Experience with Static PLC Code Analysis at CERN

Authors
Tsiplaki, C., Fernandez, B., Blanco, E.

Oral or poster
Poster

Jacow Reference
THPHA160

Track
Software Technology Evolution

Status
APPROVED

Abstract

The large number of industrial control systems based on PLCs (Programmable Logic Controllers) available at CERN implies a huge number of programs and lines of code. The software quality assurance becomes a key point to ensure the reliability of the control systems.

Static code analysis is a relatively easy-to-use, simple way to find potential faults or error-prone parts in the source code. While static code analysis is widely used for general purpose programming languages (e.g. Java, C), this is not the case for PLC programs. We have analysed the possibilities and the gains to be expected from applying static analysis to the PLC code used at CERN, based on the UNICOS framework. This paper reports on our experience with the method and the available tools and sketches an outline for future work to make this analysis method practically applicable.

Paper

PLC_SA_ICALEPCS_2017.pdf