Метод дедуктивной верификации управляющих программ на процесс-ориентированном языке Reflex

Method of deductive verification of control programs in the process-oriented Reflex language

Авторы: Ануреев И.С., Гаранина Н.О., Лях Т.В., Розов А.С., Зюбин В.Е.

Authors: Anureev I.S., Garanina N.O., Liakh T.V., Rozov A.S., Zyubin V.E.

Предложен метод дедуктивной верификации аннотированных Reflex-программ [1, 2] (рис. 1.7), который включает четыре шага: аннотирование исходной Reflex-программы через задание условий запуска, ограничений на окружение и инвариантов цикла управления; трансляцию аннотированной Reflex-программы в аннотированную Си-программу; генерацию условий корректности для результирующей Си-программы; доказательство порожденных условий корректности. В качестве формального обоснования метода разработаны: операционная семантика аннотированных Reflex-программ [3, 4]; трансформационная семантика Reflex-программ в язык Си [5]; аксиоматическая семантика полученных в результате трансляции аннотированных Си-программ. Метод апробирован на тестовой управляющей программе с использованием SMT-решателя Z3. Предложенный метод является первым методом формальной верификации процесс-ориентированных программ и направлен на контроль качества программного обеспечения для программируемых логических контроллеров.

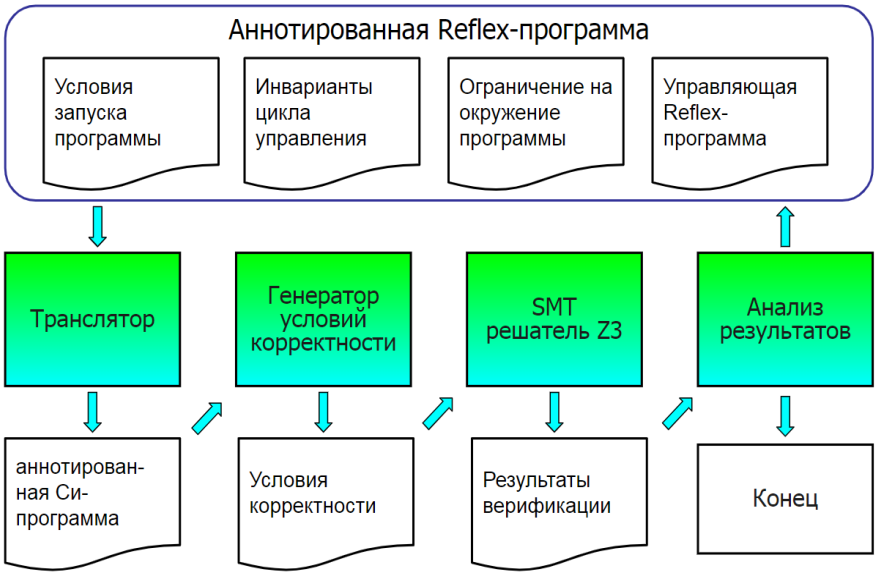

Рис. 1.7. Схема дедуктивной верификации Reflex-программ

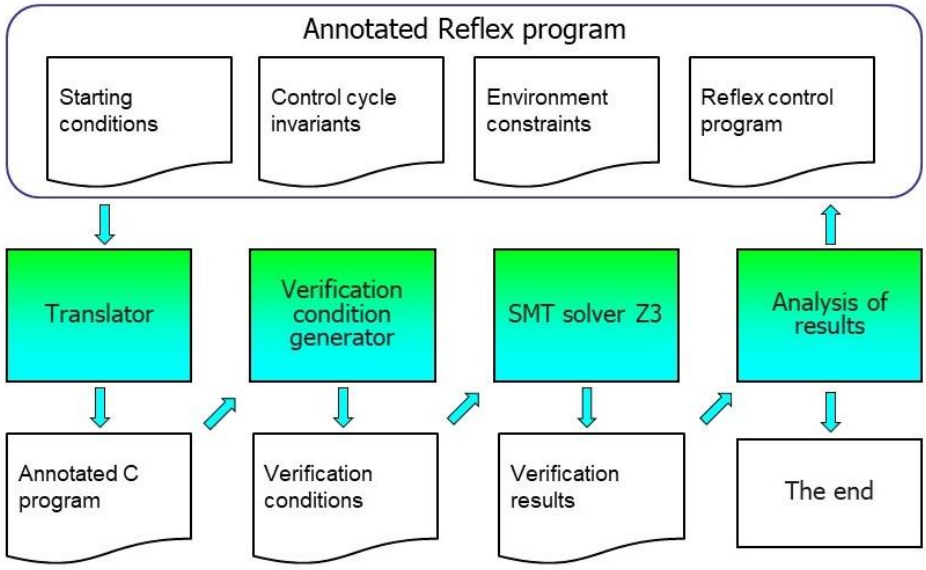

Fig. 1.7. Method of deductive verification of control programs in the process-oriented Reflex language

A method of deductive verification of annotated Reflex-programs (Fig.1.7) is proposed [1, 2], which consists of four steps: annotating the source Reflex-program by setting starting conditions, environment constraints, and control cycle invariants; translation of the annotated Reflex-program into an annotated C program; generation of verification conditions for the resulting C program, and proving the generated verification conditions. As a formal foundation of the method, we developed an operational semantics of annotated Reflex programs [3, 4]; a transformational semantics of Reflex-programs into the C language [5], and an axiomatic semantics of the resulting annotated C programs. The method was tested on a control program using the Z3 SMT solver. The proposed method is the first method for formal verification of process-oriented programs. It is used for quality control of software for programmable logic controllers.

Публикации/References:

1. Anureev I., Garanina N., Liakh T., Rozov A., Zyubin V., Gorlatch S. Two-Step Deductive Verification of Control Software Using Reflex // Lecture Notes in Computer Science. – 2019. – Vol 11964. – P. 50–63. – DOI 0.1007/978-3-030-37487-7_5.
2. Ануреев И.С., Гаранина Н.О., Лях Т.В., Розов А.С., Зюбин В.Е., Горлач С.П. Дедуктивная верификация Reflex-программ // Программирование. – 2020. – № 4. – С. 14–26. – DOI 10.31857/S0132347420040020.
3. Anureev I.S. Operational semantics of Reflex // System Informatics. – 2019. – № 14. – P. 1–10. – DOI 10.31144/si.2307-6410.2019.n14.p1-10.
4. Ануреев И.С. Операционная семантика аннотированных Reflex программ // Моделирование и анализ информационных систем. – 2019. – Т. 26, № 4. – С. 475–487.
5. Anureev I., Garanina N., Liakh T., Rozov A., Zyubin V. Towards safe cyber-physical systems: the Reflex language and its transformational semantics // IEEE International Siberian Conference on Control and Communications (SIBCON–2019) (Tomsk, Russia, April 18–20, 2019). − DOI 10.1109/SIBCON.2019.8729633.