorgesehen sind oder ob die Komponenten in verschiedenen Zielanwendungen in einer Anlage oder sogar mehreren Anlagen zum Einsatz kommen sollen.

Um den Umfang der Qualifizierung von COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, zu bestimmen, sind vor der Qualifizierung die Anforderungen an die COTS-Komponenten zu bestimmen. Diese ergeben sich z. B. aus der geplanten Zielfunktion bzw. den geplanten Zielfunktionen, der Klassifizierung dieser Zielfunktion(en), den Folgen eines fehlerhaften Verhaltens der COTS-Komponenten (z. B. bei Verursachung einer Fehlauslösung), Anforderungen an die Cybersicherheit oder Anforderungen bezüglich der Umgebungsbedingungen.

Ist der Einsatz der COTS-Komponenten in verschiedenen Zielanwendungen oder in mehreren Anlagen geplant, besteht die Möglichkeit, den Umfang der Qualifizierung von COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, in zwei Teile zu unterteilen. Der erste Teil der Qualifizierung erfolgt auf generischer Ebene ohne Berücksichtigung der anwendungsspezifischen Anforderungen. Dieser Teil der Qualifizierung

kann beispielsweise bei Verwendung in verschiedenen Anlagen, verschiedenen Zielanwendungen oder unter unterschiedlichen Umgebungsbedingungen verwendet werden. Der zweite Teil der Qualifizierung erfolgt auf anwendungsspezifischer Ebene unter Berücksichtigung der anwendungsspezifischen Anforderungen. Dabei ist darauf zu achten, dass das Verhalten der Komponenten, welches in der generischen Qualifizierung berücksichtigt wurde, geeignet ist, um die anwendungsspezifischen Anforderungen zu erfüllen. Außerdem muss die Qualifizierung auf anwendungsspezifischer Ebene unter Berücksichtigung der Betriebsumgebung (z. B. Umgebungsbedingungen wie Temperatur und Vibrationen, infrastrukturelle Bedingungen bezüglich Stromversorgung, physikalische Anforderungen wie Platzbedarf für Einbau und Wartung, Anforderungen an Schnittstellen) stattfinden, die später in der Zielanwendung zu erwarten sind.

Besitzen die COTS-Komponenten eine hohe Komplexität, ist die Qualifizierung entsprechend aufwendig oder sogar unmöglich. Um den Umfang der Qualifizierung zu verringern, können nicht genutzte Attribute von COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, in ihrer Nutzung eingeschränkt werden, um die Komplexität der Komponenten zu verringern. Beispiele hierfür sind Einschränkungen nicht benötigter Funktionen der COTS-Komponenten, Beschränkungen der möglichen Eingänge, Beschränkungen der Konfigurierbarkeit oder Einschränkungen möglicher Umgebungsbedingungen. Werden solche Einschränkungen vorgenommen, dann muss nachgewiesen werden, dass die eingeschränkten Attribute nicht zu einer Beeinträchtigung der erforderlichen Funktionen (insbesondere der Sicherheitsfunktionen) der COTS-Komponenten führen können.

Kategorie B

Hinsichtlich des Umfangs der Qualifizierung von COTS-Komponenten ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

Kategorie C

Hinsichtlich des Umfangs der Qualifizierung von COTS-Komponenten ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie C gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

**Vorgehensweise bei der Qualifizierung von COTS-Komponenten**

Kategorie A

Durch die Qualifizierung von COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, ist sicherzustellen, dass die COTS-Komponenten die vorgesehenen Funktionen in den Systemen, in denen sie eingesetzt werden sollen, unter den vorgesehenen Betriebsumgebungen sicher ausführen werden. Dazu ist nachzuweisen, dass die COTS-Komponenten alle in der Anforderungsspezifikation angegebenen Anforderungen erfüllen.

Zur Überprüfung, ob alle Anforderungen aus der Anforderungsspezifikation erfüllt sind, ist zu überprüfen, ob die Angaben des Herstellers zu den Komponenten sowie zum Entwicklungs- und Herstellungsprozess durch Nachweise wie beispielsweise Konstruktionsunterlagen, Prüfprotokolle oder Kompetenznachweise belegt sind. Neben der generischen Bewertung unter Berücksichtigung der vom Hersteller gegebenen Angaben ist zudem eine spezifische Bewertung der Komponenten erforderlich, um sicherzustellen, dass die Komponenten für die spezifische Anwendung geeignet sind.

Bereits vorhandene Qualifizierungen und Zertifizierungen (insbesondere nach DIN IEC 61508 /DIN 11/) von COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, können in die Qualifizierung einfließen, führen aber nicht automatisch zur Qualifizierung der Komponenten. Dabei können sowohl Qualifizierungen aus der Nuklearindustrie aber auch aus anderen Industriezweigen Berücksichtigung finden, sofern die gesamte Dokumentation der bereits bestehenden Qualifizierungen/Zertifizierungen vorliegt. Bereits vorhandene Qualifizierungen und Zertifizierungen bedürfen in jedem Falle einer Überprüfung hinsichtlich der Möglichkeit ihrer Berücksichtigung.

Ist eine Qualifizierung der COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, anhand der vorliegenden Nachweise des Herstellers sowie bereits vorhandener Qualifizierungen/Zertifizierungen nicht vollumfänglich möglich, besteht die Möglichkeit ergänzender Tests und Analysen, um die vorhandenen Lücken für eine erfolgreiche Qualifizierung zu schließen. Werden ergänzende Tests und Analysen durchgeführt, sind die dabei verwendeten Spezifikationen und die Ergebnisse zu dokumentieren. Beispiele für ergänzende Tests und Analysen sind das Einfügen von Fehlern zur Bestätigung der korrekten Arbeitsweise von Selbstüberwachungsfunktionen, spezifische Tests zur Bestätigung der Funktionsweise bestimmter Funktionen, spezifische Tests zur Bestätigung

des Verhaltens der Teile der Komponenten, die unvollständig oder nicht eindeutig dokumentiert sind oder spezifische Tests zur Bestimmung der Reaktion der Komponenten auf Eingangssignale, die außerhalb des zulässigen Bereiches liegen.

Bei der Qualifizierung der COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, ist sicherzustellen, dass die Komponenten keine unerwünschten Einflüsse und Auswirkungen auf die Systeme haben, in denen sie eingesetzt werden. Dazu ist durch eine Analyse sicherzustellen, dass keine unerwünschten Ereignisse, keine Gefahren, die Voraussetzungen für solche unerwünschten Ereignisse schaffen sowie keine ursächlichen Faktoren, die zu solchen Gefahren führen können, vorliegen.

Grundsätzlich sollte die Möglichkeit bestehen, bei der Qualifizierung von COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, mit anderen Betreibern zusammenzuarbeiten, um Überlappungen zu vermeiden. Dabei können beispielsweise einzelne Analysen oder Tests, die von mehreren Anlagen im Rahmen der Qualifizierung benötigt werden, nur einmalig durchgeführt und dann von den anderen Betreibern ebenfalls verwendet werden. Sobald bestimmte Analysen oder Tests für bestimmte COTS-Komponenten durchgeführt worden sind, ist es für andere Betreiber somit nicht mehr notwendig, diese nochmals durchführen zu lassen. Vorrausetzung hierfür ist, dass Anforderungen und Auslegungen, die als Grundlage für diese Analysen dienen, bei allen beteiligten Betreibern übereinstimmen.

Sind COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, einmal für den Einsatz in bestimmten Zielanwendungen qualifiziert, sollte die Möglichkeit bestehen, dass exakt die qualifizierte Version der Komponenten auf Grundlage der Qualifizierung auch in anderen kerntechnischen Anlagen eingesetzt werden kann. Dabei ist auf jeden Fall die standortspezifische Eignung separat zu analysieren.

Kategorie B

Hinsichtlich der Vorgehensweise bei der Qualifizierung von COTS-Komponenten ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

Kategorie C

Hinsichtlich der Vorgehensweise bei der Qualifizierung von COTS-Komponenten ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie C gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

**Einbeziehung der Betriebserfahrung bei der Qualifizierung**

Kategorie A

Bei der Qualifizierung von COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, besteht die Möglichkeit, die Betriebserfahrung der Komponenten mit einzubeziehen, um das Vertrauen in die Komponenten weiter zu erhöhen. Dabei muss die Betriebserfahrung der geplanten Version der zu qualifizierenden Komponenten entsprechen und die Komponenten müssen in vergleichbarer Weise unter vergleichbaren Umgebungsbedingungen eingesetzt werden wie in der geplanten Zielanwendung. Allein die Berücksichtigung der Betriebserfahrung kann nicht für eine erfolgreiche Qualifizierung der COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, ausreichen.

Kategorie B

Bei der Qualifizierung von COTS-Komponenten, die Funktionen der Kategorie B ausführen sollen, kann bereits vorhandene Betriebserfahrung der Komponenten berücksichtigt werden, wenn die Betriebsprofile und Betriebsumgebungen ähnlich und mindestens so anspruchsvoll wie in der geplanten Zielanwendung sind. Während der Qualifizierung verwendete Nachweise der Betriebserfahrung müssen überprüfbar sein und sich auf die zu qualifizierende Version der Komponente sowie sich auf bekannte Konfigurationseinstellungen der Hard- und Software beziehen. Der Umfang und das Zeitintervall der Betriebserfahrung muss ausreichen, um ein angemessenes Vertrauen in die Komponenten zu schaffen. Zudem sollte die Betriebserfahrung auf mehreren Anwendungen bei einer Reihe von Organisationen beruhen, wobei nachzuweisen ist, dass die Betriebserfahrung für die geplante Zielanwendung relevant ist.

Verwendete Informationen zur Betriebserfahrung sollten nachvollziehbar und unter Angabe der verwendeten Methode aufgezeichnet worden sein. Diese Aufzeichnungen sollten Anzahl und Historie der aufgetretenen Fehler beinhalten. Zudem sollten die Daten aus der Betriebserfahrung Aufschluss über das Potential für gemeinsam verursachte

Ausfälle geben sowie Maßnahmen zur Instandhaltung und Modifikationen an den Komponenten beinhalten.

Für COTS-Komponenten, die Funktionen der Kategorie B ausführen sollen, kann der Rückfluss der Betriebserfahrung in gerechtfertigten Fällen fehlende spezifische Nachweise ersetzen. Allein die Berücksichtigung der Betriebserfahrung kann nicht für eine erfolgreiche Qualifizierung der COTS-Komponenten, die Funktionen der Kategorie B ausführen sollen, ausreichen.

Kategorie C

Bei der Qualifizierung von COTS-Komponenten, die Funktionen der Kategorie C ausführen sollen, kann bereits vorhandene Betriebserfahrung der Komponenten berücksichtigt werden, wenn die Betriebsprofile und Betriebsumgebungen ähnlich wie in der geplanten Zielanwendung sind. Während der Qualifizierung verwendete Nachweise der Betriebserfahrung sollten sich auf die zu qualifizierende Version der Komponente sowie auf bekannte Konfigurationseinstellungen der Hard- und Software beziehen. Für den Fall, dass die Betriebserfahrung für Komponenten mit anderen Hard- und Softwareversionen in Betracht gezogen werden soll, ist eine Analyse der Unterschiede zwischen den Versionen und eine Begründung, inwieweit die Betriebserfahrung der einzelnen Versionen einbezogen werden kann, vorzulegen.

Für COTS-Komponenten, die Funktionen der Kategorie C ausführen sollen, kann der Rückfluss der Betriebserfahrung in gerechtfertigten Fällen fehlende spezifische Nachweise ersetzen. Allein die Berücksichtigung der Betriebserfahrung kann nicht für eine erfolgreiche Qualifizierung der COTS-Komponenten, die Funktionen der Kategorie C ausführen sollen, ausreichen.

**Analyse der Fehlermöglichkeiten von COTS-Komponenten**

Kategorie A

Für COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, ist eine Analyse durchzuführen, um die Fehlermöglichkeiten und Ausfallarten der COTS-Komponenten zu bestimmen. Dabei sind neben den Komponenten auch alle Schnittstellen einzubeziehen. Es kann beispielsweise eine Fehlermöglichkeits- und Einflussana-

lyse (FMEA, Failure Modes and Effects Analysis) durchgeführt werden, die sich in verschiedene Aspekte wie die Untersuchung des Ausfallverhaltens des Systems, die Untersuchung der Komponenten oder die Untersuchung der Arbeitsschritte im Rahmen des Herstellungsprozesses unterteilen kann. Weitere mögliche Analysen sind beispielsweise eine Fehlerbaumanalyse (FTA, Fault Tree Analysis) oder eine Gefährdungs- und Betriebsfähigkeitsanalyse (HAZOP, Hazards and Operability Analysis).

Für COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, ist das CCF-Potential (CCF, Common Cause Failure, Ausfälle aufgrund gemeinsamer Ursache) zu analysieren. Dazu sind geeignete Verfahren vorzusehen, um die Zuverlässigkeit der Komponenten nachzuweisen. Es müssen geeignete Maßnahmen getroffen werden, damit systematische Fehler beherrscht werden.

Für COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, ist der Nachweis zu erbringen, dass möglichst alle Fehlerarten rechtzeitig erkannt und gemeldet werden können. Der Anteil erkannter Fehlerarten sollte möglichst maximiert werden und muss alle gefährlichen Fehler umfassen.

Kategorie B

Für COTS-Komponenten, die Funktionen der Kategorie B ausführen sollen, ist eine Analyse durchzuführen, um die Fehlermöglichkeiten und Ausfallarten der COTS-Komponenten zu bestimmen. Dabei sind neben den Komponenten auch alle Schnittstellen einzubeziehen.

Für COTS-Komponenten, die Funktionen der Kategorie B ausführen sollen, sollte das CCF-Potential analysiert werden. Dazu sollten geeignete Verfahren vorgesehen werden, um die Zuverlässigkeit der Komponenten nachzuweisen.

Für COTS-Komponenten, die Funktionen der Kategorie B ausführen sollen, sollte der Nachweis erbracht werden, dass möglichst alle Fehlerarten rechtzeitig erkannt und gemeldet werden können.

Kategorie C

Für COTS-Komponenten, die Funktionen der Kategorie C ausführen sollen, sollte eine Analyse durchgeführt werden, um die Fehlermöglichkeiten und Ausfallarten der COTS-

Komponenten zu bestimmen, wobei neben den Komponenten auch alle Schnittstellen einbezogen werden sollten. Es sollte der Nachweis erbracht werden, dass möglichst alle Fehlerarten rechtzeitig erkannt und gemeldet werden können.

**Cybersicherheit von COTS-Komponenten**

Kategorie A

Durch eine Schwachstellenanalyse, bei der sowohl Täter von außen als auch Innentäter zu berücksichtigen sind, sind COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, auf mögliche Schwachstellen für Cyberangriffe zu untersuchen. Bei dieser Analyse sind beispielsweise eine Bewertung der Entwicklungs- und Betriebsumgebung des Herstellers, eine Bewertung der Komponenten hinsichtlich komplexen, unerwünschten, nicht verwendeten oder bösartigen Codes, eine Bewertung hinsichtlich Schwachstellen in den Kommunikationsfunktionen der Komponenten, eine Überprüfung hinsichtlich der Möglichkeit eines Fernzugriffs, eine Überprüfung der Materialhandhabungs- und Versandprozesse zum Schutz vor Änderungen während des Versands sowie eine Untersuchung der Robustheit integrierter Schutzfunktionen (z. B. Jumper zum Schreibschutz, änderbare Passwörter) zu berücksichtigen.

Für COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, sind Maßnahmen zu ergreifen, um diese vor Cyberangriffen zu schützen. Da entsprechende Angriffe zu verschiedenen Zeitpunkten erfolgen können (z. B. bei der Herstellung, während des Versands, bei der Inbetriebnahme, während des Betriebs) ist eine Überprüfung und Bewertung dieser Maßnahmen zu mehreren Zeitpunkten notwendig. Mögliche Maßnahmen zum Schutz gegen Cyberangriffe sind beispielsweise eine Verifizierung und Validierung der Software, Konfigurationskontrollen beim Hersteller, eine sichere Entwicklungs- und Betriebsumgebung, vertrauenswürdige Lieferanten in der Lieferkette des Herstellers, eine Härtung der Komponenten bezüglich Cybersicherheit (z. B. Passwortschutz, Protokollierung, Deaktivierung ungenutzter Schnittstellen, Verriegelung von Gehäusen), Anforderungen an Verpackung und Versand sowie Schutz- und Kontrollmaßnahmen während und nach der Installation.

Kategorie B

Hinsichtlich der Cybersicherheit von COTS-Komponenten ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

Kategorie C

Hinsichtlich der Cybersicherheit von COTS-Komponenten ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie C gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

### 3.2.7 Möglichkeiten zur Fehlererkennung und Fehlervermeidung

Hinsichtlich des Aspektes der Möglichkeiten zur Fehlererkennung und Fehlervermeidung wurden folgende Anforderungen entwickelt, die nachfolgend für die Kategorien A, B und C vorgestellt werden:

- Maßnahmen zur Fehlervermeidung und zur Fehlerbeherrschung
- Vermeidung des Auftretens systematischer Fehler
- Schutz gegen unerwünschte Funktionalitäten
- Maßnahmen zur Selbstüberwachung
- Kommunikation beim Auftreten von Fehlern oder Mängeln

**Maßnahmen zur Fehlervermeidung und zur Fehlerbeherrschung**

Kategorie A

Für COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, sind Maßnahmen zur Fehlervermeidung vorzusehen. Maßnahmen zur Fehlervermeidung dienen zur Minimierung der Häufigkeit des Auftretens von Fehlern und sind in der Regel bereits bei der Entwicklung der Komponenten zu berücksichtigen. Beispiele für Maßnahmen zur Fehlervermeidung sind konstruktive, analytische oder organisatorische Maßnahmen, Maßnahmen zur Qualitätssicherung, der Nachweis der Qualität durch Prüfungen (z. B. Beständigkeit gegen spezifizierte Umgebungsbedingungen) sowie die Durchführung zusätzlicher herstellerunabhängiger Prüfungen zur Erhöhung der Nachweistiefe.

Für COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, sind Maßnahmen zur Fehlerbeherrschung vorzusehen. Maßnahmen zur Fehlerbeherrschung dienen dazu, dass auftretende Fehler zu keinen oder nur zu sicherheitstechnisch tolerierbaren Auswirkungen führen und sind in der Regel bei der anwendungsspezifischen Auslegung zu berücksichtigen. Beispiele für Maßnahmen zur Fehlerbeherrschung sind das Defence-in-Depth-Prinzip, redundanter Aufbau von Systemen, Diversität, die Verteilung von Funktionen auf verschiedene Teilsystem zur Minimierung der Auswirkung von Einzelfehlern, die Verwendung von Komponenten mit sicherheitsgerichtetem Ausfallverhalten (Fail-Safe) sowie die Unabhängigkeit von Komponenten, um Auswirkungen eines Fehlers auf andere Komponenten zu vermeiden (z. B. räumliche Trennung, elektrische Entkopplung).

Kategorie B

Hinsichtlich der Maßnahmen zur Fehlervermeidung und zur Fehlerbeherrschung ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

Kategorie C

Hinsichtlich der Maßnahmen zur Fehlervermeidung und zur Fehlerbeherrschung ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie C gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

**Vermeidung des Auftretens systematischer Fehler**

Kategorie A

Für COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, müssen fehlervermeidende und fehlerbeherrschende Maßnahmen getroffen werden, damit redundanzübergreifende systematische Ausfälle verhindert werden. Ist dies nicht möglich, sind Maßnahmen zu treffen, die dafür sorgen, dass ein systematischer Ausfall der Komponenten beherrscht wird.

Um dem systematischen Versagen mehrerer COTS-Komponenten entgegenzuwirken, ist vom Hersteller darzulegen, dass keine unbeabsichtigten Änderungen der Anwendersoftware oder Parametrierung eingetragen werden können, dass bei der Kommunikation

zwischen redundanten Komponenten keine unzulässigen Rückwirkungen auf die redundanten Komponenten auftreten können, dass eine Beaufschlagung mit fehlerhaften Daten/Eingangssignalen zu einer definierten Reaktion der Komponenten führt, das eine Beaufschlagung mit erhöhten Datenmengen zu keiner fehlerhaften Reaktion der Komponenten führt, das zeitabhängige Störungen der Software (z. B. besondere Kalenderdaten) vermieden werden, sowie dass Maßnahmen zur Robustheit der Software angemessen implementiert sind.

Für COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen und die Software enthalten, ist der Nachweis zu erbringen, dass die Software frei von möglichen Ursachen für systematische Fehler ist. Dazu ist die Gesamtarchitektur der Komponenten zu bewerten, wozu diese inklusive aller Funktionen sowie der wichtigsten Hard- und Softwarekomponenten bekannt sein muss. Für eine entsprechende Bewertung sind zudem Informationen bezüglich des allgemeinen Entwurfs, der Ein- und Ausgänge, der Datenverarbeitung, der Faktoren, die das Verhalten während des Betriebs beeinflussen können, der Abfolge und Synchronisation der Aufgaben, der Trennung zwischen Aufgaben der Hauptfunktionen und weiteren Funktionen, der beeinflussenden Faktoren für die Reaktionszeit sowie bereitgestellte Online- und Offline-Tests und Diagnosefunktionen erforderlich.

Für COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen und die Software enthalten ist nachzuweisen, dass die Hauptfunktionen der Komponenten nicht durch Interrupts beeinträchtigt werden können. Zudem müssen die Komponenten über Selbstüberwachungsmaßnahmen verfügen, die bei Erkennen eines Fehlers einen Alarm auslösen oder das Gerät sicherheitsgerichtet ausfallen lassen.

Kategorie B

Hinsichtlich der Vermeidung des Auftretens systematischer Fehler ergeben sich keine Unterschiede zwischen den Sicherheitskategorien A und B. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

Kategorie C

Für COTS-Komponenten, die Funktionen der Kategorie C ausführen sollen, sollten fehlervermeidende und fehlerbeherrschende Maßnahmen getroffen werden, damit redundanzübergreifende systematische Ausfälle verhindert werden.

Für COTS-Komponenten, die Funktionen der Kategorie C ausführen sollen und die Software enthalten, sollte der Nachweis erbracht werden, dass die Software frei von möglichen Ursachen für systematische Fehler ist. Zur Erbringung dieses Nachweises kann die Gesamtarchitektur der Komponenten bewerten werden.

**Schutz gegen unerwünschte Funktionalitäten**

Kategorie A

COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, dürfen keine unerwünschten Funktionalitäten enthalten. Es sind geeignete Methoden anzuwenden, um sicherzustellen, dass COTS-Komponenten keine unerwünschten Funktionalitäten bieten. Techniken zur Gefahren- oder Sicherheitsanalyse können bei der Bestimmung zu vermeidender Funktionen, die zur Beeinträchtigung wesentlicher Daten oder zur Gefährdung der Funktionalität der Komponenten führen können, helfen. Merkmale der COTS-Komponenten, welche die Ausführung der Hauptfunktionen beeinträchtigen oder verhindern können, müssen identifiziert und deaktiviert werden.

COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, können beispielsweise durch den Einsatz von Wrappern vor unerwünschten Funktionalitäten geschützt werden. Durch den Einsatz von Wrappern wird verhindert, dass unerwünschte Ein- und Ausgänge die Funktionalität beeinträchtigen. Dabei können Wrapper sowohl an den Eingängen der Komponenten eingesetzt werden und so unerwünschte Eingaben blockieren als auch an den Ausgängen der Komponenten eingesetzt werden und so Ausgaben nur unter bestimmten Bedingungen passieren lassen.

Kategorie B

COTS-Komponenten, die Funktionen der Kategorie B ausführen sollen, sollten keine unerwünschten Funktionalitäten enthalten. Es sollten geeignete Methoden angewendet werden, um sicherzustellen, dass COTS-Komponenten keine unerwünschten Funktionalitäten bieten. Techniken zur Gefahren- oder Sicherheitsanalyse können bei der Bestimmung zu vermeidender Funktionen, die zur Beeinträchtigung wesentlicher Daten oder zur Gefährdung der Funktionalität der Komponenten führen können, helfen. Merkmale der COTS-Komponenten, welche die Ausführung der Hauptfunktionen beeinträchtigen oder verhindern können, sollten identifiziert und deaktiviert werden.

Kategorie C

Hinsichtlich des Schutzes gegen unerwünschte Funktionalitäten ergeben sich für COTS-Komponenten, die Funktionen der Kategorie C ausführen sollen, keine Anforderungen.

**Maßnahmen zur Selbstüberwachung**

Kategorie A

COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, sind selbstüberwachend auszulegen. Dabei ist sowohl die Hardware als auch das Verhalten der Software der Komponenten zu überwachen. Der Programmcode und unveränderliche Daten müssen im Hinblick auf unbeabsichtigte Änderungen überwacht werden. Durch die Selbstüberwachungsmechanismen müssen Zufallsausfälle der Hardware, fehlerhaftes Verhalten der Software sowie fehlerhafte Datenübertragung erfasst werden.

Wird durch die Selbstüberwachungsmechanismen eine fehlerhafte Funktion der COTS-Komponenten mit wesentlichen Auswirkungen erkannt, muss in geeigneter Weise und zeitgerecht reagiert werden und es müssen diagnostische Informationen gesammelt werden. Es ist sicherzustellen, dass die fehlerhafte Funktion keinen Einfluss mehr auf den Anlagenprozess hat.

Enthalten die COTS-Komponenten Funktionen, die nicht von der Selbstüberwachung erfasst werden können oder besteht die Möglichkeit des Auftretens passiver Hardwareausfälle, die von den Selbstüberwachungsmechanismen nicht erfasst werden können, sind regelmäßige und lückenlose wiederkehrende Prüfungen durchzuführen.

Durch die Selbstüberwachungsmechanismen und die gegebenenfalls durchzuführenden Prüfungen dürfen die Funktionen der COTS-Komponenten nicht beeinträchtigt werden.

Kategorie B

Hinsichtlich der Maßnahmen zur Selbstüberwachung ergeben sich keine Unterschiede zwischen den Sicherheitskategorien A und B. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

Kategorie C

COTS-Komponenten, die Funktionen der Kategorie C ausführen sollen, sollten über Selbstüberwachungsmechanismen verfügen, die sowohl die Hardware als auch das Verhalten der Software der Komponenten überwachen können. Die Selbstüberwachungsmechanismen sollten die Funktion der Komponenten nicht beeinflussen.

**Kommunikation beim Auftreten von Fehlern oder Mängeln**

Kategorie A

Werden an COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, Mängel oder Fehler festgestellt (alle aufgetretenen Mängel/Fehler bei allen Endkunden sind hier zu berücksichtigen, nicht nur an COTS-Komponenten, die in kerntechnischen Anlagen eingesetzt sind), müssen Informationen über diese Mängel oder Fehler vom Hersteller an die Betreiber kerntechnischer Anlagen, die diese Komponenten einsetzen, weitergegeben werden. Dabei sollte der Hersteller bereits eine Bewertung abgeben, ob die Mängel/Fehler zu einem erheblichen Sicherheitsrisiko führen können. Gemeldete Mängel/Fehler sind von den Betreibern hinsichtlich deren Auswirkungen zu bewerten. Falls notwendig, sind Maßnahmen wie beispielsweise eine vorbeugende Wartung oder ein Austausch der Komponenten zu veranlassen.

Auf Seiten der Betreiber sind außerdem Maßnahmen zu treffen, dass die Informationen über Mängel/Fehler von COTS-Komponenten an die richtigen Personen innerhalb der Organisation weitergegeben werden.

Es sind regelmäßige Befragungen der Hersteller durchzuführen, um aktuelle Informationen hinsichtlich aufgetretener Mängel oder Fehler der COTS-Komponenten zu erhalten.

Um weitere Informationen über Mängel oder Fehler an Komponenten zu erhalten, sind betriebsinterne Daten über die Zuverlässigkeit der Komponenten zu sammeln. Diese sind umso aussagekräftiger, je mehr Komponenten im Einsatz sind. Es sollte in Betracht gezogen werden, Praktiken zur Fehler- und Zuverlässigkeitsüberwachung zwischen kerntechnischen Anlagen und anderen Industriezweigen zu harmonisieren, um mehr detaillierte Daten über COTS-Komponenten zu erhalten.

Kategorie B

Hinsichtlich der Kommunikation beim Auftreten von Mängeln oder Fehlern ergeben sich keine Unterschiede zwischen den Sicherheitskategorien A und B. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

Kategorie C

Werden an COTS-Komponenten, die Funktionen der Kategorie C ausführen sollen, Mängel oder Fehler festgestellt (alle aufgetretenen Mängel/Fehler bei allen Endkunden sind hier zu berücksichtigen, nicht nur COTS-Komponenten, die in kerntechnischen Anlagen eingesetzt sind), sollten Informationen über diese Mängel oder Fehler vom Hersteller an die Betreiber kerntechnischer Anlagen, die diese Komponenten einsetzen, weitergegeben werden.

Gemeldete Mängel/Fehler sollten von den Betreibern hinsichtlich deren Auswirkungen bewertet werden. Falls notwendig, sind Maßnahmen wie beispielsweise eine vorbeugende Wartung oder ein Austausch der Komponenten zu veranlassen. Auf Seiten der Betreiber sollten außerdem Maßnahmen getroffen werden, dass die Informationen über Mängel/Fehler von COTS-Komponenten an die richtigen Personen innerhalb der Organisation weitergegeben werden.

Hersteller sollten im Rahmen regelmäßiger Befragungen aktuelle Informationen hinsichtlich aufgetretener Mängel oder Fehler an den COTS-Komponenten weitergeben.

Um weitere Informationen über Mängel oder Fehler an Komponenten zu erhalten, können betriebsinterne Daten über die Zuverlässigkeit der Komponenten gesammelt werden. Diese sind umso aussagekräftiger, je mehr Komponenten im Einsatz sind. Es sollte in Betracht gezogen werden, Praktiken zur Fehler- und Zuverlässigkeitsüberwachung zwischen kerntechnischen Anlagen und anderen Industriezweigen zu harmonisieren, um mehr detaillierte Daten über COTS-Komponenten zu erhalten.

### 3.2.8 Änderungsmanagement

Hinsichtlich des Aspektes des Änderungsmanagements wurden folgende Anforderungen entwickelt, die nachfolgend für die Kategorien A, B und C vorgestellt werden:

- Erfassung von Änderungen
- Umfang von Änderungen
- Durchführung von Änderungen in mehreren Redundanten
- Hardwareänderungen
- Softwareänderungen

**Erfassung von Änderungen**

Kategorie A

COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, sind während des gesamten Lebenszyklus hinsichtlich ihres aktuellen Zustands und durchgeführter Änderungen zu überwachen. Mit dem Hersteller der Komponenten sind verbindliche Vorgaben für die Durchführung von Änderungen an Hard- und Software zu treffen. Es ist sicherzustellen, dass die Endnutzer über alle Änderungen an den COTS-Komponenten vom Hersteller informiert werden. Hierzu sind entsprechende Vereinbarungen zu treffen.

Änderungen an Hard- und Software oder dem Herstellungsprozess der COTS-Komponenten können eine vorherige Qualifizierung ungültig machen und möglicherweise zusätzliche Maßnahmen zur Aufrechterhaltung der Qualifizierung oder eine neue Qualifizierung erforderlich machen. Für den Fall, dass Änderungen an COTS-Komponenten vorgenommen werden müssen, sind die Gründe für die Änderungen darzulegen, die Änderungen selbst zu beschreiben sowie eine Analyse der Auswirkungen der Änderungen durchzuführen. Liegen diese Informationen nicht vor, sind geänderte Komponenten wie neue Komponenten zu behandeln.

Beabsichtigte Änderungen wie Kalibrierung oder Neukonfiguration sind in der Regel unbedenklich, solange das Verhalten der Komponente gleichbleibt und die Anforderungsspezifikationen erfüllt werden.

Kategorie B

Hinsichtlich der Erfassung von Änderungen ergeben sich keine Unterschiede zwischen den Sicherheitskategorien A und B. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

Kategorie C

COTS-Komponenten, die Funktionen der Kategorie C ausführen sollen, sollten während des gesamten Lebenszyklus hinsichtlich ihres aktuellen Zustands und durchgeführter Änderungen überwacht werden. Es sollte sichergestellt werden, dass die Endnutzer über alle Änderungen an den COTS-Komponenten vom Hersteller informiert werden.

**Umfang von Änderungen**

Kategorie A

Es ist sicherzustellen, dass durch vorgenommene Änderungen nicht die Betriebserfahrungen, die bei der Qualifizierung der Komponenten berücksichtigt wurden, beeinträchtigt werden. Zudem ist sicherzustellen, dass Änderungen die Hauptfunktionen der Komponenten nicht konzeptionell ändern. Außerdem muss sichergestellt werden, dass jede Änderung den Sicherheitsanforderungen und Grundlagen des Designs entspricht. Die Kompatibilität neuer Komponenten ist vor deren Einsatz zu prüfen.

Änderungen müssen von geringem Umfang und einfach zu überprüfen sein, damit keine neue Qualifizierung der COTS-Komponenten erforderlich wird. Sind Änderungen an COTS-Komponenten erforderlich, ist zu analysieren, ob aufgrund dieser Änderungen auch Änderungen an den Wartungs- und Betriebspraktiken oder erweiterter Schulungsbedarf des Personals erforderlich werden.

Kategorie B

Hinsichtlich des Umfangs von Änderungen ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

Kategorie C

Hinsichtlich des Umfangs von Änderungen ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie C gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

**Durchführung von Änderungen in mehreren Redundanten**

Kategorie A

Für den Fall, dass Änderungen an COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, vorgesehen sind und diese Komponenten in mehreren Redundanten eingesetzt werden, muss der Einsatz der geänderten COTS-Komponenten in den unterschiedlichen Redundanten mit einer hinreichenden zeitlichen Staffelung erfolgen, damit das Potential für gemeinsam verursachte Ausfälle begrenzt wird.

Kommen Komponenten in unterschiedlichen Systemen mit unterschiedlicher Sicherheitskategorie zum Einsatz und sind Änderungen an diesen Komponenten geplant, sollten die geänderten Komponenten zuerst in den Systemen mit der geringeren sicherheitstechnischen Bedeutung zum Einsatz kommen.

Kategorie B

Hinsichtlich der Durchführung von Änderungen in mehreren Redundanten ergeben sich keine Unterschiede zwischen den Sicherheitskategorien A und B. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

Kategorie C

Für den Fall, dass Änderungen an COTS-Komponenten, die Funktionen der Kategorie C ausführen sollen, vorgesehen sind und diese Komponenten in mehreren Redundanten eingesetzt werden, sollte der Einsatz der geänderten COTS-Komponenten in den unterschiedlichen Redundanten mit einer hinreichenden zeitlichen Staffelung erfolgen, damit das Potential für gemeinsam verursachte Ausfälle begrenzt wird.

**Hardwareänderungen**

Kategorie A

Um sicherzustellen, dass Hardwareänderungen erfasst werden, ist die Hardware neuer, aber bereits qualifizierter COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, mit der Hardware der ursprünglichen COTS-Komponenten zu vergleichen. Dies ist nicht erforderlich, wenn sichergestellt ist, dass der Hersteller transparent arbeitet und ein diszipliniertes Änderungsmanagement betreibt, wodurch alle Änderungen kommuniziert werden.

Für den Fall, dass Hardwareänderungen durchgeführt worden sind, sind die Auswirkungen dieser Änderungen zu untersuchen. Dabei ist beispielsweise zu untersuchen, ob die technischen Daten zwischen den beiden Komponenten (original und geändert) gleichwertig sind, insbesondere hinsichtlich der elektrischen Daten, der Geometrie, des Funktionsprinzips, der Struktur und Technik, des Materials sowie des Antwortverhaltens. Des Weiteren ist zu untersuchen, ob neue Funktionen hinzugefügt worden sind.

Kategorie B

Hinsichtlich der Hardwareänderungen ergeben sich keine Unterschiede zwischen den Sicherheitskategorien A und B. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

Kategorie C

Um sicherzustellen, dass Hardwareänderungen erfasst werden, sollte die Hardware neuer, aber bereits qualifizierter COTS-Komponenten, die Funktionen der Kategorie C ausführen sollen, mit der Hardware der ursprünglichen COTS-Komponenten verglichen werden.

**Softwareänderungen**

Kategorie A

Grundsätzlich sind Änderungen der Software auszuschließen oder nur in sehr geringem Umfang durchzuführen. Sind Änderungen der Software unumgänglich, ist sicherzustellen, dass Softwareänderungen an Komponenten, die Funktionen der Kategorie A ausführen sollen, erfasst werden. Dazu muss vom Hersteller ein Software-Versionsmanagement umgesetzt werden, damit alle Versionen einer Software eindeutig identifizierbar sind. Ist sichergestellt, dass der Hersteller transparent arbeitet und ein diszipliniertes Software-Versionsmanagement betreibt, kann davon ausgegangen werden, dass Softwareänderungen erfasst werden. Ist dies nicht der Fall, muss die Software neuer, aber bereits qualifizierter COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, mit der Software der ursprünglichen COTS-Komponenten verglichen werden, beispielsweise durch eine Prüfsumme oder eine Überprüfung der Hashwerte.

Für den Fall, dass Softwareänderungen durchgeführt worden sind, ist eine Folgenabschätzung dieser Änderungen durchzuführen. Kommt diese zu dem Ergebnis, dass die Softwareänderungen Auswirkungen auf die Funktion der Komponenten haben, ist eine Nachqualifizierung oder eine neue Qualifizierung der Komponente erforderlich.

Kategorie B

Hinsichtlich der Softwareänderungen ergeben sich keine Unterschiede zwischen den Sicherheitskategorien A und B. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

Kategorie C

Um sicherzustellen, dass Softwareänderungen erfasst werden, sollte die Software neuer, aber bereits qualifizierter COTS-Komponenten, die Funktionen der Kategorie C ausführen sollen, mit der Software der ursprünglichen COTS-Komponenten verglichen werden.

### 3.2.9 Wartung und Instandhaltung

Hinsichtlich des Aspektes der Wartung und Instandhaltung wurden folgende Anforderungen entwickelt, die nachfolgend für die Kategorien A, B und C vorgestellt werden:

- Durchführung von Wartungs- und Instandhaltungstätigkeiten
- Wartung und Instandhaltung in mehreren Redundanten
- Verwendete Werkzeuge zur Wartung und Instandhaltung
- Lebensdauer der COTS-Komponenten
- Sicherstellung der Ersatzteilversorgung/Ersatzteilhaltung

**Durchführung von Wartungs- und Instandhaltungstätigkeiten**

Kategorie A

Für Wartungs- und Instandhaltungstätigkeiten an COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, müssen geeignete Voraussetzungen geschaffen werden, um die Wartungs- und Instandhaltungstätigkeiten rasch und rückwirkungsfrei durchführen zu können. Die Möglichkeit des Austausches von Einzelkomponenten bei laufendem Betrieb sollte geprüft werden.

Es ist festzuhalten, welche COTS-Komponenten bei den Wartungs- und Instandhaltungstätigkeiten ausgewechselt wurden. Zudem sind der Grund für die Auswechslung, festgestellte Ausfälle und ihre Ursachen sowie die daraus abgeleiteten Reparaturmaßnahmen festzuhalten.

Kategorie B

Hinsichtlich der Durchführung von Wartungs- und Instandhaltungstätigkeiten ergeben sich keine Unterschiede zwischen den Sicherheitskategorien A und B. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

Kategorie C

Für Wartungs- und Instandhaltungstätigkeiten an COTS-Komponenten, die Funktionen der Kategorie C ausführen sollen, sollte ein Austausch von Komponenten rasch möglich sein. Zudem muss der Austausch rückwirkungsfrei durchführbar sein.

Es sollte festgehalten werden, welche COTS-Komponenten bei den Wartungs- und Instandhaltungstätigkeiten ausgewechselt wurden. Zudem sollten der Grund für die Auswechslung, festgestellte Ausfälle und ihre Ursachen sowie die daraus abgeleiteten Reparaturmaßnahmen festgehalten werden.

**Wartung und Instandhaltung in mehreren Redundanten**

Kategorie A

Um die Wartung und Instandhaltung von COTS-Komponenten zur Ausführung von Funktionen der Kategorie A in mehreren Redundanten zu ermöglichen, muss sowohl in der Systemauslegung als auch im Aufbau des Systems die Separation, Entkopplung und räumliche Trennung redundanter Systemstrukturen implementiert werden.

Wartungs- und Instandhaltungsmaßnahmen von COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, müssen in einer Redundante, ohne Rückwirkungen auf die anderen Redundanten, möglich sein.

Kategorie B

Hinsichtlich der Wartung und Instandhaltung in mehreren Redundanten ergeben sich keine Unterschiede zwischen den Sicherheitskategorien A und B. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

Kategorie C

Um die Wartung und Instandhaltung von COTS-Komponenten zur Ausführung von Funktionen der Kategorie C in mehreren Redundanten zu ermöglichen, muss sowohl in der Systemauslegung als auch im Aufbau des Systems die Separation, Entkopplung und räumliche Trennung redundanter Systemstrukturen implementiert werden.

**Verwendete Werkzeuge zur Wartung und Instandhaltung**

Kategorie A

Wird die Wartung und Instandhaltung von COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, vom Anlagenbetreiber selbst durchgeführt, müssen die dazu erforderlichen Werkzeuge und weitere benötigte Informationen beim Anlagenbetreiber vorliegen.

Wird die Wartung und Instandhaltung von COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, vom Hersteller durchgeführt, ist ein Wartungsvertrag abzuschließen, in dem festgehalten wird, welche Mittel zur Wartung der Hersteller aufzubewahren hat. Zudem sind Vereinbarungen für den Fall zu treffen, dass der Hersteller den Support einer Komponente einstellt (z. B. alle notwendigen Mittel zur Wartung der Komponente gehen in diesem Fall an den Anlagenbetreiber über).

Kategorie B

Hinsichtlich der verwendeten Werkzeuge zur Wartung und Instandhaltung von COTS-Komponenten ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

Kategorie C

Hinsichtlich der verwendeten Werkzeuge zur Wartung und Instandhaltung von COTS-Komponenten ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie C gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

**Lebensdauer der COTS-Komponenten**

Kategorie A

COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, sind hinsichtlich ihrer zu erwartenden Lebensdauer zu bewerten, damit ein Austausch der Komponenten vor dem Ende ihrer Lebensdauer geplant werden kann.

Neben der zu erwartenden Lebensdauer der COTS-Komponenten ist auch die zu erwartende Dauer der Unterstützung durch den Hersteller zu berücksichtigen. Dabei sind möglichst lange Zeiträume der Unterstützung durch den Hersteller wünschenswert.

Kategorie B

Hinsichtlich der Lebensdauer der COTS-Komponenten ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

Kategorie C

Hinsichtlich der Lebensdauer der COTS-Komponenten ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie C gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

**Sicherstellung der Ersatzteilversorgung/Ersatzteilhaltung**

Kategorie A

Es ist eine geeignete Strategie zur Sicherstellung der Ersatzteilversorgung/Ersatzteilhaltung für COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, anzuwenden. Diese Strategie muss auf der Produktstrategie des Herstellers der COTS-Komponenten basieren. Für den Fall, dass der Hersteller sich zum Einsatz eines Erfahrungsrückfluss-, Konfigurations- und Änderungsmanagements für die COTS-Komponenten verpflichtet, ist es ausreichend, genügend Ersatzteile zur Aufrechterhaltung des Betriebs vorzuhalten. Wendet der Hersteller kein Erfahrungsrückfluss-, Konfigurations- und Änderungsmanagement für die COTS-Komponenten an, ist für einen ausreichenden Ersatzteilvorrat für die angedachte Betriebsdauer der COTS-Komponenten zu sorgen. Die Strategie zur Sicherstellung der Ersatzteilversorgung/Ersatzteilhaltung muss bei Änderungen an den COTS-Komponenten und damit verbundenen möglichen Änderungen der Produktstrategie des Herstellers angepasst werden.

Bei der Lagerung von Ersatzteilen für COTS-Komponenten, die Funktionen der Kategorie A ausführen, ist das Alterungsverhalten zu beachten.

Kategorie B

Hinsichtlich der Sicherstellung der Ersatzteilversorgung/Ersatzteilhaltung ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

Kategorie C

Hinsichtlich der Sicherstellung der Ersatzteilversorgung/Ersatzteilhaltung ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie C gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

### 3.2.10 Dokumentation

Hinsichtlich des Aspektes der Dokumentation wurden folgende Anforderungen entwickelt, die nachfolgend für die Kategorien A, B und C vorgestellt werden:

- Dokumentation der Eigenschaften der COTS-Komponenten
- Dokumentation des Design- und Herstellungsprozesses der COTS-Komponenten
- Dokumentation der Ergebnisse der Qualifizierung der COTS-Komponenten
- Benutzerdokumentation zum sicheren Betrieb von COTS-Komponenten
- Benötigte Informationen nach Einstellung des Supports durch den Hersteller

**Dokumentation der Eigenschaften der COTS-Komponenten**

Kategorie A

Für COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, sind die für die Zielfunktion geforderten Eigenschaften der COTS-Komponenten zu dokumentieren. Zu dieser Dokumentation zählen beispielsweise eine Systembeschreibung, der Komponentenaufbau, Kenndaten, eine Beschreibung aller Funktionen der Komponenten, eine Beschreibung der Schnittstellen, Einschränkungen für die Verwendung der Komponenten, eine Beschreibung der Hard- und Software, vorhandene Überwachungsmechanismen, vorhandene Maßnahmen zur Fehlererkennung, eine Beschreibung des Ausfallverhaltens, die spezifizierten Umgebungsbedingungen sowie Dokumentationen zu bereits durchgeführten Prüfungen.

Änderungen an COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, sind zu dokumentieren. Dies betrifft sowohl Änderungen an der Hardware als auch Änderungen an der Software. Zudem ist die Änderungshistorie der COTS-Komponenten festzuhalten. Die Dokumentation der Änderung muss eine Beschreibung der Änderung, eine Begründung für die Änderung sowie eine Bewertung der sicherheitstechnischen Auswirkungen der Änderung beinhalten.

Kategorie B

Hinsichtlich der Dokumentation der Eigenschaften der COTS-Komponenten ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

Kategorie C

Hinsichtlich der Dokumentation der Eigenschaften der COTS-Komponenten ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie C gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

**Dokumentation des Design- und Herstellungsprozesses der COTS-Komponenten**

Kategorie A

Für COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, muss vom Hersteller eine Dokumentation des Designprozesses der Komponenten vorgelegt werden. Diese muss gegebenenfalls durch spezifische, die Zielfunktion betreffende Dokumente ergänzt werden, wie beispielsweise Vorgaben zum spezifischen Designprozess.

Zudem ist vom Hersteller für COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, eine Dokumentation des Herstellungsprozesses zu erstellen. Dazu zählen beispielsweise eine Beschreibung der Verifizierungs- und Testprotokolle für jede Entwicklungsphase oder Informationen zur Identifikation der Version der Komponenten.

Kategorie B

Hinsichtlich der Dokumentation des Design- und Herstellungsprozesses der COTS-Komponenten ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

Kategorie C

Hinsichtlich der Dokumentation des Design- und Herstellungsprozesses der COTS-Komponenten ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie C gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

**Dokumentation der Ergebnisse der Qualifizierung der COTS-Komponenten**

Kategorie A

Die Ergebnisse der Qualifizierung von COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, sind zu dokumentieren. Diese Dokumentation muss beispielsweise eine Identifikation der zu prüfenden Komponenten einschließlich Versionsnummer und Konfiguration, die wichtigsten Funktions- und Leistungsanforderungen (z. B. Klassifizierung, Anforderungsspezifikation, Umgebungsbedingungen), die Bewertung aller Anforderungen für die Qualifizierung, die Angabe der höchsten Sicherheitsklasse, für die die Komponenten qualifiziert sind, die Angabe möglicher spezifischer Anwendungen, für die die Komponenten geeignet sind, Angaben aller Beschränkungen für den Einsatz sowie möglicherweise erforderliche Änderungen an den Komponenten oder der geplanten Zielanwendung für eine Integration der Komponenten enthalten.

Zudem muss die Dokumentation der Qualifizierung von COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, die erforderliche Redundanz, für die die Komponente qualifiziert ist, den erforderlichen Einsatz diversitärer Komponenten, spezifische Optionen bezüglich einer erforderlichen Aktivierung oder Deaktivierung nicht benötigter Funktionen der Komponenten, Grenzen der Betriebsumgebung sowie gegebenenfalls besondere Maßnahmen, die während des Betriebs der Komponenten zu beachten sind, enthalten.

Kategorie B

Hinsichtlich der Dokumentation der Ergebnisse der Qualifizierung der COTS-Komponenten ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

Kategorie C

Hinsichtlich der Dokumentation der Ergebnisse der Qualifizierung der COTS-Komponenten ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie C gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

**Benutzerdokumentation zum sicheren Betrieb von COTS-Komponenten**

Kategorie A

Für COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, ist vom Hersteller eine Benutzerdokumentation zu erstellen, damit der Betrieb der COTS-Komponenten sicher durchgeführt werden kann. Zu dieser Benutzerdokumentation kann beispielsweise ein Sicherheitshandbuch mit allen Anforderungen für den sicheren Betrieb, ein Installationshandbuch mit Festlegungen bezüglich der Installation der COTS-Komponenten und der Verbindung zu anderen Komponenten, ein Betriebshandbuch mit Festlegungen zur Interaktion zwischen Benutzer und COTS-Komponenten sowie ein Wartungshandbuch mit allen Aspekten der Wartung der COTS-Komponenten gehören.

Zudem müssen für den sicheren Betrieb von COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, Dokumente mit Informationen bezüglich z. B. der Funktionen der COTS-Komponenten, deren Fehlermöglichkeiten, Konfigurationsmöglichkeiten der Funktionen, Anforderungen an die Selbstüberwachung, Einschränkungen zum Betrieb sowie Anforderungen und Verfahren für wiederkehrende Prüfungen vom Hersteller bereitgestellt werden.

Kategorie B

Hinsichtlich der Benutzerdokumentation zum sicheren Betrieb von COTS-Komponenten ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie B gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

Kategorie C

Hinsichtlich der Benutzerdokumentation zum sicheren Betrieb von COTS-Komponenten ergeben sich keine Unterschiede für die verschiedenen Sicherheitskategorien. Für Kategorie C gelten somit die Anforderungen, die für Kategorie A aufgestellt wurden.

**Benötigte Informationen nach Einstellung des Supports durch den Hersteller**

Kategorie A

Für COTS-Komponenten, die Funktionen der Kategorie A ausführen sollen, ist zu berücksichtigen, welche Informationen zu den Komponenten vorhanden sein müssen, um den Betrieb sowie die Wartung und Instandhaltung der Komponenten weiter zu ermöglichen. Dazu muss der Hersteller bereit sein, diverse Informationen und Dokumente zur Verfügung zu stellen oder er muss zusichern, dass diese bei ihm verfügbar bleiben. Zu diesen Informationen und Dokumenten gehören beispielsweise Installationskopien von Konfigurationswerkzeugen wie Editoren und Compilern, eine Kopie der Betriebsumgebung dieser Werkzeuge, Kopien der Quelldateien und Bibliotheken, spezielle Hardware-Tools, Aufzeichnungen zur Fertigung sowie Kopien der gesamten Dokumentation (Spezifikation, Prüfberichte, usw.).

Kategorie B

Für COTS-Komponenten, die Funktionen der Kategorie B ausführen sollen, sollte berücksichtigt werden, welche Informationen zu den Komponenten vorhanden sein müssen, um den Betrieb sowie die Wartung und Instandhaltung der Komponenten weiter zu ermöglichen. Dazu sollte der Hersteller bereit sein, diverse Informationen und Dokumente zur Verfügung zu stellen oder er sollte zusichern, dass diese bei ihm verfügbar bleiben. Zu diesen Informationen und Dokumenten gehören beispielsweise Installationskopien von Konfigurationswerkzeugen wie Editoren und Compilern, eine Kopie der Betriebsumgebung dieser Werkzeuge, Kopien der Quelldateien und Bibliotheken, spezielle

Hardware-Tools, Aufzeichnungen zur Fertigung sowie Kopien der gesamten Dokumentation (Spezifikation, Prüfberichte, usw.).

Kategorie C

Für COTS-Komponenten, die Funktionen der Kategorie C ausführen sollen, sollte berücksichtigt werden, welche Informationen zu den Komponenten vorhanden sein müssen, um den Betrieb sowie die Wartung und Instandhaltung der Komponenten weiter zu ermöglichen. Dazu wäre es hilfreich, wenn der Hersteller bereit ist, diverse Informationen und Dokumente zur Verfügung zu stellen.

# 4 Zusammenfassung

Dieser Bericht fasst die Ergebnisse der Arbeiten zum Vorhaben 4721R01550 „Entwicklung eines Bewertungsansatzes für den Einsatz von kommerziellen (COTS) Komponenten in Kernkraftwerken“ zusammen. In Kapitel 2 dieses Berichtes sind die Ergebnisse der Arbeiten zu Arbeitspaket 1 hinsichtlich der Ermittlung und Auswertung nationaler und internationaler Vorgehensweisen hinsichtlich des Umgangs mit COTS-Komponenten dargestellt. Kapitel 3 dieses Berichtes stellt die Ergebnisse der Arbeiten zu Arbeitspaket 2 bezüglich der Entwicklung eines Ansatzes zur Bewertung des Einsatzes von COTS-Komponenten dar.

Im Rahmen von Arbeitspaket 1 wurden anhand einer Literaturrecherche diverse Dokumente ermittelt, die sich mit der Thematik des Einsatzes von COTS-Komponenten in sicherheitstechnisch wichtigen elektro- und leittechnischen Einrichtungen befassen. Dabei wurden neben der Kerntechnik auch Dokumente aus den Bereichen Luft- und Raumfahrttechnik, Bahn oder Militär berücksichtigt, sofern diese öffentlich verfügbar waren. Die im Erstscreening als relevant betrachteten Dokumente wurden detailliert hinsichtlich Anforderungen an den Einsatz von COTS-Komponenten ausgewertet, wobei folgende 14 Dokumente betrachtet wurden, deren Inhalte in Abschnitt 2.1 zusammengefasst sind:

- VDI/VDE-Richtlinie 3528 „Anforderungen an Serienprodukte und Kriterien für deren Einsatz in der Sicherheitsleittechnik in Kernkraftwerken“ /VDI 11/
- IAEA NR-T-3.31 „Challenges and Approaches for Selecting, Assessing and Qualifying Commercial Industrial Digital Instrumentation and Control Equipment for Use in Nuclear Power Plant Applications” /IAE 20/
- BS IEC 62671 „Nuclear Power Plants – Instrumentation and control important to safety – Selection and use of industrial digital devices of limited functionality” /BSI 13/
- “Guidance for Commercial Grade Dedication” /DOE 11/
- DIN EN 61513 „Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen“ /DIN 13/
- DIN EN 60880 „Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie A“ /DIN 10b/

- IEC 62138 „Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category B or C functions” /IEC 18/
- DIN EN 60987 „Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen an die Hardware-Auslegung rechnerbasierter Systeme“ /DIN 10c/
- “Commercial-Off-The-Shelf (COTS) Hardware and Software for Train Control Applications: System Safety Considerations” /DOT 03/
- “Simple and Complex Electronic Hardware Approval Guidance” /DOT 17/
- AMC 20-152A „Development Assurance for Airborne Electronic Hardware” /EAS 21/
- “Commercial off the Shelf (COTS) security issues and approaches” /DOA 06/
- “Joint Software Systems Safety Engineering Handbook” /DOD 10/
- “Space product assurance – Commercial electrical, electronic and electromechanical (EEE) components” /ESA 13/

Ebenfalls im Rahmen von Arbeitspaket 1 wurde nach Vorgehensweisen hinsichtlich des Einsatzes von COTS-Komponenten in elektro- und leittechnischen Einrichtungen in kerntechnischen Anlagen im Ausland recherchiert. Bei dieser Recherche wurden Informationen aus 23 Ländern ermittelt, wobei sich Detaillierungsgrad und Menge der verfügbaren Informationen zwischen den einzelnen Ländern stark unterscheiden. Es wurden fünf Länder ausgewählt, deren Vorgehensweise hinsichtlich des Einsatzes von COTS-Komponenten detailliert ausgewertet wurde. Folgende fünf Länder wurden betrachtet, deren Vorgehensweise in Abschnitt 2.2 zusammengefasst ist:

- Belgien
- Finnland
- Kanada
- Vereinigtes Königreich
- USA

Im Rahmen von Arbeitspaket 2 wurden die ermittelten Erkenntnisse und Anforderungen hinsichtlich des Einsatzes von COTS-Komponenten bezüglich verschiedener Aspekte

zusammengefasst und mit den Anforderungen aus dem nationalen kerntechnischen Regelwerk hinsichtlich dieser Aspekte verglichen. Dabei wurden die folgenden Aspekte betrachtet:

- Auswahl und Beschaffung von COTS-Komponenten
- Qualitätsmanagement des Herstellers und dessen Zulieferer
- Design- und Entwicklungsprozess der COTS-Komponenten
- Komplexität der COTS-Komponenten
- Technische Eigenschaften und Einsatzort bzw. -art der COTS-Komponenten
- Qualifizierung von COTS-Komponenten
- Möglichkeiten zur Fehlererkennung und Fehlervermeidung
- Änderungsmanagement
- Wartung und Instandhaltung
- Dokumentation

Zur Sammlung der Anforderungen an elektro- und leittechnische Komponenten aus dem nationalen kerntechnischen Regelwerk wurden folgende Regelwerke betrachtet, deren Inhalte in Abschnitt 3.1 zusammengefasst sind:

- „Sicherheitsanforderungen an Kernkraftwerke“ /BMU 22/
- „Interpretationen zu den Sicherheitsanforderungen an Kernkraftwerke“ /BMU 15/
- KTA 3501 „Reaktorschutzsystem und Überwachungseinrichtungen des Sicherheitssystems“ /KTA 15a/
- KTA 3503 „Typprüfung von elektrischen Baugruppen der Sicherheitsleittechnik“ /KTA 15b/
- KTA 3507 „Werksprüfungen, Prüfungen nach Instandsetzung und Nachweis der Betriebsbewährung der Baugruppen und Geräte der Sicherheitsleittechnik“ /KTA 14a/
- KTA 3701 „Übergeordnete Anforderungen an die elektrische Energieversorgung in Kernkraftwerken“ /KTA 14b/
- KTA 3901 „Kommunikationseinrichtungen für Kernkraftwerke“ /KTA 17/

- KTA 3903 „Prüfung und Betrieb von Hebezeugen in Kernkraftwerken“ /KTA 20/
- DIN EN 60880 „Kernkraftwerke, Leittechnik für Systeme mit sicherheitstechnischer Bedeutung, Softwarefunktionen für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie A“ /DIN 10b/
- DIN EN 61513 „Kernkraftwerke, Leittechnik für Systeme mit sicherheitstechnischer Bedeutung, Allgemeine Systemanforderungen“ /DIN 13/

Aufbauend auf den Anforderungen an COTS-Komponenten aus Arbeitspaket 1 (Abschnitte 2.1 und 2.2) und den Anforderungen aus dem kerntechnischen Regelwerk (Abschnitt 3.1) wurde ein Ansatz zur Bewertung des Einsatzes von COTS-Komponenten entwickelt. Bei der Entwicklung des Bewertungsansatzes wurden ebenfalls die zehn genannten Aspekte betrachtet, wobei für jeden Aspekt fünf Anforderungen, jeweils für die Kategorien A, B und C nach DIN EN 61226 entwickelt wurden. Folgende Anforderungen für die jeweiligen Aspekte wurden entwickelt, deren Inhalte in Abschnitt 3.2 dargestellt sind:

- Auswahl und Beschaffung von COTS-Komponenten
    - Anforderungsspezifikation an COTS-Komponenten
    - Eignung der COTS-Komponenten für die Zielanwendung
    - Auswahl des Herstellers der COTS-Komponenten
    - Dokumentation im Rahmen der Auswahl von COTS-Komponenten
    - Vorhandensein einer bereits durchgeführten Qualifizierung/Zertifizierung
- Qualitätsmanagement des Herstellers und dessen Zulieferer
    - Qualitätsmanagementsystem des Herstellers
    - Qualitätssicherung während des Design- und Entwicklungsprozesses
    - Qualitätssicherung bei Verwendung von Werkzeugen
    - Umgang mit Problemen oder Mängeln
    - Qualitätsmanagement und Qualitätssicherung der Zulieferer
- Design- und Entwicklungsprozess der COTS-Komponenten
    - Designprozess der COTS-Komponenten

    - Lebenszyklus des Design- und Entwicklungsprozesses
    - Konfigurationsmanagement für die Entwicklung von COTS-Komponenten
    - Entwicklungssicherheitskonzept für COTS-Komponenten
    - Softwareentwicklungsprozess für COTS-Komponenten
- Komplexität der COTS-Komponenten
    - Beitragende Attribute zur Komplexität von COTS-Komponenten
    - Bewertung der Komplexität der COTS-Komponenten
    - Möglichkeiten zur Konfiguration der COTS-Komponenten
    - Vorhandensein nicht genutzter/nicht benötigter Funktionen
    - Einfachheit der Software von COTS-Komponenten
- Technische Eigenschaften und Einsatzort bzw. -art der COTS-Komponenten
    - Funktionale Eignung der COTS-Komponenten für die Zielanwendung
    - Qualitätssicherung der COTS-Komponenten für die Zielanwendung
    - Integration der COTS-Komponenten in die Zielanwendung
    - Einsatz der COTS-Komponenten in der Zielanwendung
    - Umgebungsbedingungen am Einsatzort der COTS-Komponenten
- Qualifizierung von COTS-Komponenten
    - Umfang der Qualifizierung von COTS-Komponenten
    - Vorgehensweise bei der Qualifizierung von COTS-Komponenten
    - Einbeziehung der Betriebserfahrung bei der Qualifizierung
    - Analyse der Fehlermöglichkeiten von COTS-Komponenten
    - Cybersicherheit von COTS-Komponenten
- Möglichkeiten zur Fehlererkennung und Fehlervermeidung
    - Maßnahmen zur Fehlervermeidung und zur Fehlerbeherrschung
    - Vermeidung des Auftretens systematischer Fehler

    - Schutz gegen unerwünschte Funktionalitäten
    - Maßnahmen zur Selbstüberwachung
    - Kommunikation beim Auftreten von Fehlern oder Mängeln
- Änderungsmanagement
    - Erfassung von Änderungen
    - Umfang von Änderungen
    - Durchführung von Änderungen in mehreren Redundanten
    - Hardwareänderungen
    - Softwareänderungen
- Wartung und Instandhaltung
    - Durchführung von Wartungs- und Instandhaltungstätigkeiten
    - Wartung und Instandhaltung in mehreren Redundanten
    - Verwendete Werkzeuge zur Wartung und Instandhaltung
    - Lebensdauer der COTS-Komponenten
    - Sicherstellung der Ersatzteilversorgung/Ersatzteilhaltung
- Dokumentation
    - Dokumentation der Eigenschaften der COTS-Komponenten
    - Dokumentation des Design- und Herstellungsprozesses der COTS-Komponenten
    - Dokumentation der Ergebnisse der Qualifizierung der COTS-Komponenten
    - Benutzerdokumentation zum sicheren Betrieb von COTS-Komponenten
    - Benötigte Informationen nach Einstellung des Supports durch den Hersteller

Der entwickelte Bewertungsansatz kann als Grundlage genutzt werden, um COTS-Komponenten hinsichtlich der Möglichkeit des Einsatzes in sicherheitstechnisch wichtigen elektro- und leittechnischen Einrichtungen in kerntechnischen Anlagen zu bewerten. Zudem gibt der Bewertungsansatz Hinweise bezüglich zu berücksichtigender Aspekte

und Anforderungen bei der Qualifizierung von COTS-Komponenten. Der Bewertungsansatz wurde in erster Linie auf der Basis von Anforderungen entwickelt, die für Kernkraftwerke aufgestellt wurden. Da der Bewertungsansatz Anforderungen hinsichtlich allgemein gültiger Aspekte aufstellt und nach den Kategorien der Sicherheitsfunktionen aufgebaut ist, ergibt sich aber prinzipiell auch die Möglichkeit, diesen auf andere kerntechnische Anlagen (z. B. Forschungsreaktoren, Zwischenlager) anzuwenden, wenn in diesen die sicherheitstechnisch wichtigen Funktionen entsprechend den Kategorien nach /DIN 10a/ kategorisiert worden sind.

Bei der Anwendung des Bewertungsansatzes ist zu bewerten, inwieweit die aufgestellten Anforderungen von den in Betracht gezogenen COTS-Komponenten erfüllt werden. Es ist zu erwähnen, dass die Anwendung des Bewertungsansatzes keine Qualifizierung von COTS-Komponenten ersetzt. Der Bewertungsansatz soll lediglich dazu dienen, die grundsätzliche Möglichkeit des Einsatzes von COTS-Komponenten in sicherheitstechnisch wichtigen elektro- und leittechnischen Einrichtungen in kerntechnischen Anlagen zu bewerten. Zudem soll der Bewertungsansatz Hinweise geben, welche Aspekte und Anforderungen bei einer Qualifizierung von COTS-Komponenten zu berücksichtigen sind.

## Literaturverzeichnis


/ALI 18/ Alithya, “Justification of Commercial Digital I&C Devices – A Canadian Perspective”, IAEA „Technical Meeting on Justification of Commercial Industrial Instrumentation and Control Equipment for Nuclear Power Plant Applications“, Toronto, Kanada, Juni 2018

/BEL 13/ BelV, „Assessment of Pre-existing and Commercial-Off-The-Shelf Software For Use in Functions Important to Safety”, R-SG-13-001-0-e-1, Juli 2013

/BMU 22/ Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz, BMUV, RS-Handbuch 3-0.1, „Sicherheitsanforderungen an Kernkraftwerke“, Februar 2022

/BMU 15/ Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz, BMUV, RS-Handbuch 3-0.2, „Interpretationen zu den Sicherheitsanforderungen an Kernkraftwerke“, März 2015

/BSI 13/ British Standards Institution, BSI, „Nuclear Power Plants. Instrumentation and control important to safety. Selection and use of industrial digital devices of limited functionality”, BS IEC 62671:2013-03-31, 2013

/CSA 07/ Canadian Standards Association, CSA, “Qualification of Pre-Developed Software for Use in Safety-Related Instrumentation and Control Applications in Nuclear Power Plants”, N290.14-07, 2007

/CSA 15/ Canadian Standards Association, CSA, Qualification of digital hardware and software for use in instrumentation and control applications for nuclear power plants”, N290.14:15, 2015

/DIN 10a/ Deutsches Institut für Normung, DIN, „Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Kategorisierung leittechnischer Funktionen“, DIN EN 61226:2010-08, 2010

/DIN 10b/ Deutsches Institut für Normung, DIN, „Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie A“, DIN EN 60880:2010-03, 2010

/DIN 10c/ Deutsches Institut für Normung, DIN, „Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen an die Hardware-Auslegung rechnerbasierter Systeme“, DIN EN 60987:2009, 2010

/DIN 11/ Deutsches Institut für Normung, DIN, „Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 1: Allgemeine Anforderungen“, DIN EN 61508-1:2011-02, 2011

/DIN 13/ Deutsches Institut für Normung, DIN, „Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung“, DIN EN 61513:2013-09, 2013

/DOA 06/ D. Doan, Naval Postgraduate School, California, USA, “Commercial off the Shelf (COTS) security issues and approaches”, 2006

/DOD 10/ Department of Defense, Naval Ordnance Safety and Security Activity “Joint Software Systems Safety Engineering Handbook”, 2010

/DOE 11/ U.S. Department of Energy, Office of environmental safety and quality “Guidance for commercial grade dedication”, 2011

/DOT 03/ U.S. Department of Transportation, Federal Railroad Administration, “Commercial-Off-The-Shelf (COTS) Hardware and Software for Train Control Applications: System Safety Considerations”, 2003

/DOT 17/ U.S. Department of Transportation, Federal Aviation Administration, “Simple and Complex Electronic Hardware Approval Guidance”, 2017

/EAS 21/ European Union Aviation Safety Agency, AMC 20-152 A, “Development of Assurance for Airborne Electronic Hardware”, 2021

/EPR 96/ Electric Power Research Institute, EPRI, “Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications”, TR-106439, 1996

/ESA 13/ European Space Agency, ESA, European Cooperation for Space Standardization, ECSS, “Space product assurance – Commercial electrical, electronic and electromechanical (EEE) components”, ECSS-Q-ST-60-13C, 2013

/IAE 20/ International Atomic Energy Agency, IAEA, “Challenges and Approaches for Selecting, Assessing and Qualifying Commercial Industrial Digital Instrumentation and Control Equipment for Use in Nuclear Power Plant Applications”, NR-T-3.31, 2020

/IEC 18/ International Electrotechnical Commission, IEC, „Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category B or C functions“, IEC 62138:2018-07, 2018

/KEL 19/ KELPO, “Development of the licensing and qualification processes for the systems and equipment of nuclear facilities in Finland” Final report, Januar 2019

/KEL 20/ KELPO 2, “Developing licensing and qualification of nuclear facilities, phase 2” Report, Januar 2020

/KTA 14a/ Sicherheitstechnische Regel des Kerntechnischen Ausschusses, KTA „Werksprüfungen, Prüfungen nach Instandsetzung und Nachweis der Betriebsbewährung der Baugruppen und Geräte der Sicherheitsleittechnik“ KTA 3507, November 2014

/KTA 14b/ Sicherheitstechnische Regel des Kerntechnischen Ausschusses, KTA „Übergeordnete Anforderungen an die elektrische Energieversorgung in Kernkraftwerken“, KTA 3701, November 2014

/KTA 15a/ Sicherheitstechnische Regel des Kerntechnischen Ausschusses, KTA Reaktorschutzsystem und Überwachungseinrichtungen des Sicherheitssystems, KTA 3501, November 2015

/KTA 15b/ Sicherheitstechnische Regel des Kerntechnischen Ausschusses, KTA „Typprüfung von elektrischen Baugruppen der Sicherheitsleittechnik“ KTA 3503, November 2015

/KTA 17/ Sicherheitstechnische Regel des Kerntechnischen Ausschusses, KTA „Kommunikationseinrichtungen für Kernkraftwerke“, KTA 3901, November 2017

/KTA 20/ Sicherheitstechnische Regel des Kerntechnischen Ausschusses, KTA „Prüfung und Betrieb von Hebezeugen in Kernkraftwerken“, KTA 3903 Dezember 2020

/NEI 19/ Nuclear Energy Institute, NEI, “Guidance on Using IEC 61508 SIL Certification to Support the Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Related Applications”, NEI 17-06, Revision B, 2019

/NRC 22/ U.S. NRC, “Dedication of Commercial-Grade Digital Instrumentation and Control Items for Use in Nuclear Power Plants”, Regulatory Guide RG 1.250, Revision 0, 2022

/ONR 19/ Office for Nuclear Regulation, ONR, “Computer Based Safety Systems”, Nuclear Safety Technical Assessment Guide, NS-TAST-GD-046, Revision 6, April 2019

/ONR 20/ Office for Nuclear Regulation, ONR, “Safety Assessment Principles for Nuclear Facilities”, 2014 Edition, Revision 1, Januar 2020

/ROG 18/ Rogalski, David, Ontario Power Generation, “Insights into the issues of using commercial software in nuclear power plants”, IAEA „Technical Meeting on Justification of Commercial Industrial Instrumentation and Control Equipment for Nuclear Power Plant Applications“, Toronto, Kanada, Juni 2018

/TRA 21/ Tractebel Engie, „Belgian experience with the supply of nuclear safety equipment”, EC-JRC “Workshop on Commercial Grade Dedication”, 2021

/VDI 11/ Verein Deutscher Ingenieure; Verband der Elektrotechnik, Elektronik, Informationstechnik, „Anforderungen an Serienprodukte und Kriterien für deren Einsatz in der Sicherheitsleittechnik in Kernkraftwerken“, VDI/VDE 3528, August 2011

/XIN 18/ Xing, Anqing, SNC Lavalin, Candu, “An Overview of Candu’s Qualification Programs for I&C Systems & Components”, IAEA „Technical Meeting on Justification of Commercial Industrial Instrumentation and Control Equipment for Nuclear Power Plant Applications“, Toronto, Kanada, Juni 2018

/STU 19/ Stuk, Radiation and Nuclear Safety Authority, Guide YVL E.7, “Electrical and I&C equipment of a nuclear facility”, 2019

**Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH**

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

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

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

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

www.grs.de

**ISBN 978-3-910548-58-9**