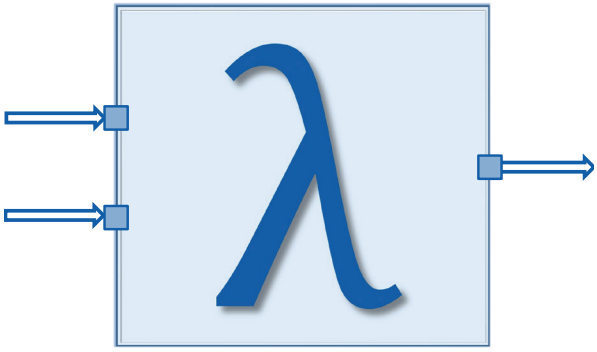
SE | RWTH AACHEN UNIVERSITY

RWTH Aachen University
Software Engineering Group

Towards an Isabelle Theory for distributed, interactive systems – the untimed case

Technical Report



Jens Christoph Bürger
Hendrik Kausch
Deni Raco
Jan Oliver Ringert
Bernhard Rumpe
Sebastian Stüber
Marc Wiartalla

Aachener Informatik-Berichte,
Software Engineering — Band 45

Hrsg: Prof. Dr. rer. nat. Bernhard Rumpe

Aachener Informatik-Berichte, Software Engineering

herausgegeben von
Prof. Dr. rer. nat. Bernhard Rumpe
Software Engineering
RWTH Aachen University

Band 45

**Jens Christoph Bürger, Hendrik Kausch, Deni Raco,
Jan Oliver Ringert, Prof. Dr. rer. nat. Bernhard Rumpe,
Sebastian Stüber, Marc Wiartalla,**
RWTH Aachen University

Towards an Isabelle Theory for distributed, interactive systems

The untimed case

Shaker Verlag
Düren 2020

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.d-nb.de.

Printed in Germany.

ISBN 978-3-8440-7265-5
ISSN 1869-9170

Shaker Verlag GmbH • Am Langen Graben 15a • 52353 Düren
Phone: 0049/2421/99011-0 • Telefax: 0049/2421/99011-9
Internet: www.shaker.de • e-mail: info@shaker.de

Abstract

This report describes a specification and verification framework for distributed interactive systems. The framework encodes the untimed part of the formal methodology FOCUS [BS01] in the proof assistant Isabelle [Pau90] using domain-theoretical concepts. The key concept of FOCUS, the stream data type, together with the corresponding prefix-order, is formalized as a pointed complete partial order. Furthermore, a high-level API is provided to hide the explicit usage of domain theoretical concepts by the user in typical proofs. Realizability constraints for modeling component networks with potential feedback loops are implemented. Moreover, a set of commonly used functions on streams are defined as least fixed points of the corresponding functionals and are proven to be prefix-continuous.

As a second key concept the stream processing function (SPF) is introduced describing a statefull, deterministic behavior of a message-passing component. The denotational semantics of components in this work is a defined set of stream processing functions, each of which maps input streams to output streams.

Furthermore, an extension of the framework is presented by using an isomorphic transformation of tuples of streams to model component interfaces and allowing composition. The structures for modeling component networks are implemented by giving names to channels and defining composition operators. This is motivated by the advantage that a modular modeling of component networks offers, based on the correctness of components of the decomposed system and using proper composition operators, the correctness of the whole system is automatically derived by construction.

To facilitate automated reasoning, a set of theorems is proven covering the main properties of these structures. Moreover, essential proof methods such as stream-induction are introduced and support these by further theorems. These examples demonstrate the principle usability of the modeling concepts of FOCUS and the realized verification framework for distributed systems with security and safety issues such as cars, airplanes, etc. Finally, a running example extracted from a controller in a car is realized to demonstrate and validate the framework.

Contents