

Introduzione alla specifica formale di sistemi critici

L'obiettivo del corso è introdurre ed ampliare le conoscenze relative alle metodologie di modellazione/specifica e analisi formale di sistemi critici con l'ausilio del metodo formale *Asbstrat State Machines*. In particolare, attraverso l'uso pratico del toolset ASMETA, si illustreranno casi di studio reali di specifica e prime forme di analisi formale per sistemi reattivi e discreti. Verrà infine accennato un argomento trasversale al corso sul problema di Resource Allocation e tecniche formali per affrontarlo.

Prerequisiti: Basi solide di Matematica (Algebra), logica, semantica dei linguaggi, Ingegneria del Software, Interesse per la specifica dei sistemi reattivi e sistemi software e per la loro analisi.

Argomenti trattati:

- Comprensione del problema della specifica e analisi formale di sistemi critici. Metodi formali versus metodi semi-formali (come l'Unified Modeling Language) della Model-driven Engineering.
- I formalismi state-like ed il metodo formale delle Abstract State Machines (ASMs) per la modellazione e analisi (validazione e verifica) di sistemi reattivi.
- Esperienza con il toolset ASMETA per la specifica e primi metodi di analisi formale in ASM. In particolare, si illustrerà l'uso dei tool *Asmeats* e *AsmetaV* per, rispettivamente, la simulazione e la simulazione guidata da scenari di specifiche ASM di opportuni sistemi (*Advanced Clock*, *Safety Injection System*, *Sluice Gate System*, *ATM*, ecc..) scelti come casi di studio.
- Cenni alle recenti tendenze della ricerca in tecniche e metodologie di analisi formale.
- Argomento trasversale al corso: tecniche formali di Resource Allocation, Trading and Adaptation in Self-Managing con applicazioni in ambito aeronautico e internet-ware.

Testi e materiale:

- E.Börger, R. Stärk. *Abstract State Machines: A Method for High-Level System Design and Analysis*, Springer Verlag, 2003.
- Doron Peled. *Software Reliability Methods*. Springer, 2001.
- Altro materiale (articoli, siti web, guide, ecc..) fornito durante il corso

Docente: Patrizia Scandurra

Assistant Professor (researcher)
Dipartimento di Ingegneria dell'Informazione e Metodi
Matematici (DIIMM), University of Bergamo - Viale Marconi, 5 -
24044 Dalmine (BG)
Phone +39 035 2052358
Fax +39 035 2052310
Web page <http://cs.unibg.it/scandurra/>