ICS 27.120.20

VDI/VDE-RICHTLINIEN

April 2018

VEREIN DEUTSCHER INGENIEURE

VERBAND DER ELEKTROTECHNIK ELEKTRONIK INFORMATIONSTECHNIK

Anforderungen an Serienprodukte und Kriterien für deren Einsatz in der Sicherheitsleittechnik in Kernkraftwerken

Vorgehen zum Nachweis der Dissimilarität und für eine abgestufte Qualifizierung für dissimilar einzusetzende Serienprodukte

Requirements of commercial-grade products and criteria for their use in the instrumentation and control systems important to safety in nuclear power plants

Procedure for the proof of dissimilarity and for a graded qualification for dissimilar used commercial-grade products

VDI/VDE 3528

Blatt 1.1 / Part 1.1

Ausg. deutsch/englisch
Issue German/English

Die deutsche Version dieser Richtlinie ist verbindlich.

The German version of this standard shall be taken as authoritative. No guarantee can be given with respect to the English translation.

Inhalt Seite

Contents Page

VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA)
Fachbereich Anwendungsfelder der Automation

Vorbemerkung

Der Inhalt dieser Richtlinie ist entstanden unter Beachtung der Vorgaben und Empfehlungen der Richtlinie VDI 1000.

Allen, die ehrenamtlich an der Erarbeitung dieser Richtlinie mitgewirkt haben, sei gedankt.

Eine Liste der aktuell verfügbaren Blätter dieser Richtlinienreihe ist im Internet abrufbar unter www.vdi.de/3528.

Einleitung

Die sicherheitstechnisch wichtige Leittechnik in Kernkraftwerken ist zur Erhöhung der Zuverlässigkeit im Allgemeinen mehrfach redundant ausgelegt. Die dabei übliche dreifache oder vierfache Redundanz in homogener Gerätetechnik erzielt gegenüber einer einfachen Auslegung einen hohen Effekt auf die sich ergebende Zuverlässigkeit. Allerdings würde durch Hinzufügen weiterer Redundanzen dieser positive Effekt nicht noch stärker wirksam, da sich in solchen Systemkonfigurationen der Einfluss des Common Cause Failure (CCF) bemerkbar macht und die erreichbare Zuverlässigkeit begrenzt. Für eine weitere Erhöhung der Zuverlässigkeit sind damit Maßnahmen gegen CCF erforderlich.

In der DIN EN 62340 werden Maßnahmen gegen CCF aufgeführt. Diese kann man grob in Maßnahmen zur

- Vermeidung von Auslegungsfehlern,
- Sicherstellung/Erhöhung der Robustheit gegen Auslegungsfehler und
- Eingrenzung des Auswirkungsbereichs von CCF gliedern.

Für eine wirksame Beherrschung von CCF ist die Berücksichtigung aller drei Aspekte erforderlich.

Maßnahmen zur Vermeidung von Auslegungsfehlern beziehen sich im Wesentlichen auf die Qualitätssicherung der Hardware- und Softwareerstellung inklusive der Verifizierungs- und Validierungsmaßnahmen. Maßnahmen zur Sicherstellung/ Erhöhung der Robustheit gegen Auslegungsfehler umfassen einerseits den Nachweis der Robustheit der Hardware durch entsprechende praktische Prü-

Preliminary note

The content of this standard has been developed in strict accordance with the requirements and recommendations of the standard VDI 1000.

We wish to express our gratitude to all honorary contributors to this standard.

A catalogue of all available parts of this series of standards can be accessed on the Internet at www.vdi.de/3528.

Introduction

The I&C systems important to safety in nuclear power plants are generally designed with multiple redundancy in order to increase reliability. The customary triple or quadruple redundancy with homogeneous equipment technology has a great effect on the resulting reliability in comparison with single systems. Adding further redundancies, however, does not increase that favourable effect any further, as the influence of common cause failure (CCF) becomes apparent in such system configurations and limits the achievable level of reliability. Measures to counteract CCF are therefore necessary if reliability is to be further increased.

DIN EN 62340 presents measures to cope with CCF. These can roughly be subdivided into measures for

- avoidance of design faults,
- ensuring and increasing robustness in the face of design faults, and
- scope of effect of CCF.

All three aspects have to be taken into account if CCF is to be effectively overcome.

Measures to avoid design faults essentially concern quality assurance during the production of hardware and software, including the verification and validation processes. Measures to ensure and increase robustness in the face of design faults comprise on the one hand demonstration of the robustness of the hardware by appropriate practical tests, and on the other hand the application of best prac-

fungen und andererseits die Anwendung von Best-Practice-Auslegungsprinzipien mit großen Designmargen zur Vermeidung von fehlerträchtigen oder fehleranfälligen Konstruktionen. Die Beherrschung eines CCF erfolgt durch die Begrenzung des Auswirkungsbereichs von latenten Fehlern auf einen Teil des Leittechniksystems, sodass die leittechnische Funktion weiterhin aufrechterhalten bleibt. Hieraus resultieren Maßnahmen wie räumliche Trennung, Fehlerfortpflanzungsbarrieren und auch der Einsatz von dissimilarer Gerätetechnik.

Im Hinblick auf die Beherrschung des CCF aufgrund eines gerätebedingten latenten Fehlers ist die Auslegung der unabhängigen Teilsysteme des Leittechniksystems so vorzunehmen, dass sie nicht durch den gleichen gerätebedingten Fehler beeinträchtigt werden können. Um diesen Ausschluss beim Auswirkungsbereich führen zu können, sind diese Teilsysteme in unterschiedlichen, im Sinne dieser Regel dissimilaren Gerätetechniken auszuführen. Auch die Anwendung des Äquivalenzprinzips, mit dem die Möglichkeit besteht, die Erfüllung des nächsthöheren Qualifizierungslevels in Anspruch zu nehmen, erfordert den Einsatz von dissimilaren Geräten in geeignet verschalteten Strukturen (siehe VDI/VDE 3528 Blatt 1, Abschnitt 5.4).

Die Realisierung von unabhängigen Teilsystemen in der Leittechnikarchitektur mit dissimilaren Geräten mit einer Basisqualifizierung, wie sie in dieser Richtlinie beschrieben ist, wirkt bei geeigneter Verschaltung der Teilsysteme grundsätzlich positiv auf die Zuverlässigkeit des Gesamtsystems.

Der Begriff Dissimilarität beschreibt eine Beziehung zwischen zwei Gerätetechniken, die nur im Rahmen einer detaillierten Untersuchung festgestellt werden kann. Im Rahmen dieser Untersuchung wird geprüft, ob die zwei infrage stehenden Gerätetechniken hinsichtlich Hardware, Software, Entwicklungswerkzeugen, Entwicklungsteams, Fertigung und Test hinreichend unähnlich/ungleichartig sind und damit als dissimilar bezeichnet werden können (siehe VDI/VDE 3528 Blatt 1, Abschnitt 3).

Um bereits im Rahmen der kerntechnischen Typprüfung die Grundgedanken des Äquivalenzprinzips umzusetzen, gibt diese Richtlinie Empfehlungen für ein abgestuftes Qualifizierungsvorgehen auf folgender Basis:

- Nachweis von gegenüber den kerntechnischen Regeln abgestuften Anforderungen bezüglich Maßnahmen zur Erkennung von eventuell im Rahmen der Entwicklung eingebrachten latenten Fehlern
- Nachweis der Dissimilarität der einzusetzenden Gerätetechniken

tice dimensioning principles with large design margins in order to avoid designs which are potentially faulty or susceptible to faults. Limiting the consequence of a CCF is achieved by limiting the area of impact of latent faults to a part of the I&C system, so that the I&C function is preserved. The resulting measures include spatial separation, barriers to fault propagation and use of dissimilar equipment technology.

With regard to overcoming the CCF which results from a latent fault in a particular device, the independent parts of the I&C system are to be designed in such a way that they cannot be impaired by the same device-related fault. In order to preclude such an event in the area affected, these parts of the system are to be implemented with different, and within the terms of this standard, dissimilar, equipment technologies. Application of the equivalence principle, with which there is an opportunity to achieve fulfilment of the next higher qualification level, also requires the use of dissimilar devices in suitably connected structures (see VDI/VDE 3528 Part 1, Section 5.4).

The implementation of independent subsystems in the I&C system architecture using dissimilar devices with basic qualification, such as is described in this standard, and with suitable connection of the subsystems, fundamentally has a beneficial effect on the reliability of the system as a whole.

The term dissimilarity describes a relationship between two equipment technologies which can only be identified in the course of a detailed examination. In that examination, it is ascertained whether the two equipment technologies in question are sufficiently unlike and disparate in terms of hardware, software, development tools, development teams, manufacturing and testing to be described as dissimilar (see VDI/VDE 3528 Part 1, Section 3).

In order to incorporate the fundamental ideas of the equivalence principle at the early stage of nuclear type testing, this standard presents recommendations for a graduated qualification procedure on the following basis:

- demonstration of fulfilment of graduated requirements in relation to nuclear regulatory standards with regard to measures for detection of latent faults potentially incorporated in the course of development
- demonstration of the dissimilarity of the equipment technologies to be employed

Durch den Einsatz dissimilarer Geräte in den Teilsystemen des Leittechniksystems in Verbindung mit der Basisqualifizierung kann damit in einem mindestens vergleichbaren Maß wie bei den z.B. nach KTA 3503 typgeprüften Geräten sichergestellt werden, dass nicht alle Teilsysteme durch den gleichen gerätebedingten Fehler beeinträchtigt werden. Zielsetzung des Qualifizierungsvorgehens entsprechend dieser Richtlinie ist es, geeignete Seriengeräte kerntechnisch qualifizieren zu können, auch wenn diese nicht explizit für den kerntechnischen Markt entwickelt wurden. Diese Vorgehensweise berücksichtigt die industriellen Gegebenheiten.

Dieses Qualifizierungsvorgehen ermöglicht eine Reduzierung der Anforderungen für den Nachweis der Maßnahmen zur Fehlervermeidung (QS-Maßnahmen im Rahmen der Entwicklung), deren vollständige Erfüllung im Allgemeinen bei bereits entwickelten Geräten aus dem Industriebereich nicht gezeigt werden kann. Des Weiteren kann sich die Prüfung der Realisierung hauptsächlich auf die Spezifikationsebene konzentrieren und die Prüfung der Implementierung auf besondere Aspekte entfallen. Neben den Vorteilen, die dieses Vorgehen hinsichtlich des Qualifizierungsaufwands bietet, ist mit einem Verzicht auf die Vorlage von Unterlagen zu den Implementierungsdetails auch einer der größten Hinderungsgründe für die Qualifizierung von Seriengeräten beseitigt, da diese Unterlagen sehr oft Restriktionen der Hersteller, z.B. aufgrund des Know-how-Schutzes, unterliegen. Die Funktionsnachweise (Funktionstests) und Eigenschaftsnachweise (Grenzbelastungsanalyse, Ausfallratenbestimmung, Umweltprüfungen) sind von der Abstufung der Anforderungen nicht betroffen. Diese stellen auch kein Qualifizierungshindernis dar, da sie auch an bereits fertig entwickelten Geräten durchgeführt werden können.

1 Anwendungsbereich

VDI/VDE 3528 Blatt 1 gibt Empfehlungen, wie die Auslegungsziele der Sicherheitsleittechnik[1)] bei Verwendung von Geräten unterschiedlicher Qualifizierungstiefe erreicht werden können. Es zeigt Möglichkeiten auf, wie die mit einer abgestuften Qualifizierungstiefe verbundenen fehlenden Nachweise zur Vermeidung latenter Fehler durch eine entsprechende Auslegung der Sicherheitsleittechnik kompensiert und damit deren Auswirkungen toleriert werden können. Dies erfordert die Verwendung zueinander dissimilarer Produkte, deren Dissimilarität nachgewiesen ist.

With the use of dissimilar devices in the subsystems of the I&C system in conjunction with basic qualification, it can be ensured to an extent at least comparable to that ensured, for example, by devices type tested to KTA 3503, that not all the subsystems are impaired by the same device-related fault. The objective of the qualification procedure as set out in this standard is to be able to qualify suitable commercial grade devices for nuclear applications, even if they were not developed specifically for the nuclear market. This procedure takes account of the circumstances in the industry.

This qualification procedure permits a reduction in the requirements for demonstration of measures to avoid faults (QA measures in the course of development), as industrial equipment which has already been developed cannot generally be seen to comply with these in full. Furthermore, the review of the implementation can mainly concentrate on the specification level, and inspections for special aspects of implementation are not required. Apart from the advantages which this procedure provides with regard to the amount of cost and effort required for qualification, dispensing with the submission of documentation on the implementation details also removes one of the greatest obstacles to the qualification of commercial grade equipment, as those documents are very often subject to manufacturers' restrictions, for instance to ensure the protection of know-how. The functional test documentation and documentation on characteristics (critical load analysis, failure rate determination and environmental tests) are not affected by the downgrading of requirements. They also do not present any obstacle to qualification, as they can be performed on equipment which has already been completely developed.

1 Scope

VDI/VDE 3528 Part 1 presents recommendations on how the design objectives applicable to I&C systems important to safety[1)] can be achieved when equipment of different qualification depths is used. It illustrates opportunities to compensate for the lack of documentation on the avoidance of latent faults which is associated with a downgraded qualification level by corresponding design of the I&C systems important to safety, with the result that the effects of that latent faults can be tolerated. This requires the use of products which are dissimilar to each other and for which dissimilarity has been demonstrated.

[1)] Dieser Begriff umfasst auch Geräte der Elektrotechnik (z.B. Schutzgeräte). /
This term also includes electrical equipment (e.g. protection devices).

Die hier vorliegende Richtlinie enthält Empfehlungen, wie der Nachweis der Dissimilarität zwischen Geräten und die hierzu erforderliche Basisqualifizierung geführt werden sollte. Die mit diesem Nachweis erreichte Qualifizierung entspricht der Designvariante 2 der VDI/VDE 3528 Blatt 1.

Die Richtlinie ist anwendbar, wenn die Dissimilarität als Mittel zur Erhöhung der Toleranz gegenüber den Auswirkungen latenter Fehler kreditiert werden soll.

2 Normative Verweise

Das folgende zitierte Dokument ist für die Anwendung dieser Richtlinie erforderlich:

VDI 3528 Blatt 1:2017-06 Anforderungen an Serienprodukte und Kriterien für deren Einsatz in der Sicherheitsleittechnik in Kernkraftwerken; Allgemeiner Teil

This standard contains recommendations on how the demonstration of dissimilarity between devices and the basic qualification required should be managed. The qualification achieved by that demonstration corresponds to design variant 2 in VDI/VDE 3528 Part 1.

This standard is applicable when the dissimilarity is to be used as a means of increasing the tolerance of the effects of latent faults.

2 Normative references

The following referenced document is indispensable for the application of this standard:

VDI 3528 Part 1:2017-06 Requirements of commercial grade products and criteria for their use in the instrumentation and control systems important to safety in nuclear power plants; General part