ICS 01.040.33; 33.040.20

VDI/VDE-RICHTLINIEN

Juli 2002
July 2002

VEREIN DEUTSCHER INGENIEURE

VERBAND DER ELEKTROTECHNIK ELEKTRONIK INFORMATIONSTECHNIK

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

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

VDI/VDE 3527

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

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

Fachausschuss Leittechnik in Kernkraftwerken

VDI/VDE-Handbuch Regelungstechnik
VDI-Handbuch Energietechnik

Seite

Page

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 Kommunikatonsverbindungen. 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