

**Kernkraftwerke –  
Leittechnik für Systeme mit sicherheitstechnischer Bedeutung –  
Softwareaspekte für rechnerbasierte Systeme zur Realisierung von  
Funktionen der Kategorie A**

**Inhalt**

	Seite
Einleitung.....	9
1 Anwendungsbereich .....	11
2 Normative Verweisungen.....	11
3 Begriffe.....	12
4 Formelzeichen und Abkürzungen .....	18
5 Allgemeine Anforderungen für Software-Projekte .....	19
5.1 Einleitung .....	19
5.2 Softwaretypen .....	21
5.3 Vorgehensweise zur Software-Entwicklung .....	21
5.4 Software-Projektmanagement .....	23
5.5 Software-Qualitätssicherungsplan .....	23
5.6 Konfigurationsmanagement.....	24
5.7 Zugriffsschutz.....	25
6 Software-Anforderungen.....	27
6.1 Spezifikation der Software-Anforderungen.....	27
6.2 Selbstüberwachung .....	27
6.3 Periodische Prüfungen .....	28
6.4 Dokumentation.....	28
7 Auslegung und Implementierung .....	29
7.1 Prinzipien der Auslegung und Realisierung.....	29
7.2 Sprachen und zugehörige Übersetzer und Werkzeuge.....	31
7.3 Detaillierte Empfehlungen.....	32
7.4 Dokumentation.....	34
8 Software-Verifizierung .....	34
8.1 Software-Verifizierungsvorgang.....	34
8.2 Software-Verifizierungstätigkeiten .....	35
9 Softwareaspekte der Systemintegration .....	39
9.1 Softwareaspekte des Systemintegrationsplans.....	39
9.2 Systemintegration .....	40
9.3 Verifizierung des integrierten Systems .....	40
9.4 Prozeduren zur Fehlerbehebung .....	41
9.5 Softwareaspekte zum Bericht über die Verifizierung des integrierten Systems.....	41
10 Softwareaspekte der Systemvalidierung .....	42
10.1 Softwareaspekte des Systemvalidierungsplans .....	42

	Seite
10.2 Systemvalidierung .....	42
10.3 Softwareaspekte im Bericht zur Systemvalidierung .....	42
10.4 Prozeduren zur Fehlerbehebung .....	43
11 Software-Modifizierung .....	43
11.1 Prozedur zur Modifizierungsanfrage .....	44
11.2 Prozedur zur Durchführung einer Software-Modifizierung .....	45
11.3 Software-Modifizierung nach Auslieferung .....	46
12 Softwareaspekte bei Installation und Betrieb .....	47
12.1 Installation der Software auf der Anlage .....	47
12.2 Zugriffsschutz der Software auf der Anlage .....	47
12.3 Anpassung der Software an die Bedingungen auf der Anlage .....	47
12.4 Operateurtraining .....	48
13 Vorkehrungen gegen CCF durch Softwarefehler .....	48
13.1 Allgemeines .....	48
13.2 Software-Auslegung gegen CCF .....	49
13.3 Ursachen und Auswirkungen von CCF durch Softwarefehler .....	50
13.4 Realisierung von Diversität .....	50
13.5 Abwägung der Vor- und Nachteile bei Verwendung von Diversität .....	51
14 Software-Werkzeuge für die Erstellung von Software .....	51
14.1 Allgemeines .....	51
14.2 Auswahl der Werkzeuge .....	52
14.3 Anforderungen an Werkzeuge .....	52
15 Qualifizierung vorgefertigter Software .....	57
15.1 Allgemeines .....	57
15.2 Allgemeine Anforderungen .....	57
15.3 Bewertungs- und Beurteilungsprozess .....	58
15.4 Anforderungen an die Systemintegration und Modifizierung vorgefertigter Software .....	66
Anhang A (normativ) Software-Sicherheitslebenszyklus und Details von Software-Anforderungen .....	67
Anhang B (normativ) Detaillierte Anforderungen und Empfehlungen für Auslegung und Realisierung .....	69
Anhang C (informativ) Beispiel für anwendungsorientiertes Software-Engineering (Software-Entwicklung mit anwendungsorientierten Sprachen) .....	82
Anhang D (informativ) Sprache, Übersetzer, Linkage-Editor .....	86
Anhang E (informativ) Software-Verifizierung und Prüfung .....	88
Anhang F (informativ) Typische Liste für Software-Dokumentation .....	95
Anhang G (informativ) Überlegungen zu CCF und Diversität .....	96
Anhang H (informativ) Werkzeuge zur Erstellung und Prüfung von Spezifikation, Auslegung und Realisierung .....	100
Anhang I (informativ) Anforderungen betreffend vorgefertigte Software .....	102
Anhang J (informativ) Zusammenhang zwischen IEC 61513 und dieser Norm .....	104

	Seite
Bild 1 – Tätigkeiten im System-Sicherheitslebenszyklus (nach IEC 61513) .....	19
Bild 2 – Softwarebezogene Tätigkeiten im System-Sicherheitslebenszyklus.....	20
Bild 3 – Entwicklungstätigkeiten im Software-Sicherheitslebenszyklus nach dieser Norm .....	22
Bild 4 – Übersicht des Qualifizierungsvorgangs von vorgefertigter Software (PDS) .....	59
Bild 5 – Beziehung der Bewertung und Analyse vorgefertigter Software mit dem Qualifizierungsplan des Systems, in das die vorgefertigte Software integriert ist.....	60
Bild C.1 – Lebenszyklus für anwendungsorientiertes Software-Engineering .....	85
Tabelle 1 – Prozess- und Produktaspekte von Auslegung und Implementierung .....	33
Tabelle J.1 – Zusammenhang zwischen IEC 61513 und dieser Norm.....	105
Tabelle J.2 – Abschnitte aus IEC 60880, die bei der nächsten Überarbeitung von IEC 61513 zu berücksichtigen sind .....	108