

Inhalt

	Seite
Vorwort.....	2
Einleitung	4
1 Anwendungsbereich	5
2 Normative Verweisungen	6
3 Begriffe	7
4 Abkürzungen.....	11
5 Bedingungen und Strategie zur Beherrschung von CCF	11
5.1 Allgemeines	11
5.2 CCF-Charakteristiken	11
5.3 Prinzipielle CCF-Mechanismen digitaler leittechnischer Systeme	12
5.4 Bedingungen zur Bekämpfung von CCF in einzelnen leittechnischen Systemen	12
5.5 Auslegungsstrategie zur Beherrschung von CCF	13
6 Anforderungen zur Beherrschung von Fehlern in der Anforderungsspezifikation	14
6.1 Ableitung der Anforderungsspezifikation für die Leittechnik aus der sicherheitstechnischen Auslegungsbasis der Anlage.....	14
6.2 Anwendung des DiD-Prinzips und der funktionalen Diversität.....	15
6.3 CCF-Gesichtspunkte für bestehende Anlagen.....	16
7 Auslegungsmaßnahmen gegen koinzidentes Versagen leittechnischer Systeme.....	16
7.1 Das Prinzip der Unabhängigkeit.....	16
7.2 Auslegung unabhängiger leittechnischer Systeme	17
7.3 Anwendung funktionaler Diversität.....	17
7.4 Vermeidung von Fehlerfortpflanzung über Kommunikationspfade	18
7.5 Auslegungsmaßnahmen gegen Systemausfall wegen Wartungsarbeiten.....	18
7.6 Integrität der leittechnischen Systemhardware	18
7.7 Vorkehrungen gegen Abhängigkeit von externen Daten oder Meldungen	19
7.8 Sicherstellung physikalischer Trennung und Robustheit für Umgebungsbedingungen.....	19
8 Toleranz gegen angenommene latente Softwarefehler	19
9 Anforderungen zur Vermeidung von Systemversagen infolge Wartung während des Betriebs	20
Anhang A (informativ) Beziehung zwischen IEC 60880 und dieser Norm	21
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen	22