TÜV-Prüfung der Sicherheit und Fehlertoleranz elektronischer Steuerungen

TÜV Approval of Safety-aspects and Fault Tolerance of Electronic Systems

Ekkehard Pofahl

Sicherheitsgerichtete elektronische Steuerungen dringen in Bereiche vor, in denen bisher Vorbehalte gegen Elektronik und Software bestanden haben. In den letzten Jahren sind generische Standards entstanden, die Anforderungen für Elektrik, Elektronik und Software in der Sicherheitstechnik formulieren. Auf der anderen Seite sind im Rahmen der Öffnung der europäischen Märkte viele nationalstaatliche Überwachungsfunktionen früherer Zeiten, z. B. durch die Gewerbeaufsichtsämter entfallen, mit Hinblick auf eine erweiterte Haftung im Rahmen von Produkthaftungsgesetzen. Unabhängig von behördlichen Zwängen kann die Einhaltung von Standards und Richtlinien von den Technischen Überwachungsvereinen (TÜV) als unabhängiger Stelle im Rahmen einer „Third Party Inspection" erfolgen. Der Artikel gibt einen Überblick über die dabei angewendeten Methoden.

Safety related programmable electronic systems (PES) are used in areas, where traditionally no electronic and software was tolerated. Over the past years generic standards have been created, which identify requirements for electric, electronic and software used in safety technique. On the other hand the strict regulations of the past days, e. g. by governmental organizations, have been loosened because of European product liability laws. Independent of government enforcement the adherence to standards and guidelines can be assessed by the German Technical Supervisory Agencies (TÜV) by means of a „third party inspection". The article gives an overview about the methods used during such an inspection.

1 Einleitung

Die privatrechtlich organisierten Technischen Überwachungsvereine (TÜV) nehmen traditionell seit über 130 Jahren Industrieanlagen ab. Als neutrale unabhängige internationale Dienstleistungskonzerne dokumentieren sie mit interdisziplinärer Kompetenz die Sicherheit und Qualität von neuen und bestehenden Produkten, Systemen und Dienstleistungen. Die TÜV-Organisationen sind nur zu einem kleinen Teil noch staatsentlastend tätig, z. B. bei der Überwachung der Sicherheitseinrichtungen von Kernkraftwerken. Der weitaus größte Anteil der Tätigkeiten liegt jedoch im freiwirtschaftlichen Bereich. Ein Schwerpunkt der Tätigkeiten bildet die Erstabnahme und die wiederkehrende Prüfung von Industrie- und sonstigen technischen Anlagen (Aufzüge, Fahrtreppen). Während dieser Prüfungen wird die Einhaltung der gängigen technischen Sicherheitsstandards (Elektrik, Hydraulik, Klimatechnik etc.) überprüft. Die Arbeit der TÜV-Organisationen wird von der Überzeugung getragen, dass gesellschaftliche und industrielle Entwicklung ohne technischen Fortschritt nicht möglich ist.

Mit dem Eindringen programmierbarer Technik in sicherheitsrelevante Bereiche gehört zu einer technischen Begutachtung die Prüfung der gesamten Sicherheitskette bestehend aus Hardware- und Softwarekomponenten. Im Gegensatz zu traditionellen Sicherheitseinrichtungen bestimmt nun die Anwendersoftware einer sicherheitskritischen Anlage die Funktion. Die Begutachtung muss insbesondere die funktionsbestimmenden Programme für die eingesetzten speicherprogrammierbaren Steuerungen (SPS) beinhalten, zusätzlich zur traditionellen Überprüfung der korrekten Installation und Verkabelung (Kabelführung, Kabelquerschnitte, elektrische Sicherheit).

Für höhere Sicherheitskategorien müssen in der Regel sicherheitsgerichtete Steuerungen mit definiertem Ausfall- und Degradationsverhalten eingesetzt werden. Wie solche Steuerungen programmiert und parametriert werden müssen, damit sie ihre Sicherheitsfunktionen auch ausüben, ist in der Regel in einem für jede sicherheitsgerichtete Steuerung erhältlichen Sicherheitshandbuch („Safety Manual") beschrieben. Viele sicherheitsgerichtete Steuerungen sind, zusammen mit den Sicherheitshandbüchern,

im Rahmen einer Typprüfung auf die Einhaltung der erhöhten Anforderungen an generische Sicherheitsfunktionen getestet worden. Zu diesen sicherheitsgerichteten Eigenschaften gehören unter anderem die Fehlersicherheit der in den SPS verwendeten Komponenten, permanente Diagnose aller Bauteile und sonstige umfangreiche Selbsttests.

2 Normenentwicklung und Standardisierungsarbeit

Da die traditionellen Standards bis vor kurzem Elektronik und Software gar nicht oder nur allgemein behandelten („Es darf keine Gefahr davon ausgehen"), wurde Anfang der 80er Jahre eine Arbeitsgemeinschaft von TÜV Rheinland und TÜV Bayern eingesetzt, die ein erstes Klassifizierungsschema und Maßnahmen erarbeitete, wie Mikroelektronik sicher gemacht werden kann. Die Ergebnisse wurden 1984 im Handbuch „Mikrocomputer in der Sicherheitstechnik" publiziert [4]. Diese Grundsatzarbeiten flossen in den Standard DIN V VDE 0801 „Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben" [2] ein, um schließlich im internationalen Standard IEC 61508 „**Functional safety of electrical/electronic/ programmable electronic safety-related systems**" [1] zu enden, der in diesem Schwerpunktheft verschiedentlich zitiert wird. Der Standard IEC 61508 ist auch als europäischer Standard EN 61508 erschienen.

Aufbauend auf den Prinzipien der IEC 61508 befinden sich die Normen der Reihe IEC 61511 zur Funktionalen Sicherheit von Prozessleitsystemen in der Bearbeitung. Sie werden wahrscheinlich als EN 61511 bzw. DIN EN 61511 auch in das europäische und deutsche Normenwerk übernommen werden.

Sicherheitsstandards zu einer neuen Technik oder Technologie können erst dann formuliert werden, wenn sich diese Technik durchgesetzt hat. Daraus resultiert ein Zeitverzug, der Innovationen hemmen kann. Bei der Abfassung der Standards wurde daher weitestgehend darauf geachtet, neue Techniken nicht per se auszuschließen, und für bekannte Techniken (z. B. Elektrik und diskrete Elektronik) Regeln zu formulieren.

3 „X-by-wire"

Mechanische, hydraulische oder pneumatische Funktionen in technischen Geräten wie Flugzeugen und anderen Fahrzeugen weichen aus technischen und wirtschaftlichen Gründen zunehmend einer Steuerung durch Elektronik und Elektromechanik. Zuerst wurde die mit „Fly-by-wire" bezeichnete Technik zur sehr sicherheitskritischen Steuerung von Flugzeugen verwendet. Die hydraulische und mechanische Rudersteuerung wurde durch eine drahtgebundene elektrische/elektronische Steuerung ersetzt. Dies war gerechtfertigt, da die großen Verkehrsmaschinen bei Ausfall von Hilfsenergien allein mit Muskelkraft sowieso nicht mehr gesteuert werden konnten. Und die Verteilung von elektrischer Hilfsenergie ist im Notfall leichter zu koordinieren als Hilfssysteme für pneumatische oder hydraulische Systeme. Damit ist gegenüber der traditionellen Technik durch „Fly-by-wire" eine vergleichbare, wenn nicht bessere, Sicherheit für den Flugbetrieb gewährleistet.

Mittlerweile besteht der Drang, viele andere technische sicherheitskritische Steuerungen mit elektronischen Steuerungen auszurüsten. Ein modernes Kraftfahrzeug lässt sich z. B. nach Ausfall der Lenkunterstützung allein mit Muskelkraft im gesamten Geschwindigkeitsbereich nicht mehr sicher steuern. Hier besteht eine vergleichbare Situation wie bei den Flugzeugen vor Einführung der „Fly-by-wire" Techniken.

Wiewohl der Gesetzgeber in Deutschland zur Zeit noch eine mechanische Verbindung des Lenkrades mit dem Lenkgestänge fordert, wird es mit Sicherheit in naher Zukunft die ersten „Steer-by-wire" und „Break-by-wire" Systeme geben, die eine vergleichbare oder sogar eine höhere Sicherheit gewährleisten wie die traditionellen Systeme. Die Prototypen dieser Systeme können in kritischen Situationen den Fahrerwunsch heute schon wesentlich besser technisch umsetzen als traditionelle Systeme. Bevor diese Systeme jedoch in Serie eingesetzt werden, müssen umfangreiche Failure-Mode-Effect Analysen (FMEAs) und Praxis-Versuche die Alltagstauglichkeit nachweisen. Maßstab ist auch hier, dass die Sicherheit durch den Einsatz der neuen Technik erhöht werden muss.

Ohne Frage werden die „X-by-wire" Techniken zukünftig ihren Einsatz finden. Im Folgenden werden die Methoden beleuchtet werden, mit denen Standardsteuerungen klassifiziert und geprüft werden. Abgewandelt und an die neuen Randbedingungen (Echtzeitsteuerungen im Sub-Millisekundenbereich, kein sicherer Zustand) angepasst, lassen sich diese Methoden auch zur Validation und Verifikation der „X-by-Wire" Techniken einsetzen.

4 Fehlertoleranz und Degradationsverhalten

Kein technisches Gerät ist vor Defekten und Fehlern gefeit. Diese Defekte und Fehler können sowohl systematischer Art sein (Entwurfsfehler), als auch auf Ermüdungserscheinungen oder sonstige Alterungseffekte zurückgeführt werden. Die einfachste Forderung an sichere Geräte lautet mithin, dass Fehler und Ausfälle nicht zu gefährlichen Zuständen führen dürfen. Mittels technischer Maßnahmen wie Redundanz, Diversität, Überdimensionierung und nicht technischer Maßnahmen wie Prozeduren, Instruktionen, Verhaltensvorschriften und Arbeitsanweisungen erreicht man in der Praxis, dass Fehler in technischen Geräten vermieden oder beherrscht werden und sich dadurch nicht gefährlich auswirken können. Verdeckte Fehler oder passive Fehler, die sich erst im Anforderungsfall offenbaren, können in der Regel nur durch regelmäßige Prüfungen oder automatische Diagnoseroutinen beherrscht werden.

Mit den Mitteln der Software und der dazugehörenden Hardware lässt sich nun sowohl ein hoher Grad an Fehlerdiagnostik erreichen, als auch das Verhalten eines Gerätes im Fehlerfall vorherbestimmen. Dies ist eine neue Qualität von elektronischen Steuerungen, die bisher ohne Software gar nicht oder nur sehr schwer implementiert werden konnte. In einem dreifach redundanten System lässt sich zum Beispiel per Software festlegen, ob nach dem Ausfall von 2 Kanälen der Betrieb mit dem letzten Kanal weiter aufrecht erhalten werden soll (z. B. beim Landeanflug eines Flugzeuges) oder der sichere Zustand eingenommen werden soll (z. B. bei einer Brennersteuerung).

5 Typprüfung

Im Rahmen einer Typ-Prüfung wird die grundsätzliche Eignung einer sicherheitsgerichteten Steuerung für bestimmte Einsatzbereiche festgestellt. Dies entbindet die Sachverständigen bei der Anlagenabnahme davon, die internen Details der Steuerungen im Rahmen von Einzelabnahmen erneut zu überprüfen.

Eine Typ-Prüfung ist typischerweise in drei Phasen unterteilt: Konzeptprüfung, Hauptprüfung, Zertifizierung (vgl. Bild 1).

Während der Konzeptprüfung wird das Konzept einer technischen Einrichtung überprüft. Die sicherheitsrelevanten Teile des Gesamtkonzeptes sind sinnvollerweise in einem eigenen Sicherheitskonzept zusammengefasst (Terminus der IEC 61508: „Safety Requirement Specification“). Als Ergänzung der Spezifikation dient die Validierungsplanung (Terminus der IEC 61508 „Verification and Validation (V&V) Plan“). Den Abschluss einer Konzeptprüfung bildet ein Konzeptbericht, in dem bei positivem Ergebnis die prinzipielle Eignung der Steuerungskonzeption bestätigt wird. Dies wird dadurch erreicht, dass alle Forderungen zur Fehlervermeidung und Fehlerbeherrschung mit der notwendigen Wirksamkeit konzeptionell eingeplant sind.

Im Rahmen der Konzeptprüfung wird auch der Prüfplan für die Hauptprüfung aufgestellt. Die Hauptprüfung selbst verifiziert die richtige und vollständige Umsetzung des Konzeptes und besteht in der Regel aus Hardwareprüfung, Softwareprüfung und Integrationsprüfung. Hard- und Softwareprüfung unterteilen sich weiter in einen theoretischen und einen praktischen Teil. Im Rahmen der Hauptprüfung erfolgen sowohl die Überprüfung der Dokumentation als auch der Nachweis von sicherheitsrelevanten Eigenschaften durch Umweltprüfungen (elektrische und mechanische Beanspruchungen) und Fehler-Einbringungs-Tests (Fault-Insertion-Test).

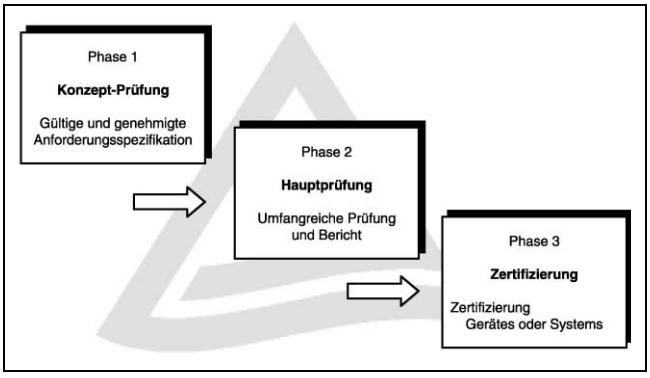

Bild 1: Phasen der Typprüfung.

Daneben muss auch der Lebenszyklus der Produktentwicklung betrachtet werden.

Nach erfolgreicher Hauptprüfung wird das Ergebnis der Prüfung auf einem Zertifikat festgehalten.

Während für die Hardware die Prüfungen relativ klar formuliert sind, z. B. in dem Standard IEC 61131-2 [6] für speicherprogrammierbare Steuerungen, gestaltet sich die Überprüfung der Softwarekomponenten elektronischer Steuerungen sehr viel komplizierter.

5.1 Software

Der hohe Verifikationsaufwand bei der Validierung und Verifizierung von Software hat die Betreiber der deutschen Kernkraftwerke seinerzeit noch davon abgehalten, programmierbare Elektronik bei der Überwachung der Sicherheitssysteme der Kernkraftwerke einzusetzen: die in den Sicherheitskreisen eingesetzte Elektronik ist diskret mehrkanalig aufgebaut und ohne Software implementiert.

Das Verhalten elektronischer Baugruppen wird heute durch Software bestimmt, während die Funktionsweise traditioneller Sicherheitstechnik durch Elektromechanik (Relais, Schütze) und durch diskrete Elektronik bestimmt war. Ein Einsatz von komplexer Elektronik ohne Software ist heute aber nicht mehr vorstellbar.

In der Sicherheitstechnik verwendete Software lässt sich in folgende Kategorien einteilen:

Software der Entwicklungsumgebung („Engineering Workstation“):

- Entwicklung des Anwenderprogramms
- Simulation des Anwenderprogramms
- Debugging des Anwenderprogramms
- Download und Verify der Anwenderprogramme

Software für die Funktion der Systeme:

- Real-Time-Betriebssysteme
- Firmware der Ein-/Ausgabe-Baugruppen
- VHDL-Code für die verwendeten FPGAs/EPLDs/ASICs
- Funktionsbibliotheken
- Anwendersoftware

Software, die für die Entwicklung und Herstellung der Steuerung selbst benötigt wird:

- Compiler, Assembler, Linker

- Programmiereinrichtungen
- Simulations- und Testsysteme

Damit beim Einsatz von hoch integrierten Bauteilen und der sie steuernden Software das Risiko, das von einem Prozess bzw. einer Anlage ausgeht, innerhalb tolerierbarer Grenzen bleibt, müssen ausreichende Maßnahmen zur **Fehlervermeidung, Fehlererkennung** und **-beherrschung** ergriffen werden. Die Wirksamkeit dieser Maßnahmen nachgewiesen werden.

In den Sicherheitsnormen werden für die Erstellung von Software Empfehlungen gegeben, mit denen die Erstellung fehlerarmer Software gefördert wird. Mit diesen Maßnahmen sollen Fehler vermieden, begangene Fehler erkannt und beherrscht werden.

Während einer Typ-Prüfung wird jede der oben gelisteten Softwarekomponenten individuell mit geeigneten Methoden auf Eignung hin überprüft.

Als Beispiel, dass vorhandene Normen die Technik nicht unbedingt prägen, sei der weite Einsatz der Programmiersprache „C“ genannt. Alle Fachleute raten dringend davon ab, „C“ für die Erstellung von sicherheitsrelevanter Software zu verwenden (Tabelle C.1, Teil 7 der IEC 61508 [1], NASA Software Safety Standard [5], u. v. a. m.). Trotzdem werden die Betriebssysteme sehr vieler sicherheitsgerichteter Systeme in der Programmiersprache „C“ oder „C++“ entwickelt. Um den Sicherheitsnachweis trotz dieser fehlerträchtigen Sprache sicherzustellen, sind dann im Einzelfall zusätzliche Verfahren nötig, um auch mit der Programmiersprache „C“ die nötige Sicherheit zu erreichen.

5.2 Software – Änderungsmanagement

Software und Software-Werkzeuge sind nicht stetig. In der Regel kann die Auswirkung von „kleinen“ Änderungen nicht ohne weiteres überblickt werden. Deswegen muss für sicherheitsrelevante Software ein sorgfältiges Änderungsmanagement eingerichtet werden. Entsprechende Prozeduren müssen sowohl für die Änderungen der Betriebs-/ und Entwicklungssoftware, als auch für die Änderungen der Anwendersoftware aufgestellt werden.

Auf der Seite der Betriebssystem-Software kann z. B. mit dem maschinellen Vergleich der Binärcodes nachgewiesen werden, dass singuläre Änderungen im Quellcode auch nur singuläre Änderungen der ausführbaren Programme bewirken. Ein Binärvergleich ist nur bei geringfügigen Änderungen möglich. Die Auswirkung größerer Änderungen muss durch erneute Prüfung untersucht werden.

Für die Änderung von Anwenderprogrammen nach einer Abnahme muss ein Änderungsmanagement-Verfahren aufgesetzt werden. Jede Änderung muss zunächst spezifiziert und sodann formal abgenommen werden. Vor der Implementierung sollte eine Simulation erfolgen, bevor die geänderte Software in die Anlage überspielt wird. Einige Entwicklungsumgebungen stellen hier Hilfsmittel bereit.

6 TÜV-Kooperation „Funktionale Sicherheit”

Nachdem Mitte der achtziger Jahre die ersten sicherheitsrelevanten Steuerungen von den technischen Überwachungsvereinen erfolgreich einer Typ-Prüfung unterzogen worden waren, tauchte bei vielen Anwendern solcher Steuerungen der Wunsch auf, die Methoden, die bei der Prüfung verwendet werden, kennenzulernen. Diesem Wunsch folgend, und um sicherzustellen, dass die unterschiedlichen TÜV-Organisationen nach gleichen Grundsätzen prüfen, wurde mit der Gründung der TÜV-Kooperation zwischen TÜV Rheinland und TÜV Bayern (heute TÜV Süddeutschland) ein regelmäßiger Erfahrungsaustausch innerhalb der TÜV-Organisationen vereinbart. Diese Arbeitsgemeinschaft stellt durch regelmäßige Treffen die Anwendung der gleichen Methodik bei der Typ-Prüfung sicher und publiziert darüber hinaus eine gemeinsame Liste der von den TÜV-Organisationen typgeprüften sicherheitsrelevanten Steuerungen [3]. Die Arbeitsgemeinschaft heißt heute „TÜV Cooperation Functional Safety“ und ist im Internet unter www.tuv-fs.com zu finden [3].

Nachdem seit 1984 mehrere verschiedene Klassifizierungsschemata eingeführt wurden, gewinnt die Klassifizierung in Safety Integrity Levels (SIL) nach IEC 61508 mehr und mehr an Bedeutung. Für eine Übergangszeit werden in den Zertifikaten vergleichbare Klassifizierungen noch parallel aufgeführt, um eine Vergleichbarkeit der Steuerungen, z. B. auch bei lang laufenden Ausschreibungsverfahren, zu gewährleisten. Zur Zeit sieht es so aus, als würde sich die Klassifizierung in Safety Integrity Levels (SIL) nach IEC 61508 durchsetzen.

Auf der Homepage der „TÜV Cooperation Functional Safety“ sind die generellen Grundsätze und Standards, nach denen qualifiziert wird, gelistet und erläutert.

Liste der typgeprüften Steuerungen

Sofern die Hersteller dies wünschen, werden die Resultate der Typprüfung auf der Homepage der „TÜV Cooperation Functional Safety“ gelistet [3]. Dies bietet Anwendern von Steuerungen einen ersten Überblick über die verschiedenen Implementierungen sicherer Steuerungen.

7 Sicherstellung korrekter Installation

Leider lässt es sich nicht immer ausschließen, dass bei der Installation einer an sich fehlersicheren Sicherheitssteuerung Fehler gemacht werden, die dazu führen, dass ein sicherer Betrieb nicht gewährleistet ist.

Deswegen werden Regeln und Auflagen formuliert, die einen bestimmungsgemäßen Einsatz der sicherheitsrelevanten Steuerungen sicherstellen sollen. Ferner können Auflagen dergestalt formuliert werden, dass für bestimmte Anwendungen nur ganz bestimmte Hard- und Softwarekomponenten zum Einsatz kommen dürfen. Diese Auflagen

standen traditionell in den Prüfberichten der Prüfinstitute unter dem Kapitel ,,Auflagen".

Es stellte sich heraus, dass beim Einsatz der Steuerungen, die ,,normal" und sicherheitsgerichtet verwendet werden können, diese Randbedingungen den Projektierungsfirmen und den Endanwendern häufig nicht bekannt waren. Meist waren einfache logistische Gründe dafür ausschlaggebend, dass die Information nicht geeignet weitergeleitet wurde. Häufig wurde die Nichteinhaltung der Auflagen erst bei der Abnahme erkannt; die nachträgliche Implementierung der Sicherheitsrichtlinien war dann oft sehr kostenträchtig.

Unter anderem aus diesem Grunde haben die Hersteller von sicherheitsgerichteten Steuerungen alle Aspekte für den Einsatz Ihrer Produkte (Installation, Betrieb, Wartung) in sicherheitsrelevanten Bereichen heute in Sicherheitshandbüchern zusammengestellt, die mit dem Produkt ausgeliefert werden. Während der Typ-Prüfung werden diese Handbücher mit überprüft und ersetzen die sonst üblichen Auflagen. In den Zertifikaten wird sodann auf diese Sicherheitshandbücher verwiesen.

8 Zusammenfassung

Mit den Fortschritten der Technik muss auch die Prüfung dieser Techniken weiterentwickelt werden. Insbesondere die sich abzeichnenden ,,X-by-Wire" Techniken verlangen eine sehr sorgfältige Prüfung, bevor sie auf breiter Front, zum Beispiel in Kraftfahrzeugen, eingesetzt werden.

Die technischen Überwachungsvereine stehen als neutrale Diskussionsforen auch zwischen konkurrierenden Herstellern von sicherer Elektronik bereit, um sicherzustellen, dass durch den Einsatz von Elektronik und Software die Anwendung der Technik sicherer wird.

In der Praxis muss ein Kompromiss zwischen dem Einsatz betriebsbewährter Technik und der Verwendung von neuen Technologien gefunden werden.

Auch wenn sich bei dem Einsatz von Software durch fehlerhafte Entwicklungsumgebungen, Compilerfehler, allgemeine Softwarefehler und Spezifikationsfehler Probleme ergeben, ist eine sichere Elektronik ohne Software heute nicht mehr vorstellbar.

Wenn im Jahr 2004 die deutsche Norm VDE 0801 endgültig zurückgezogen wird, steht die internationale Norm IEC 61508 bereit, die Rolle als Standard für die Entwicklung von elektronischen Steuerungen mit funktionaler Sicherheit zu übernehmen.

Literatur

[1] IEC 61508 ,,Functional safety of electrical/electronic/ programmable" electronic safety-related systems
http://www.iec.ch/

[2] DIN V VDE 0801 (VDE 0801):1990-01 und DIN V VDE 0801/A1 (VDE 0801/A1):1994-10 ,,Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben"
Die DIN V VDE 0801 wird im August 2004 zurückgezogen, siehe
http://www.dke.de/de/facharbeit/mitteilungen/EN61508.htm

[3] ,,TÜV Cooperation Functional Safety" mit Liste typgeprüfter Steuerungen, http://www.tuv-fs.com

[4] Handbuch ,,Mikrocomputer in der Sicherheitstechnik", Hölscher/Rader, 1984, Verlag TÜV Bayern/Rheinland

[5] NASA-STD-8719.13A (1996), ,,NASA Software Safety Standard" http://www.hq.nasa.gov/office/codeq/doctree/871913.htm

[6] DIN EN 61131 Speicherprogrammierbare Steuerungen.

Manuskripteingang: 10. Juni 2002.

Dipl.-Phys. Ekkehard Pofahl ist beim TÜV Rheinland/Berlin-Brandenburg im Geschäftsfeld ASI (Automation, Software, Informationstechnologie, http://tuvasi.com) verantwortlich für das Competence Center Software Engineering. Die Interessen- und Arbeitsgebiete umfassen alle Aspekte moderner Softwareerstellung, von der Entwicklung von Programmierrichtlinien bis zum Begutachtung von Compilern und der Prüfung von grafischen Programmgeneratoren im Rahmen von System- und Baumusterprüfungen von sicherheitsrelevanten elektrischen und elektronischen Anlagen und Geräten.

Adresse: TÜV Anlagentechnik GmbH, Geschäftsfeld ASI, Am Grauen Stein, D-51105 Köln, Tel.: 0221-806-2981, E-Mail: ekkehard@pofahl.de