Grundlagen der funktionalen Sicherheit
in der Maschinen-, Prozess-, Fahrzeug- und Gebäudetechnik

Die neue internationale Norm IEC 61508 gilt als Basic Safety Publication und hat in den letzten drei Jahren zu einer weltweiten Verbreitung der Forderung nach funktionaler Sicherheit komplexer elektronischer Steuerungen bei Endanwendern geführt. Die IEC 61508, die bereits als Europäische Norm EN 61508 übernommen wurde, ist nur ein erster Schritt in einer langen Kette von Normen zur funktionalen Sicherheit von computerbasierten Systemen und Software und ist seit August 2004 in Deutschland in nationales Recht umgesetzt. Diese Normenreihe dient als generischer Standard für die Entwicklung von sicherheitskritischen elektrischen, elektronischen und programmierbaren elektronischen Systemen und ist als Grundlage für die Entwicklung zukünftiger anwendungsorientierter Normen und Produktnormen vorgesehen. Damit gelten die bisherigen Normen wie DIN V VDE0801, DIN V 19250 und DIN V 19251 nicht mehr.

Ziel ist es, durch die fachgemäße Anwendung des Standards sicherzustellen, dass der Entwickler eines sicherheitskritischen Systems, der Errichter oder der Betreiber einer sicherheitskritischen technischen Anlage durch die Risikoreduzierung seine Sorgfaltspflicht erfüllt und den Stand der Technik eingehalten hat.

Die Herausforderung der neuen IEC 61508: Der neue Standard erfordert ein Umdenken im Hinblick auf die Betrachtung des ganzheitlichen Systemansatzes, der die sicherheitstechnischen Anforderungen an einzelne komplexe Geräte auf die komplette Sicherheitsinstallation vom Sensor bis Aktor einschließlich der Managementrahmenbedingungen erweitert (Phasenmodell, Lebenszyklusmodell). Er bietet dem Entwickler gegenüber den bisherigen Standards auch die Chance, durch entsprechendes Systemdesign das geforderte Sicherheitsniveau zu erreichen. Hinweise in der Norm, die gegenüber den zurückgezogenen Normen deutlich an Verbindlichkeit gewonnen haben, helfen ihm dabei.
Die IEC 61508 führt zu einer Neubetrachtung der Anforderungen an die Sicherheitsnachweise in der Hardware- und Software-Entwicklung.

Die Konsequenzen aufgrund der Umsetzung der neuen IEC 61508:
Der Standard fordert einen quantitativen Nachweis für das verbleibende Restrisiko auf Basis einer Berechnung der Versagenswahrscheinlichkeit. Zusätzlich zu den technischen Forderungen sind organisatorische Maßnahmen zur Vermeidung von Fehlern vorgeschrieben, die das verbleibende Restrisiko minimieren. Richtige Entscheidungen hinsichtlich Sicherheitsstrukturen, Entwurfsverfahren und Werkzeugen bei der Entwicklung von sicherheitsgerichteten Systemen und frühzeitige Verifikation der Entwicklungsergebnisse vermeiden Korrekturen sowie Fehlentwicklungen und senken dadurch Ihre Entwicklungszeit und Kosten.

Kurz und knapp:

Die neue internationale Norm IEC 61508 gilt als Basic Safety Publication und hat in letzter Zeit zu einer weltweiten Verbreitung der Forderung nach funktionaler Sicherheit komplexer elektronischer Steuerungen bei Endanwendern geführt. Der Standard fordert einen quantitativen Nachweis für das verbleibende Restrisiko, auf Basis einer Berechnung der Versagenswahrscheinlichkeit.
TÜV NORD bietet Hilfe bei der Entwicklung, Prüfung und Zertifizierung sicherheitsrelevanter Produkte aus den Bereichen Maschinen-, Prozess-, Fahrzeugtechnik und Gebäudetechnik.

TÜV NORD
Zertifizierung

TÜV NORD bietet Hilfe bei der Entwicklung, Prüfung und Zertifizierung sicherheitsrelevanter Produkte aus den Bereichen Maschinentechnik, Prozesstechnik, Fahrzeugtechnik und Gebäudetechnik, z. B. durch:

- Seminare und Inhouse-Schulungen zur Anwendung des internationalen Standards IEC 61508
- Konstruktive Unterstützung bei der Interpretation von nationalen und internationalen Standards
- Optimierung von Entwicklungsprozessen
- Prüfung von Sicherheitskonzepten
- Sicherheits-, Zuverlässigkeits- und Verfügbarkeitsanalysen
- Durchführung von Fehlerbaumanalysen (FTA) und Fehlereffektanalysen (FMEA/FMEDA)
- Durchführung von Sicherheitsanalysen und Sicherheitskonzeptionen, Berechnung der Restfehlerwahrscheinlichkeit von Sicherheitsloops in Anlagen
- Optimierung von Systemstrukturen sicherheitsgerichteter Systeme mittels Markov-Analysen, Erstellen von Markov-Modellen
- Unterstützung beim Aufbau von Qualitätsmanagementsystemen unter Berücksichtigung der IEC 61508
- Bestimmung von sicherheitsrelevanten Parametern im Rahmen der IEC 61508 und IEC 61511 wie PFDavg, HFT, CCF, SFF, λ_{su}, λ_{du}, λ_{dd}, λ_{sd}
- Evaluierung von Betriebssystemen und Prüfung von sicherheitsrelevanten Software-Applikationsbausteinen
- Nachweise der funktionalen Sicherheit gemäß IEC 61508 (DIN EN 61508, VDE 0803), IEC 61511, IEC 62061: Safety Integrity Level – SIL

- ISO 13849-1: Performance Level (EN 954-1)
- Zulassungsunterstützende Prüfung von Sicherheitsnachweisen und Funktionsnachweisen für Bahntechnik insbesondere gemäß EN 50126, EN 50128, EN 50129, EN 50155
- Andere sektorspezifische Standards wie z. B. IEC 61800-5-2, EN 60947-5-3

Ihr Ansprechpartner:
TÜV NORD CERT
Safety Related Services – SRS
Herr Dr. Ulrich Adolph
Langemarckstraße 20
45141 Essen

Telefon +49 (0) 2 01/8 25-24 60
Telefax +49 (0) 5 11/9 86 28 99 19 00
info.tncert@tuev-nord.de

Wir freuen uns auf den Dialog mit Ihnen!

Mehr Info?

☐ **Ja, ich interessiere mich näher für folgende Themen:**

- ☐ Grundlagen der funktionalen Sicherheit
- ☐ Schulung zur funktionalen Sicherheit
- ☐ Functional Safety Management
- ☐ Funktionale Sicherheit

☐ **Bitte nehmen Sie mit mir Kontakt auf.**

Absender (bitte in Blockschrift)

Unternehmen		PLZ/Ort	
Herr/Frau		Telefon	
Position		Telefax	
Straße		E-Mail	