Formal methods  (4 hours, corresponding to 5 credits in PdM standard)

The course aims at introducing the students to the application of formal methods to the practice of software engineering, with particular reference to concurrent, distributed, and real-time systems.

Course topics

Part one: the basics of formal methods
- Introduction to formal methods  (2 hours teaching)
  - What do we mean by “formal method (FM)?”
  - What are they for?
  - Distinguishing features of FMs
  - FMs in the context of software life cycle
- Recalls of formal specification  (2 hours teaching)
- Formal verification: the Hoare’s approach  (10 hours teaching including class exercises)
- Other formal-based verification techniques: model-checking  (2 hours teaching)
- A classical FM: the B method  (4 hours teaching including class exercises)

Part two: formal methods for concurrent, distributed and real-time systems
- Introductory remarks: distinguishing features of concurrent and real-time systems and their consequences on the use of formal methods for such systems (2 hours)
- Survey of some operational and descriptive formalisms for concurrent and real time systems (timed automata, timed Petri nets, timed CSP, …; temporal logics, with particular reference to the TRIO language)  (8 hours teaching)
- The dual language approach  (4 hours teaching)
- The TRIO method and its tools for the development of distributed and real-time systems  (6 hours teaching)
- Case studies in the application of the TRIO method  (6 hours teaching)

Teaching material

There is no complete textbook. However, the following texts will approximately cover the program course:
Mandrioli and Ghezzi, Theoretical foundations of computer science (mainly, chapter 5), John Wiley and Sons, 1987
Sekerinski and Sere (eds), Program development by refinement, Springer, 1999
(or other equivalent book on th B method)
Heitmeyer and Mandrioli (eds), Formal methods for real-time computing, John Wiley, 1996
The teacher will also prepare aiding transparencies and will distribute scientific papers on the TRIO lanaguage, its use, its tools, and its application.

Course and exam organization
The course will consist of approx. 46 hours of class teaching, including exercises illustrated by the teacher and/or the TAs. Several homeworks will be assigned and corrected. At least one of them will consist in the development of a complete case study and will include the use of some supporting tool. Students will be required to produce appropriate and complete documentation. Two midterm class tests will be done, one after Part One and one after the first section of Part Two. The integration of the above work will produce the final evaluation. Thus, no formal final exam is scheduled.