Application BASTRI
Fiches Equipes

NOVALTIS (SR0364BR)
NOVel ALgorithms and VALidation Techniques for Time-critical and high Integrity Systems
NOVALTIS

Statut: Terminée

Responsable : Gerard Le_Lann

Mots-clés de "A - Thèmes de recherche en Sciences du numérique - 2023" : Aucun mot-clé.

Mots-clés de "B - Autres sciences et domaines d'application - 2023" : Aucun mot-clé.

Domaine : Systèmes communicants
Thème : Systèmes embarqués et mobilité

Période : 01/12/2004 -> 31/12/2006

Dates d'évaluation :

Etablissement(s) de rattachement : <sans>
Laboratoire(s) partenaire(s) : <sans UMR>

CRI : Centre Inria de Paris
Localisation : Rocquencourt
Code structure Inria :

Numéro RNSR : 200421407F
N° de structure Inria: SR0364BR

Présentation

Background & Objectives:
NOVALTIS builds upon project REFLECS. New challenges are:

(A1) Models and Algorithms

- **Safety and liveness**: To explore most extreme asynchronous computational/system models, to specify and prove distributed algorithms in such models aimed at solving *agreement problems* in distributed fault-tolerant computing, while circumventing *impossibility results* (research on the *Theta-model*)

- **Timeliness and asynchrony**: To examine how to use purely asynchronous (time-free) algorithms or partially synchronous algorithms for solving problems in distributed *real-time* computing, where strict *timeliness* properties must be proven to hold (research on the *design immersion principle*)

- **Timeliness and overloads**: To investigate scheduling problems (algorithms, schedulability analyses, feasibility conditions) that arise with timeliness/scheduling attributes more complex than constant deadlines, assuming overloads are normal conditions (research on *time utility function (TUF)-driven schedulers*)

- **Composed safety, liveness, timeliness and dependability**: To devise, specify, and prove algorithms directed at endowing a distributed computing system with a specific combination of safety, liveness, timeliness, and dependability properties (research drawing from multiple disciplines, such as, e.g., Concurrency Control, *Serializability theory*, *Distributed Algorithms*, *Scheduling theory*)

(A2) Proof-Based System Engineering (PBSE)

- To address issues arising with the *early phases in a project lifecycle* (application requirement capture, system design and forward validation), for systems bound to meet specified properties *very high coverage*

- To investigate how to maintain a *continuous chain of proofs* from application requirement capture to implementation of a validated system-solution

- To introduce *system-level proof obligations in system engineering methods* used for real projects, notably proofs of combined safety, liveness, dependability, and timeliness properties

- To blend together *scientific rigor (proof obligations) and reality* (proof assumptions, design assumptions, must be shown to be provably...
To contribute to the development of PBSE tools

(A3) Analyses of causes of mishaps or failures:
- To examine documented cases of mishaps, quasi-failures or failures experienced with projects (before system deployment) and with deployed critical systems
- To identify causes of difficulties, with a special focus on system engineering faults
- Contributions to the safety-critical forum (moderated by York University, UK).

Publications

Axes de recherche

Scientific areas:
- (A1) System-level algorithms, specifications and proofs: Research on computational/system models and distributed algorithms for critical computing systems where combined safety, liveness, timeliness & dependability properties must be predicted
- (A2) System-level engineering methods: Research on proof-based system engineering (PBSE) methods directed at critical and/or complex computer-based applications and systems
- (A3) Analyses of causes of mishaps or failures: Diagnoses of real causes of difficulties experienced with projects (time/budget overruns, cancellations) and with deployed critical systems (failures or quasi-failures)

Major application domains (2005):
Defense (all forces), Aerospace (deep space exploration, earth orbiting vehicles, autonomous systems).

Relations industrielles et internationales

Established partnership with academia (2005):
- Vienna University of Technology, Austria
- École Polytechnique Fédérale de Lausanne (EPFL), Switzerland
- Virginia Tech, USA

Established partnership with industry (2005):
- DGA (French MoD)
- Safran
- MITRE Corp., USA