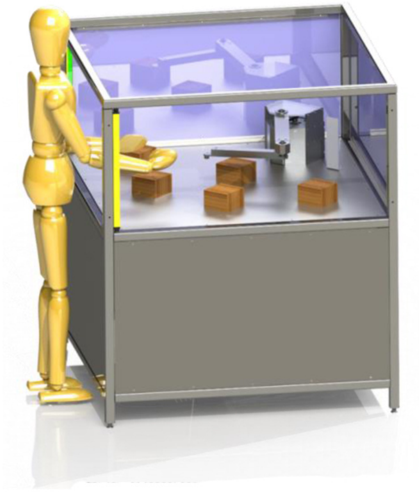
Hes·so
Haute Ecole Spécialisée
de Suisse occidentale
Fachhochschule Westschweiz
University of Applied Sciences
Western Switzerland



INTEGRATED SAFETY

Software Environment for Safety Functions of innovative, low-series machines

Project Summary

Lots of so-called Safety PLCs are available for performing “Boolean” safety functions on machines. The certification of conformity to the EU Directive on Machinery is relatively simple to achieve when they are used.

Innovative machines such as collaborative robots with non-Cartesian kinematics require more sophisticated software functions that are not available in up-to-date safety components. The most important one is the ability to manage and compute also with numerical values in a safe way.

The standard series IEC 61508 defines all requirements that have to be met for certifying such safety software functions. The corresponding workload is acceptable for machines that are produced in high volume. But this investment in human resources and external expertise is no more affordable when machines are produced in low volume or individually customized. This is the situation of many innovative machine manufacturers.

The goal of this project is showing if and how the simpler requirements of ISO 13849 can be met for assessing safety up to Performance Level PL d. This standard opens the possibility of using two software-based systems in parallel that are “diverse” enough, e.g. a standard PLC and a PC-based PLC, provided that they cross-check each other.

We considered during this project all safety functions that most drive manufacturers offer, and the difficulty to interface them with other devices via fieldbuses when they come from different providers. We also considered the tendency within standardization committees to strengthen ISO 13849 requirements for software certification.

Our conclusion is that the best solution to help SME in designing sophisticated, numerical safety functions within their control software is realizing some kind of a “Safety NC” that is able to perform safe calculation of numerical values instead of Boolean values only. We found a potential solution by combining existing products, among them the real-time OS PikeOS from SYSGO that is certified up to SIL 4 for avionics and train applications, together with the machine design environment ConceptRT from OBJECTIS SA.

In addition an existing, ConceptRT-based demonstrator has been modified: A light curtain and EtherCAT-based binary safety devices have been added for reducing motion speed in case of human intrusion. By doing this improvement, we acquired experience in using safety components.

Valorisation

The demonstrator has been exhibited at the SINDEX 2014 fair in Bern, Switzerland.

In addition, the suppliers mentioned above have been contacted for possibly launching a new project, the goal of which would be developing this “Safety NC”.

Contact / Mr Bernard Schneider (bernard.schneider@heig-vd.ch)
Author / Mr Bernard Schneider

This project has been carried out by Bernard Scheider in collaboration with Wolfram Luithardt, Nicolas Broch, Olivier Nasrallah, Julien Despond, Vincent Gonet and Thomas Gabella

ISYS

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

Institut d'
Automatisation
Industrielle