ClearSy

The B formal Method: from Research to Teaching

An Overview of Atelier B 4.0
What is Atelier B

- An industrial tool for developing software and systems with the B method
- Provides tools for developing with B
  - Multi-user project management
  - Typechecking of components
- Allows validation of B projects
  - Generation of proof obligations
  - Automatic prover
  - Interactive prover
- Code generation
  - Code translators for C, C++ and Ada
Industrial references: Software development

- **KVB: Alstom**
  - Automatic Train Protection for the French railway company (SNCF),
  - installed on 6,000 trains since 1993
  - 60,000 lines of B; 10,000 proofs; 22,000 lines of Ada

- **SAET METEOR: Siemens Transportation Systems**
  - 3 safety-critical software parts: onboard, section, line
  - 107,000 lines of B; 29,000 proofs; 87,000 lines of Ada
Industrial references: Software development

- **Roissy VAL**: ClearSy (for STS)
  - Section Automatic Pilot: light driverless shuttle for Paris-Roissy airport (ADP), 2006
  - 28,000+155,000 lines of B; 43,000 proofs; 158,000 lines of Ada

- **URBALIS EVOLUTION**: Alstom, Clearsy (for Alstom)

- **LINE 1 of Paris (new project)**: Siemens Transportation Systems
  - Automatic Train Control: new driverless metro line 1 in Paris (RATP)
Industrial references: B-System

- **Peugeot Automobiles**
  - Model of the functioning of subsystems (lightings, airbags, engine, ...) for Peugeot aftersales service
  - Goal: Understanding precisely the functioning of cars to build tools to diagnose breakdowns

- **RATP (Paris Transportation)**
  - Model of automatic platform doors to equip an existing metro line
  - Goal: Verifying consistency of System Specification

- **EADS**
  - Model of tasks scheduling of the software controlling stage separation of Ariane rocket
Industrial references: B-System

- FDIR strategy validation with B (Thales Alenia Space/CNES)
  - Formation flying satellite system
- INRS (French Institute for Workers Safety)
  - Model of a mechanical press complying with safety requirements (protection of the hands of the press operator)
  - Building the software specification of the press controller
- DOF1 : CLeaSy (for RATP)
  - Device to Open and Close the Platform Doors on line 1,
  - Safety Level SIL4
  - from the B system models to the B software models and the Lader program for Simatic Siemens Automata
What's new with Atelier B 4.0 (1)

- Core features
  - BART automatic refinement tool
  - Improvements to the well-definition proofs
  - Comenc translator (already available with Atelier B 3.7.2)

- Redesigned GUI
  - Allows parallelisation of typecheck, PO generation and interactive proofs
  - Lots of interactive prover improvements
  - Provides a B editor
What's new with Atelier B 4.0

- Supported platforms
  - Linux
  - Solaris
  - Mac Os X
  - Windows

- A new distribution policy
  - Free (non paying) version every two years
  - Paying tool support
    - Allows getting intermediary versions between the free version
    - Other goodies
  - Open-sourcing of many tools and documents
    - Reference manual, trainings...
    - Comenc, Bart, GUI...
Atelier B 4.0 on Linux
Atelier B 4.0 on Windows
Atelier B 4.0 on Mac Os
Conclusion

- Atelier B 4.0 Currently in development
  - First beta planned for September 2008
    - Opened to people with Atelier B 3.7 support contract
  - Final version in late 2008/early 2009
- Version 3.7.2 freely available for academics and students
- B4free still available
16 juin 2008

Thanks