World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:16, No:06, 2022

Petra: Simplified, Scalable Verification Using an Object-Oriented, Compositional Process Calculus

Authors : Aran Hakki, Corina Cirstea, Julian Rathke

Abstract : Formal methods are yet to be utilized in mainstream software development due to issues in scaling and implementation costs. This work is about developing a scalable, simplified, pragmatic, formal software development method with strong correctness properties and guarantees that are easy prove. The method aims to be easy to learn, use and apply without extensive training and experience in formal methods. Petra is proposed as an object-oriented, process calculus with composable data types and sequential/parallel processes. Petra has a simple denotational semantics, which includes a definition of Correct by Construction. The aim is for Petra is to be standard which can be implemented to execute on various mainstream programming platforms such as Java. Work towards an implementation of Petra as a Java EDSL (Embedded Domain Specific Language) is also discussed.

Keywords : compositionality, formal method, software verification, Java, denotational semantics, rewriting systems, rewriting semantics, parallel processing, object-oriented programming, OOP, programming language, correct by construction
Conference Title : ICFEME 2022 : International Conference on Formal Engineering Methods and Applications
Conference Location : Istanbul, Türkiye
Conference Dates : June 27-28, 2022