Statische Analyse von SPS-Programmen nach IEC 61131

Diplomarbeit für: Florian Angerer
Matr.Nr.: 0657360

Aufgabenstellung

Unter statischer Programmanalyse versteht man die Analyse eines Programms rein auf Basis des Source-Codes und ohne das Programm auszuführen. Mit statischer Programmanalyse kann man Qualitätsaussagen über ein Programm in der Form von Komplexitätszahlen, Verletzungen von Programmierrichtlinien, potentielle Schwachstellen, bis hin zu richtigen Programmfehlern erhalten. Methoden die eingesetzt werden sind eine regelbasierte Auswertung der Programmstruktur, Methoden der Kontrollflussanalyse und Methoden zur Datenflussanalyse von Programmen.

Für die klassischen Programmiersprachen wie C, C++, Java, oder C# sind Werkzeuge zur statischen Programmanalyse seit langem etabliert. Beispiele sind Lint für C mit dem z.B. nicht-initialisierte Variablen erkannt werden, PMD für Java, welche die Einhaltung eines Satzes von vordefinierten oder Benutzerdefinierten Regeln prüft, oder FindBugs, welches primär auf das Ausspüren von NullPointerExceptions in Java-Code abzielt.

In der Welt der SPS-Programmierung werden hauptsächlich Sprachen nach der IEC-61131-3 Norm eingesetzt. Für diese Sprachen sind bisher statische Programmanalysewerkzeuge nicht verfügbar. Die Aufgabestellung dieser Diplomarbeit ist daher für diese Sprachen Methoden zur statische Programmanalyse zu entwickeln und diese in einem Werkzeug zu implementieren. Dabei sollen die vom Auftraggeber eingesetzten Sprachen Structured Text (ST) und Sequential Function Charts (SFC) des Sprachdialekts Kemro IEC 616131 der Firma Keba AG behandelt werden.

Die Aufgabestellung umfasst im Einzelnen:

- Entwicklung einer Coco/R Grammatik für Sprachen nach der IEC-61131-3 Norm, aus dem ein Parser für SPS-Programme erzeugt werden kann.
- Entwicklung eines objektorientierten Klassensystems in Java zur Darstellung von SPS-Programmen in der Form eines Abstrakten Syntaxbaums (AST)
- Attributierung der Coco/R Grammatik zum Aufbau des AST.
- Entwurf eines Konzepts zur Implementierung von Analyseregeln zur statischen Analyse von SPS-Programmen (AST-Analyse).
- Umsetzung des Konzeptes in Java.
- Test des Systems an realistischen SPS-Projekten des Auftraggebers.

Auftraggeber

Die Arbeit wird im Rahmen einer Forschungskooperation mit dem Software Competence Center Hagenberg GmbH durchgeführt und von der Firma ENGEL Austria GmbH als Auftraggeber finanziert sowie im Rahmen des K2 Programms von der FFG gefördert.

Beginn: April 2011

Betreuung durch:

Dr. Herbert Prähofer