IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

0050

Aus der Arbeit des IFA

Ausgabe 1/2015 617.0-IFA:638.22

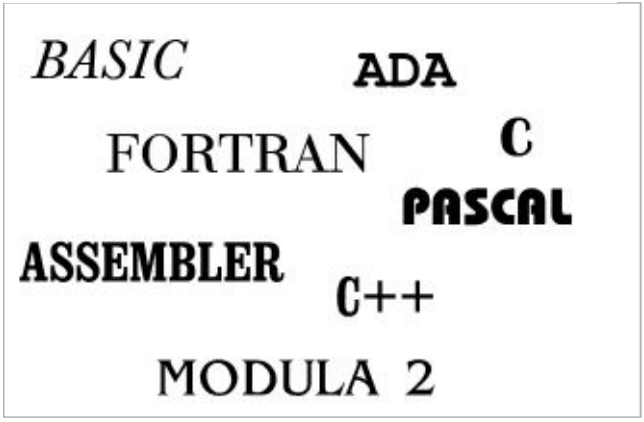
Programmiersprachen mit eingeschränktem Sprachumfang für Sicherheitsanwendungen

Problem

Aus ökonomischen, ergonomischen und/oder sicherheitstechnischen Gründen werden immer mehr Maschinen mit Rechnersystemen ausgestattet, in denen die programmierbaren Systeme auch Sicherheitsfunktionen übernehmen. Beispiele sind Werkzeugmaschinen, Drehautomaten und Roboter. Wer solche Systeme mit sicherheitsrelevanter Software entwickelt und programmiert, trägt eine besondere Verantwortung. Ähnlich wie bei der Verdrahtung einer Maschine, müssen Regeln erstellt werden, die helfen, Fehler bei der Programmierung zu vermeiden.

Derzeit gibt es eine ganze Reihe von Programmiersprachen, die von verschiedenen Herstellerfirmen für die Programmierung in der Sicherheitstechnik eingesetzt werden. Den Sachkundigen, die sich jahrelang mit diesen Sprachen befasst haben, ist klar, dass jede Programmiersprache Befehle und Konstrukte haben kann, die zu schwerwiegendem Fehlverhalten von Maschinen oder Sicherheitseinrichtungen führen können. Diese Konstrukte und Befehle sollten verhindert bzw. deren Verwendung eingeschränkt oder durch zusätzliche Maßnahmen abgesichert werden. Der Sprachumfang ist daher so weit einzuschränken, dass die Wahrscheinlichkeit von Fehlern bei der Programmierung deutlich verringert wird.

Umfassende und sprachbezogene Programmierleitfäden, die sich für Maschinensteuerungen eignen, sind derzeit nicht bekannt.



Die Praxis hat gezeigt, dass auch die, die Erfahrung in der Erstellung von Software haben, gelegentlich Hilfestellungen bei der Programmierung sicherheitsrelevanter Software benötigen und auch gerne annehmen.

Aktivitäten

Im Auftrag der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA) wurden die Programmiersprachen BASIC, PASCAL, MODULA 2, ADA, C, C++, FORTRAN und ASSEMBLER auf ihren Sprachumfang untersucht und dieser entsprechend den Erfahrungen aus der Softwareprüfung und den Ergebnissen aus Literaturstudien eingeschränkt.

Neben einem theoretischen Teil, der sich mit dem Aufbau von Programmen beschäftigt, wurden allgemeine und sprachbezogene Regeln in Form eines Nachschlagewerkes aufgestellt.

Ergebnisse und Verwendung

Die Untersuchungen zeigen, dass eine Vielzahl von Programmiersprachen für die Sicherheitstechnik einsetzbar ist, wenn die Schwächen der Sprachen entsprechende Beachtung bei der Programmierung finden. In einem allgemeinen Teil wird aufgezeigt, dass besondere Techniken zur transparenten Programmierung einen großen Anteil an der Fehlervermeidung bei der Programmierung haben (strukturierte und modulare Programmierung).

Nutzerkreis

Firmen, die Steuerungen und Maschinen herstellen, Prüfstellen

Weiterführende Informationen

- Schaefer, M. et. al.: Programmierregeln für die Erstellung von Software für Steuerungen mit Sicherheitsaufgaben. Fb 812. Schriftenreihe der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA), Dortmund. Wirtschaftsverlag NW, Bremerhaven 1998

- Reinert, D.; Schaefer, M.; Bömer, T.: Regeln für den Entwurf und die Programmierung sicherheitsbezogener Software. atp-Automatisierungstechnische Praxis 41 (1999) Nr. 6, S. 21-30

Fachliche Anfragen

IFA, Fachbereich 5: Unfallverhütung – Produktsicherheit

Literaturanfragen

IFA, Zentralbereich

Herausgeber und Druck:
Deutsche Gesetzliche Unfallversicherung e. V.
(DGUV), Glinkastraße 40, 10117 Berlin

ISSN (Internet): 2190-006X
ISSN (Druckversion): 2190-0051

Bearbeitet von: Dipl.-Ing. Günter Reuß
Institut für Arbeitsschutz der Deutschen
Gesetzlichen Unfallversicherung (IFA)
Alte Heerstraße 111, 53757 Sankt Augustin
Tel. 02241 231-02/Fax: -2234
E-Mail: ifa@dguv.de, Internet: www.dguv.de/ifa