Formal Verification of Critical Applications

David Pereira José Proença Eduardo Tovar

FVOCA 2021/2022

Formal Verification of Critical Applications

CISTER – ISEP
Porto, Portugal

https://cister-labs.github.io/fvoca2122

Last semester @ RAMDE

- High-level overview of requirements and associated processes
- Mathematical Preliminaries
  - Basic mathematical notations
  - Set theory
  - PropositionalLogic
  - First Order Logic
- Behavioural modelling with mCRL2
  - *Process algebra*
  - Equivalences
  - Verification
- Requirement analysis with EARS

Course structure

1. **Real-time models**
   - Timed Automata and Hybrid Automata
   - Temporal logic
   - Static verification using UPPAAL
2. **Program verification**
   - First Order Logic revisited
   - Abstract Program Semantics
   - Design by Contract and Hoare Logic
   - Verification of annotated programs
3. **Requirements**
   - SAT and SMT solvers
   - *Automatic* theorem proving using Z3
   - Introduction to *Interactive* theorem proving using Coq

Pragmatics

https://cister-labs.github.io/fvoca2122

Final mark = Project (60%) + Exam (40%)

- Groups of 2 students
- Project in 2 parts
- Homework's evaluation included in the project

The Team

- David Pereira (drp)
- José Proença (pro)
- Eduardo Tovar (emt)

- Microsoft Teams
- Email (@isep.ipp.pt)