ICS 13.110, 29.020, 35.240.50 November 2024

VEREIN DEUTSCHER INGENIEURE

Einführung in die Funktionale Sicherheit nach IEC 61508

VDI-EE 4020

Introduction to functional safety according to IEC 61508

VDI-EXPERTENEMPFEHLUNG

Frühere Ausgabe: 03.22

Inhalt Seite

Vorbemerkung 2
Einleitung 2
1 Anwendungsbereich 2
2 Normative Verweise 2
3 Begriffe 3
4 Formelzeichen und Abkürzungen 5
5 Grundlagen 6
6 Einordnung und Definition des Begriffs „Funktionale Sicherheit“ 7
6.1 Gesetzliche Anforderungen 7
6.2 Strategien zur Risikominderung 9
6.3 Funktionale Sicherheit als Teildisziplin der Sicherheitstechnik (Safety) 10
6.4 Beispiel für eine einfache Sicherheitsfunktion 14
7 Anwendungsgebiete der Funktionalen Sicherheit und Normenüberblick 18
8 Allgemeine Anforderungen an die Funktionale Sicherheit nach IEC 61508 19
9 Vorgehensweise zum Erreichen der Funktionalen Sicherheit 20
10 Anforderungen an die Hardware nach IEC 61508 – Details 23
11 Anforderungen an die Software nach IEC 61508 – Details 38
12 „Fallstricke“ und typische Fehler 41
13 Besonderheiten spezifischer Sektor-Anwendungsnormen 44
14 Zusammenfassung 48
Schrifttum 49

VDI-Gesellschaft Produkt- und Prozessgestaltung (GPP)
Fachbereich Sicherheit und Zuverlässigkeit

VDI-Handbuch Zuverlässigkeit

Vorbemerkung

Der Inhalt dieser Expertenempfehlung ist entstanden unter Beachtung der Vorgaben und Empfehlungen der Expertenempfehlung VDI-EE 1100.

Allen, die ehrenamtlich an der Erarbeitung dieser VDI-Expertenempfehlung mitgewirkt haben, sei gedankt.

Einleitung

Von technischen Einrichtungen und Anlagen gehen im Allgemeinen Gefährdungen für Mensch und Umwelt aus. Grundlegende Zielsetzung der Sicherheitstechnik ist es, die aus diesen Gefährdungen resultierenden Risiken so gering wie möglich zu halten, ohne jedoch die Funktion der technischen Einrichtung oder Anlage mehr als unbedingt notwendig einzuschränken.

Die Funktionale Sicherheit ist eine wichtige Teildisziplin der Sicherheitstechnik und gewinnt aufgrund der fortschreitenden Automatisierung in vielen technischen Bereichen zunehmend an Bedeutung. Diese Expertenempfehlung soll eine grundlegende Einführung zum Thema „Funktionale Sicherheit“ geben und die wichtigsten Begrifflichkeiten sowie Methoden und Strategien zum Erreichen der erforderlichen Funktionalen Sicherheit erläutern. Es werden kurz die wichtigsten sicherheitskritischen Anwendungsbereiche, die hierfür relevanten Normen der Funktionalen Sicherheit und die wesentlichen Unterschiede zwischen den Anwendungsbereichen vorgestellt.

Die Expertenempfehlung basiert im Wesentlichen auf den Anforderungen der Grundnorm zur Funktionalen Sicherheit – IEC 61508 – und soll den Einstieg in die Thematik vereinfachen. Allerdings erhebt die Expertenempfehlung hierbei nicht den Anspruch auf eine vollständige Abhandlung aller Detailanforderungen der Norm. Stattdessen soll ein einführendes Verständnis zu dem Thema „Funktionale Sicherheit“ vermittelt werden und es soll weiterhin ein Arbeiten mit der Grundnorm IEC 61508 und den für den jeweiligen Anwendungsbereich relevanten Sektor-Normen gefördert werden. Auf spezifische Besonderheiten der Sektor-Normen wird ebenfalls kurz eingegangen. Weiterhin wird auf die in der Praxis häufig vorkommenden Probleme und Missverständnisse im Zusammenhang mit der Funktionalen Sicherheit eingegangen.

Die Expertenempfehlung soll die existierende Lücke zwischen sehr kurzen und oberflächlichen Einführungen und sehr umfangreichen Veröffentlichungen zu dem Thema „Funktionale Sicherheit“ möglichst schließen. Nach dem Lesen dieser Einführung sollte es möglich sein, weiterführende Literatur wie [1; 2] zu studieren oder gezielt in den Normen der Funktionalen Sicherheit zu lesen und die Detailanforderungen zu verstehen.

1 Anwendungsbereich

Die Expertenempfehlung soll in einem überschaubaren Rahmen einen Einstieg in das Thema „Funktionale Sicherheit“ nach der Grundnorm IEC 61508 ermöglichen. Dazu werden grundlegende rechtliche Anforderungen (am Beispiel Maschinen) ebenso erläutert wie alle wichtigen normativen Begrifflichkeiten. Weiterhin wird die grundlegende Strategie zur Erfüllung der normativen Anforderungen an die Funktionale Sicherheit detailliert erklärt. Darüber hinaus wird auf häufige Missverständnisse bei Anwendung der Normen der Funktionalen Sicherheit sowie auf Besonderheiten von unterschiedlichen Sektor-Normen eingegangen. Einschränkend sei angemerkt, dass sich die in diesem Dokument vorgestellte Vorgehensweise zur Erfüllung der Hardware-Sicherheitsanforderungen an dem sogenannten Weg 1_H orientiert (erster Weg nach IEC 61508 zum Nachweis der Hardware-Sicherheitsintegrität). Auf eine Vorstellung des sogenannten Wegs 2_H (zweiter Weg nach IEC 61508 zum Nachweis der Hardware-Sicherheitsintegrität) wird verzichtet, da dies dem Rahmen eines Dokuments mit einführendem Charakter nicht gerecht werden würde. Die in der Prozessindustrie angewendete internationale Norm IEC 61511 orientiert sich jedoch stark an dem sogenannten Weg 2_H. In diesem Zusammenhang soll daher zusätzlich auf die Richtlinie VDI/VDE 2180 verwiesen werden, die umfassende Informationen zur Funktionalen Sicherheit auf Grundlage der Norm IEC 61511 beinhaltet und diese Expertenempfehlung damit fachlich sinnvoll ergänzt.