Master's Thesis

Analysis of PLC Programs Using the Program Analysis Framework SOOT

Student: *Andreas Grimmer*

Student No.: 1155123

Institute for System Software
Dr. Herbert Prähofer

Tel.: +43 732 2468-4352
Fax: +43 732 2468-4345
herbert.praehofer@jku.at

Linz, 24.11.2014

In the last decades, software became more and more important, especially in the industrial automation domain. The main reason for this shift is the requirement for more flexibility of the systems and therefore requires to move from hard-wired to programmable controllers. However, a more flexible system is also more complex and therefore ensuring the correctness of the system is not a trivial task. One common way to improve the quality of software systems is to use static program analysis to find defects in the source code. Static program analysis approximates the possible behavior of software systems and can therefore find erroneous program states.

Implementing program analysis techniques is not easy and for this reason, analysis frameworks like Soot (http://sable.github.io/soot/) have been introduced to ease implementation by avoiding redundancies. Although such analysis frameworks are intended to be language independent, they have to make some assumptions about the language's semantics, e.g., object orientation. Hence, using an analysis framework for programming languages that do not exactly match the assumed semantics of the framework requires transforming the source language in a way to correctly reflect the semantics.

In this thesis, the goal is to build a compiler that transforms PLC programs into a suitable input for the analysis framework Soot. The source language, a dialect of the IEC 61131-3 standard called *KemroIEC*, must therefore be compiled to Jimple code. Jimple is the intermediate representation used by Soot for analyzing programs and the semantics of Jimple are very similar to the semantics of the Java. The particular challenge of this thesis is to correctly reflect the value and reference semantics of the source language KemroIEC in the target language Jimple to be able to use the existing data flow, call graph and pointer analyses provided by Soot. Moreover, in order to further enable reuse of the compiler, a standardized AST model called OMG ASTM is used.

Betreuung

Dr. Herbert Prähofer, DI Florian Angerer