IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

0258

Focus on IFA's work

Edition 1/2015 617.0-IFA:638.22

Programming systems for safety controls

Problem

A "crash" on a PC and of the program in use might reasonably be regarded as a mere annoyance. Errors in the programming of safety controls, however, can have dramatic repercussions for occupational safety on machinery and plant. The reason: safety controls execute the application program code at runtime regardless of whether or not it contains errors. The scope for individual types of error in the programming of safety functions or device parameters on the PC, in the programming software or for that matter at input is much more subtile than a "crash".

Since troubleshooting during implementation or commissioning is likely to be beyond the programmer's ability, the "engineering tool" (PC-based software for application programming) itself should provide the best possible support for the detection of errors and low-error editing of the application.

Activities

The IFA is involved in the process of developing international provisions governing safety-related controls. For example, the IEC 62061 and ISO 13849 standards now have dedicated requirements concerning the development of safety-related application software for machine controls. The IFA also conducts consultation on a case-by-case basis and testing in the course of development in order for relevant standards to be satisfied on specific products.

Application programming of a safety control system for machinery and plant

All individual activities have the objective of developing a custom package of qualified error detection and error avoidance measures for the entire program implementation process (including plant configuration, program and parameter editing, declaration of variables, program compilation, program and parameter download, and application software verification.

Results and Application

Intuitive use, restriction to manageable functionality, user prompts and aids to input, tools for program verification, and a comprehensive, automatic error detection routine within the programming process will continue to be merely supportive functions for the individuals responsible for engineering and programming.

They can however support them in their responsibility to implement software in consideration for safety. The initial feedback from the field regarding programming systems tested by the IFA suggests that the acceptance amongst users is high.

Since the trend in safety technology towards user-configurable or user-programmable components continues to grow, the findings and results can also be incorporated into future product tests in which software is employed for man-machine interaction.

Area of Application

Manufacturers of safety controls and components; companies and individuals tasked with designing and engineering machinery and plant; persons programming safety-related application software

Additional Information

- Borowski, T.: Applikationssoftware für sichere (Safety-)Maschinensteuerungen erstellen. Fachmesse und Kongress SPS/IPC DRIVES Elektrische Automatisierung – Systeme und Komponenten, 27.-29. November 2007, Nürnberg – Vortrag. Tagungsband, S. 233-241. VDE-Verlag, Berlin 2007

- DIN EN 61131-6: Speicherprogrammierbare Steuerungen – Teil 6: Funktionale Sicherheit (10.13). Beuth, Berlin 2013

- www.plcopen.org/pages/tc5_safety

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: Torsten Borowski
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