IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

0050

Focus on IFA's work

Edition 1/2015 617.0-IFA:638.22

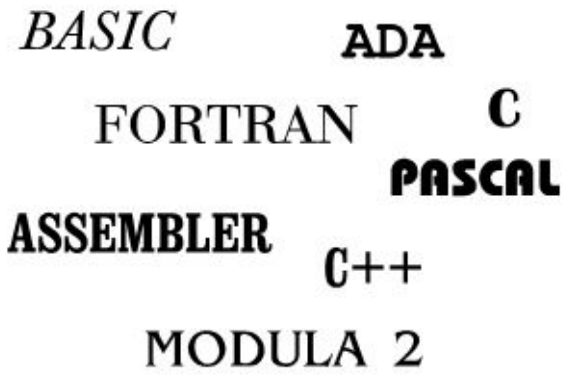
Programming languages with limited capabilities useful for safety applications

Problem

Whether for reasons of economy, ergonomics or safety, today more and more machines are equipped with computer systems in which the programmable components also handle safety functions. Examples of these include tool machines, autolathes and robots. Such systems with safety-relevant software place great responsibilities on developers and programmers. Rules need to be drafted to help avoid errors in programming, much as is currently the case in the process of wiring a machine.

There are presently a wide range of programming languages used by manufacturers to programme safety technologies and equipment. Experts who have worked with these languages for many years know that every programming language can have commands and structures that can cause serious defects in how machinery or safety equipment functions. These commands and structures need to be prevented, and their use needs to be limited or protected against with additional measures. The range of such languages should thus be restricted so as to reduce the chance of programming errors substantially.

Comprehensive and language-specific programming guides aimed at machine controls are as yet unavailable. Current practice shows that even experienced software makers occasionally require and are grateful for assistance with the programming of safety-related software.



Activities

On behalf of the Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA – Federal Institute for Occupational Safety and Health), the programming languages BASIC, PASCAL, MODULA 2, ADA, C, C++, FORTRAN and ASSEMBLER were examined to determine the range of each language, and the findings were then narrowed down to correspond to the experiences of software testers and the results of literature studies.

Aside from the theoretical section dealing with the structure of programmes, a list of general and language-specific rules was produced in the form of a reference work.

Results and Application

The studies showed that a number of programming languages can be used for safety technologies if enough attention is paid to the shortcomings of each language when writing the programmes. A general section demonstrates that special techniques for transparent programming can have a great impact on avoiding errors when developing programmes (structured and modular programming).

Area of Application

Control manufacturers, machine manufacturers, testing bodies

Additional Information

- 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

Expert Assistance

IFA, Division 5: Accident prevention – Product safety

Literature Requests

IFA, Central Division

Published and printed by:
Deutsche Gesetzliche Unfallversicherung e. V.
(DGUV), Glinkastrasse 40, 10117 Berlin

ISSN (online): 2190-006X
ISSN (print): 2190-0051

Edited by: Günter Reuß
Institut fuer Arbeitsschutz der Deutschen
Gesetzlichen Unfallversicherung (IFA)
Alte Heerstrasse 111, 53757 Sankt Augustin, Germany
Phone: +49 2241 231-02/Fax: -2234
E-mail: ifa@dguv.de, Internet: www.dguv.de/ifa