

VEREIN DEUTSCHER
INGENIEURE

VERBAND DER
ELEKTROTECHNIK
ELEKTRONIK
INFORMATIONSTECHNIK

**Kriterien zur Gewährleistung der
Unabhängigkeit von Sicherheitsfunktionen
bei der Leittechnik-Auslegung**

VDI/VDE 3527

**Design criteria serving to ensure
independence of I & C safety functions**

**Ausg. deutsch/englisch
Issue German/English**

Die deutsche Version dieser Richtlinie ist verbindlich.

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

Inhalt	Seite	Contents	Page
Vorbemerkungen	3	Preliminary note	3
1 Zweck und Geltungsbereich	4	1 Objective and scope	4
2 Begriffserläuterungen	4	2 Terms and definitions	4
2.1 Abweichung	5	2.1 Error	5
2.2 Ausfall	5	2.2 Fault	5
2.3 Ausfalltoleranz	5	2.3 Fault tolerance	5
2.4 Betriebserfahrung	5	2.4 Operational experience	5
2.5 Common-cause-bedingtes Versagen (CCF: Common Cause Failure)	6	2.5 Common cause failure (CCF)	6
2.6 Defence-in-Depth (DiD)	6	2.6 Defence in depth (DiD)	6
2.7 Deterministisches Systemverhalten	6	2.7 Deterministic system response	6
2.8 Diversität	7	2.8 Diversity	7
2.9 Einzel-Ausfall-Kriterium (Single Failure Criterion)	7	2.9 Single-failure criterion	7
2.10 Entwurfsfehler	8	2.10 Design fault	8
2.11 Fail-safe-Auslegung	8	2.11 Fail-safe design	8
2.12 Fehler	8	2.12 Fault	8
2.13 Fehlervermeidung	9	2.13 Fault avoidance	9
2.14 Funktionale Sicherheit	9	2.14 Functional safety	9
2.15 Gerätefamilie (System-Plattform)	9	2.15 Equipment family (system platform)	9
2.16 Irrtum	10	2.16 Mistake, human error	10
2.17 Redundanz	10	2.17 Redundancy	10
2.18 Security	10	2.18 Security	10
2.19 Security Zone	10	2.19 Security zone	10
2.20 Signal-Trajektorie	10	2.20 Signal trajectory	10
2.21 System	11	2.21 System	11
2.22 Systematisches Versagen	12	2.22 Systematic failure	12
2.23 Validierung	12	2.23 Validation	12
2.24 Verifizierung	12	2.24 Verification	12
2.25 Versagen	13	2.25 Failure	13
2.26 Zufallsausfall	13	2.26 Random fault	13

VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA)

Fachausschuss Leittechnik in Kernkraftwerken

**VDI/VDE-Handbuch Regelungstechnik
VDI-Handbuch Energietechnik**

Frühere Ausgaben: 4/01 Entwurf, deutsch
Former edition: 4/01 draft, in German only

Zu beziehen durch / Available from Beuth Verlag GmbH, 10772 Berlin – Alle Rechte vorbehalten / All rights reserved © Verein Deutscher Ingenieure, Düsseldorf 2002

Vervielfältigung – auch für innerbetriebliche Zwecke – nicht gestattet / Reproduction – even for internal use – not permitted

	Seite		Page
3 Fehlermodelle bei Auslegung der Leittechnik.	14	3 Fault models used in designing I & C systems.	14
3.1 Einzel-Ausfall-Kriterium	14	3.1 Single-failure criterion	14
3.2 Defence-in-Depth Prinzip in der Leittechnik.	14	3.2 The defence-in-depth principle in I & C systems.	14
3.3 Common-cause-bedingtes Versagen	14	3.3 Common cause failure	14
3.4 Barrieren gegen die Versagensausbreitung.	16	3.4 Barriers preventing the spreading of failures	16
3.4.1 Funktionale Barrieren	17	3.4.1 Functional barriers.	17
3.4.2 Gerätetechnische Barrieren.	17	3.4.2 Physical barriers.	17
3.4.3 Datentechnische Barrieren	18	3.4.3 IT barriers	18
3.5 Schutz vor unzulässigen Zugriffen	19	3.5 Protection against unauthorised access	19
3.6 Änderungs- und Konfigurations-Management.	20	3.6 Management of modifications and configurations.	20
4 Versagensmechanismen und Versagensmodelle.	22	4 Mechanisms and models of failures	22
4.1 Fehler aus der Aufgabenstellung für Leittechnik.	23	4.1 Faults resulting from the definition of the task for the I & C systems.	23
4.2 Fehler in der Leittechnik-Auslegung	24	4.2 Faults in I & C system design	24
4.3 Versagen durch Umwelteinflüsse	24	4.3 Failure due to environmental effects	24
4.4 Fehler bei Instandhaltung und Änderungen im Betrieb	25	4.4 Faults in servicing and modifications during operation	25
4.5 Versagen auf Grund von unzulässigen Eingriffen	25	4.5 Failure caused by unauthorised access.	25
5 Auslegungsempfehlungen zur Gewährleistung der Unabhängigkeit.	26	5 Design recommendations serving to ensure independence	27
5.1 Auslegungsfehler aus der Aufgabenstellung für die Leittechnik	26	5.1 Design faults resulting from the definition of the task for the I & C systems.	27
5.2 Fehler in der Leittechnik-Auslegung	26	5.2 Faults in I & C system design	27
5.3 Versagen durch Umwelteinflüsse	28	5.3 Failure due to environmental effects.	29
5.4 Fehler bei Instandhaltung und Änderungen im Betrieb	30	5.4 Faults in servicing and modifications during operation	31
5.5 Versagen auf Grund von unzulässigen Eingriffen	32	5.5 Failure caused by unauthorised access.	33
6 Erläuterung zu den Auslegungsempfehlungen.	32	6 Explanations concerning the design recommendations	33
6.1 Auslegungsfehler aus der Aufgabenstellung für die Leittechnik	32	6.1 Design faults in the definition of the task for the I & C system.	33
6.1.1 Fehlerhafte Spezifikation für die „Soll-Funktionen“ der Leittechnik.	32	6.1.1 Faulty specification of the "desired functions" of the I & C system.	33
6.2 Fehler in der Leittechnik-Auslegung	37	6.2 Faults in I & C system design	37
6.2.1 Fehlerhaft erstellte Anwendersoftware auf Grund von Fehlern im Engineeringprozess	38	6.2.1 Faulty application software resulting from faults in the engineering process	38
6.2.2 Fehlerhaft erstellte Anwendersoftware auf Grund von fehlerhaften Algorithmen.	39	6.2.2 Faulty application software resulting from faulty algorithms	39
6.2.3 Fehlerhafte Ausbreitung von Einzelfehlern über Kommunikationswege	40	6.2.3 Unwanted spreading of single faults via communications paths.	40

	Seite		Page
6.2.4	42	6.2.4	42
6.2.5	43	6.2.5	43
6.2.6	45	6.2.6	45
6.2.7	47	6.2.7	47
6.3	47	6.3	47
6.4	47	6.4	47
6.4.1	48	6.4.1	48
6.4.2	48	6.4.2	48
6.4.3	48	6.4.3	48
6.4.4	48	6.4.4	48
6.4.5	48	6.4.5	48
6.5	50	6.5	50

Vorbemerkungen

Der Einsatz neuer, rechnerbasierter Sicherheits-Leittechnik zieht oftmals eine erhebliche Veränderung der vorhandenen, bewährten leittechnischen Strukturen nach sich. Dies betrifft im Allgemeinen die Verteilung und die Konzentration der leittechnischen Funktionen sowie die Zunahme der Komplexität der leittechnischen Verarbeitungseinheiten und Kommunikationsverbindungen. Der zumeist historisch bedingte heterogene wenig komplexe und stark verteilte Aufbau der bisher eingesetzten, festverdrahteten Sicherheits-Leittechnik trägt im großen Maße dadurch zur Zuverlässigkeit bei, dass die Wahrscheinlichkeit von common-cause-bedingtem Versagen (CCF) relativ gering ist. Andererseits werden durch diesen historisch bedingten Aufbau mit unterschiedlichen Gerätefamilien häufig die Service-Arbeiten ebenso wie die Beurteilung der Konsequenzen aus Eingriffen bzw. Änderungen erschwert.

Als Voraussetzung für neuartige Strukturen oder eine Veränderung der Sicherheits-Leittechnik muss sichergestellt bleiben, dass die Sicherheitsanforderungen weiter erfüllt werden und zwar unabhängig von der eingesetzten Technologie. Insbesondere sind bei der Ablösung des heterogenen Aufbaus geeignete

Preliminary note

The implementation of new, computer-based I & C systems important to safety often entails considerable changes in the existing, proven I & C structures. In general, this concerns the distribution and concentration of I & C functions, and also the increase in complexity of I & C processing units and communications connections. As a consequence of their historical evolution, hard-wired I & C systems important to safety used to date are mostly heterogeneous in structure, not very complex and distributed to a high degree. This greatly contributes to their reliability as the probability of common cause failure (CCF) is rather small. On the other hand, this historically evolved structure involving different equipment families often renders servicing, and also the assessment of the consequences of interventions and modifications, difficult.

It is prerequisite to new structures, and to changes in the structure, of I & C systems important to safety that safety requirements continue to be met irrespective of the technology used. In particular, appropriate precautions against potential common cause failure shall be taken where the heterogeneous structure is