



Universiteit
Leiden
The Netherlands

Modelling and analysis of real-time coordination patterns

Kemper, S.

Citation

Kemper, S. (2011, December 20). *Modelling and analysis of real-time coordination patterns*. IPA Dissertation Series. BOXPress BV, 2011-24. Retrieved from <https://hdl.handle.net/1887/18260>

Version: Corrected Publisher's Version

License: [Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden](#)

Downloaded from: <https://hdl.handle.net/1887/18260>

Note: To cite this publication please use the final published version (if applicable).

Samenvatting

De toenemende omvang van huidige ingebedde software systemen maakt de verificatie van deze systemen een steeds moeilijker opgave. Sterker nog, niet alleen de omvang van de systemen neemt toe, maar om toepassingen uit de praktijk zo waarheidsgetrouw mogelijk te modelleren en te analyseren moeten ook een toenemend aantal nieuwe mechanismen en formalismen ontworpen en ondersteund worden. De twee belangrijkste functies van ingebedde software systemen zijn dat ze in real-time moeten kunnen reageren op invoer uit de omgeving, en dat ze in een modulaire, op componenten gebaseerde manier ontwikkeld kunnen worden. Het laatste komt neer op het specificeren van het systeem door middel van afzonderlijke componenten (elk waarvan een bepaald aspect van het gedrag implementeert), samen met zogeheten connectoren die de coördinatiepatronen voor de communicatie tussen de componenten implementeren.

Om ervoor te zorgen dat het gedrag van het uiteindelijke systeem correct is (dat betekent, zich gedraagt zoals verwacht) en veilig (dat betekent, dat er geen fouten optreden), moet het systeem gecontroleerd worden voordat het in werking kan worden gesteld. Hiervoor zijn twee dingen nodig: ten eerste, formele modellen die expressief genoeg zijn om alle aspecten van het systeem zo waarheidsgetrouw mogelijk te beschrijven, en die in het bijzonder zowel real-time mechanismen bevatten als constructies om componenten en connectoren te combineren. Ten tweede, formele methoden om het formele model van het systeem te analyseren en te controleren of deze voldoet aan bepaalde eigenschappen, zoals met name juistheid van de coördinatiepatronen.

In dit proefschrift introduceren wij verschillende technieken met verschillende uitdrukkingsmogelijkheden voor het modelleren en analyseren van de coördinatiepatronen van op componenten gebaseerde real-time systemen. We presenteren de volgende drie operationele modellen van real-time systemen: Timed Automata, Timed Constraint Automata, en Timed Network Automata. Vervolgens geven we een vertaling voor elk van deze formele modellen naar een representatie in propositielogica met lineaire wiskunde, die het mogelijk maakt om beproefde op logica gebaseerde technieken, zogeheten SAT en SMT solvers, te gebruiken voor de analyse van de real-time eigenschappen van de betreffende operationele modellen. We geven een bewijs van juistheid voor de logische representatie, waaruit blijkt dat de resultaten verkregen door middel van deze technieken eveneens gelden voor de verschillende

operationele modellen.

Vervolgens presenteren wij een techniek voor verdere abstractie van de logische representatie die ons in staat stelt de omvang en complexiteit van deze te verminderen, door het verwijderen van die onderdelen die worden beschouwd als niet relevant voor de verificatie van een bepaalde eigenschap. We bewijzen dat deze techniek inderdaad leidt tot een over-abstractie die ons in staat stelt te concluderen dat een fout die in het abstracte systeem niet kan optreden ook in het oorspronkelijke systeem niet kan optreden. Tenslotte betogen we de toepasbaarheid en bruikbaarheid van onze theorie met een implementatie die het ontwerp en de analyse van op componenten gebaseerde real-time systemen ondersteunt.