

発表概要

アシュアランス駆動プログラミングに向けて

石井 正樹^{1,a)} 井出 真広¹ 倉光 君郎^{1,2}

2013年6月4日発表

アシュアランスケースは、システムのディペンダビリティ要求を議論し、その確信や合意を得る手段として安全工学分野から利用が広がっている。本研究では、アシュアランスケースの記法の1つである GSN (Goal Structuring Notation) を用いて、スクリプトを記述する手法に取り組んでいる。我々は、まずプログラミング言語の視点から GSN の操作的意味論を定義する。それに基づいて、GSN の要素からプログラムのモジュール化を行い、最終的に GSN が議論するディペンダビリティ要求の実現に対応づけられた実行可能コードの生成を行う (つまり、実行失敗は、ディペンダビリティ要求の未達と解釈される)。本論文は、操作的意味論および型システムを導入した、アシュアランス駆動によるプログラミングを提案する。

Toward Assurance Driven Programming

MASAKI ISHII^{1,a)} MASAHIRO IDE¹ KIMIO KURAMITSU^{1,2}

Presented: June 4, 2013

Assurance Case is a tool to discuss the system dependability requirement. It is widely used in safety community to obtain the agreement and assurance of the requirement. In this study, we are using a method of writing a script with Goal Structuring Notation (GSN), which is one of the assurance case notations. We define the operational semantics of GSN from the point of view of programming language. Based on it, we modularized program from elements of GSN and finally, we went the generation of executable code corresponding to the realization of dependability request discussed in GSN (i.e., the execution fails, the request is interpreted as unreached dependability). By introducing a type system and operational semantics, this paper proposes the Assurance Driven Script Programming.

¹ 横浜国立大学
Yokohama National University, Yokohama, Kanagawa 240-8501, Japan

² 科学技術振興機構/CREST
Japan Science and Technology Agency/CREST, Chiyoda, Tokyo 102-0075, Japan

^{a)} masaki.ishii511@gmail.com