16 juin 2008 - NANTES

ClearSy

The B formal Method: from Research to Teaching

An Overview of Atelier B 4.0

Antoine Requet

CLEARSY
SYSTEM ENGINEERING

Parc de la Duranne
320 Av Archimède
Les Pléiades III – Bât. A
13 857 Aix-en-Provence Cedex 3

Téléphone : 04.42.37.12.70
Télécopie : 04.42.37.12.71

www.ClearSy.com

CLEARSY
System Engineering

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
  - Automatic Train Control: new driverless metro line 14 in Paris
  - (RATP), 1998. 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)
  - Automatic Train Protection, installed on the new metro of Pekin (2008)
- 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 : CLearSy (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)

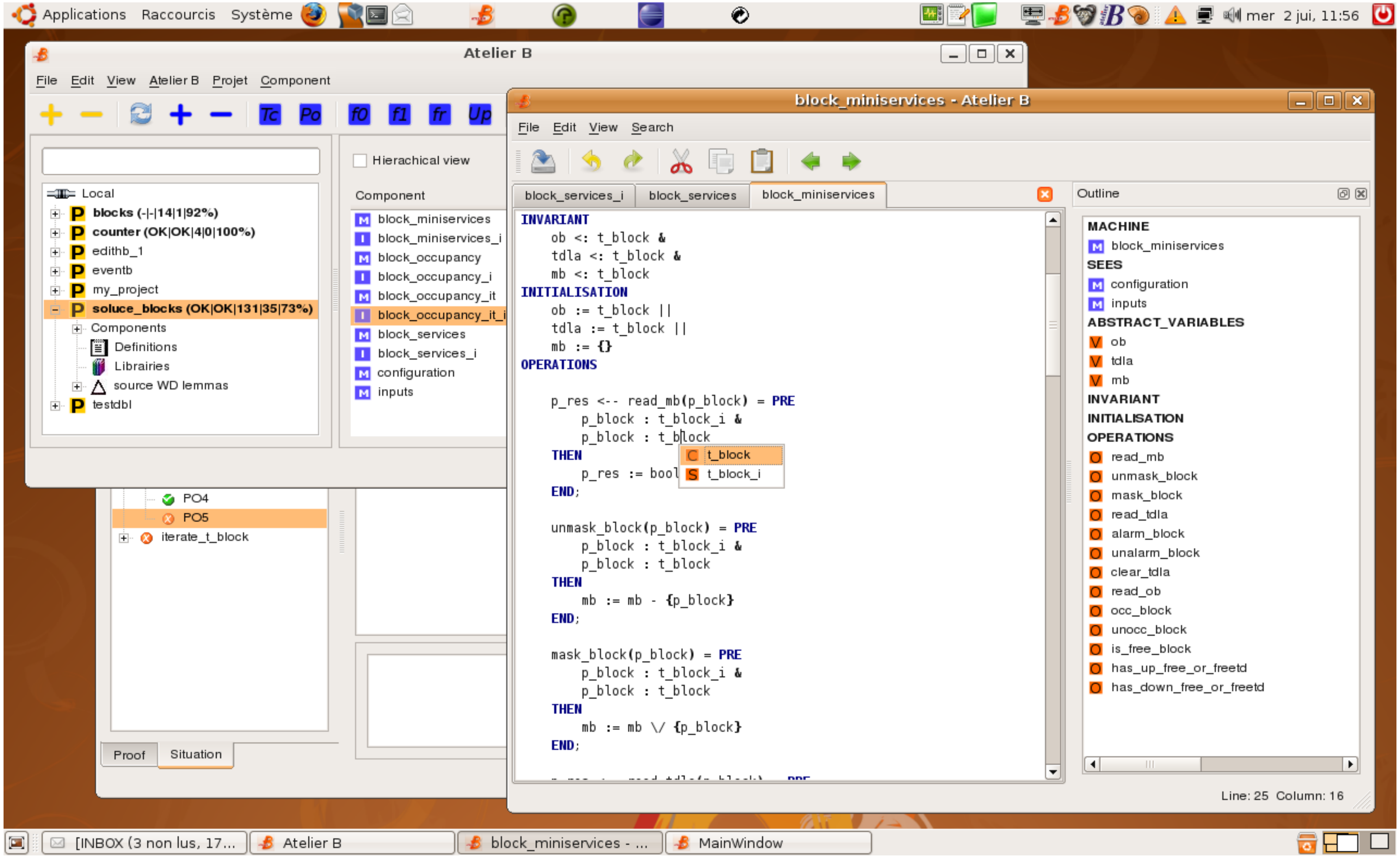
- Core features
  - BART automatic refinement tool
  - Improvements to the well-definition proofs
  - Comenc translator (already available with Atelier B 3.7.2)

- 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...

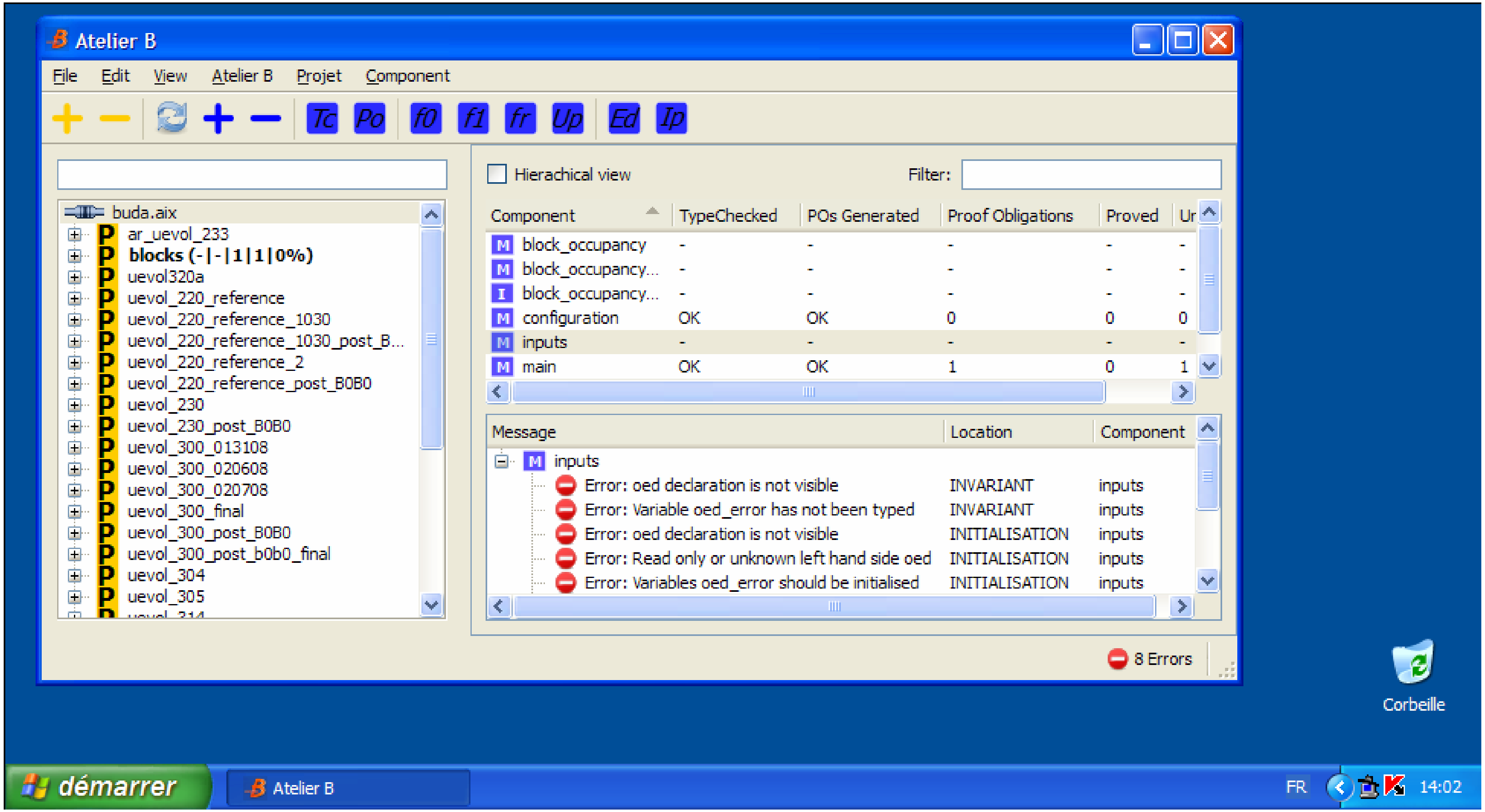
Atelier B 4.0 on Linux



```
INVARIANT
    ob <: t_block &
    tdla <: t_block &
    mb <: t_block
INITIALISATION
    ob := t_block ||
    tdla := t_block ||
    mb := {}
OPERATIONS

    p_res <-- read_mb(p_block) = PRE
        p_block : t_block_i &
        p_block : t_block
    THEN
        p_res := bool
    END;

    unmask_block(p_block) = PRE
        p_block : t_block_i &
        p_block : t_block
    THEN
        mb := mb - {p_block}
    END;

    mask_block(p_block) = PRE
        p_block : t_block_i &
        p_block : t_block
    THEN
        mb := mb \/ {p_block}
    END;
```

```
MACHINE
    block_miniservices
SEES
    configuration
    inputs
ABSTRACT_VARIABLES
    ob
    tdla
    mb
INVARIANT
INITIALISATION
OPERATIONS
    read_mb
    unmask_block
    mask_block
    read_tdla
    alarm_block
    unalarm_block
    clear_tdla
    read_ob
    occ_block
    unocc_block
    is_free_block
    has_up_free_or_freetd
    has_down_free_or_freetd
```

Atelier B 4.0 on Windows

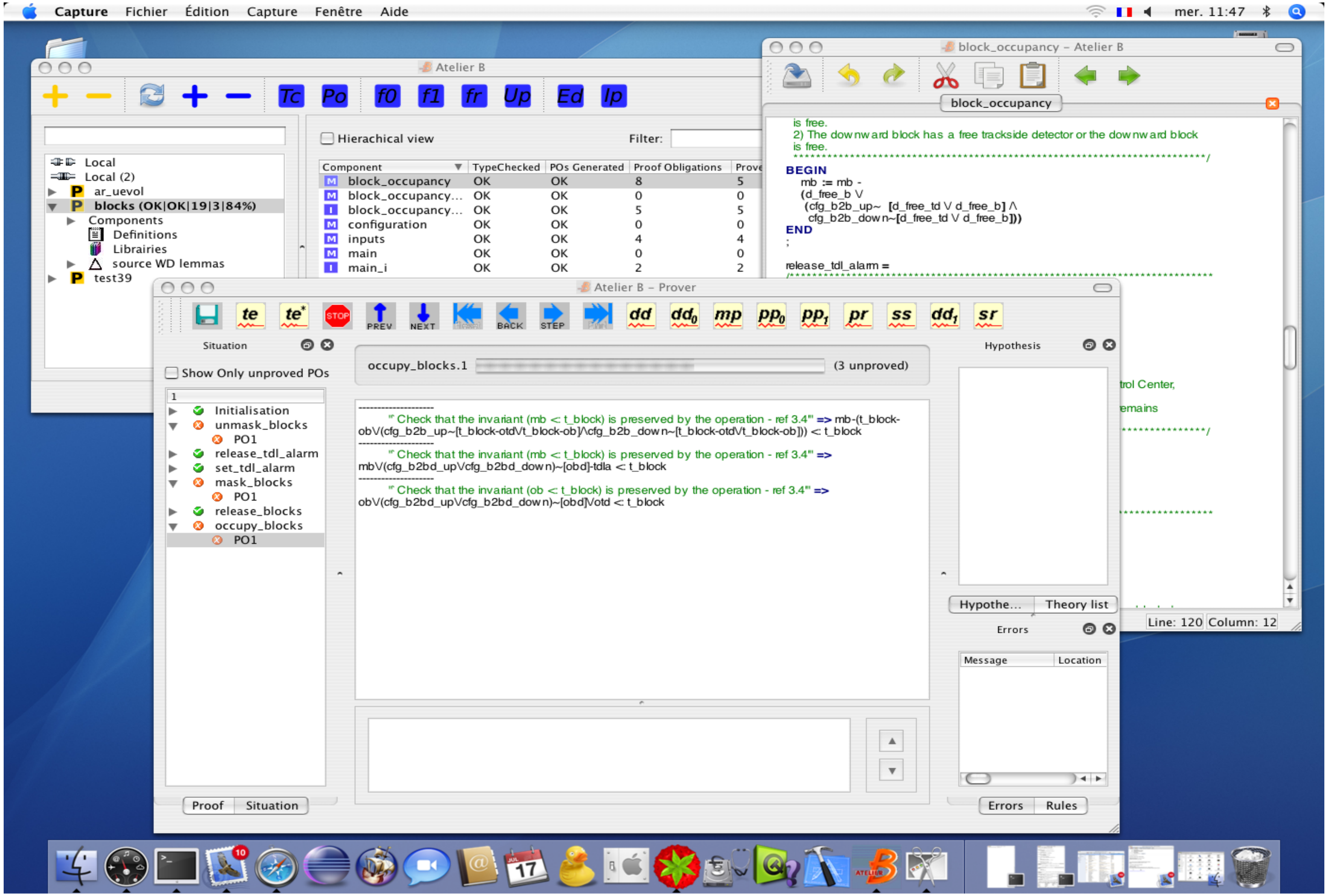


buda.aix
- ar_uevol_233
- **blocks (-|-|1|1|0%)**
- uevol320a
- uevol_220_reference
- uevol_220_reference_1030
- uevol_220_reference_1030_post_B...
- uevol_220_reference_2
- uevol_220_reference_post_B0B0
- uevol_230
- uevol_230_post_B0B0
- uevol_300_013108
- uevol_300_020608
- uevol_300_020708
- uevol_300_final
- uevol_300_post_B0B0
- uevol_300_post_b0b0_final
- uevol_304
- uevol_305
- uevol_314

Component	TypeChecked	POs Generated	Proof Obligations	Proved	Ur
M block_occupancy	-	-	-	-	-
M block_occupancy...	-	-	-	-	-
I block_occupancy...	-	-	-	-	-
M configuration	OK	OK	0	0	0
M inputs	-	-	-	-	-
M main	OK	OK	1	0	1

Message	Location	Component
M inputs		
Error: oed declaration is not visible	INVARIANT	inputs
Error: Variable oed_error has not been typed	INVARIANT	inputs
Error: oed declaration is not visible	INITIALISATION	inputs
Error: Read only or unknown left hand side oed	INITIALISATION	inputs
Error: Variables oed_error should be initialised	INITIALISATION	inputs

Atelier B 4.0 on Mac Os



Component	TypeChecked	POs Generated	Proof Obligations	Prove
M block_occupancy	OK	OK	8	5
M block_occupancy…	OK	OK	0	0
I block_occupancy…	OK	OK	5	5
M configuration	OK	OK	0	0
M inputs	OK	OK	4	4
M main	OK	OK	0	0
I main_i	OK	OK	2	2

```
  is free.
  2) The downward block has a free trackside detector or the downward block
  is free.
  ************************************************************************/
BEGIN
   mb := mb -
   (d_free_b ∨
    (cfg_b2b_up~  [d_free_td ∨ d_free_b] ∧
     cfg_b2b_down~[d_free_td ∨ d_free_b]))
END
;

release_tdl_alarm =
/*************************************************************************
```

```
1
▶ ✓ Initialisation
▼ ⊗ unmask_blocks
      ⊗ PO1
▶ ✓ release_tdl_alarm
▶ ✓ set_tdl_alarm
▼ ⊗ mask_blocks
      ⊗ PO1
▶ ✓ release_blocks
▼ ⊗ occupy_blocks
      ⊗ PO1
```

occupy_blocks.1 (3 unproved)

```
--------------------
      " Check that the invariant (mb <: t_block) is preserved by the operation - ref 3.4"' => mb-(t_block-
ob∨(cfg_b2b_up~[t_block-otd∨t_block-ob]∧cfg_b2b_down~[t_block-otd∨t_block-ob])) <: t_block
--------------------
      " Check that the invariant (mb <: t_block) is preserved by the operation - ref 3.4"' =>
mb∨(cfg_b2bd_up∨cfg_b2bd_down)~[obd]-tdla <: t_block
--------------------
      " Check that the invariant (ob <: t_block) is preserved by the operation - ref 3.4"' =>
ob∨(cfg_b2bd_up∨cfg_b2bd_down)~[obd]∨otd <: t_block
```

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

CLEARSY
SYSTEM ENGINEERING

Parc de la Duranne
320 Av Archimède
Les Pléiades III – Bât. A
13 857 Aix-en-Provence Cedex 3

Téléphone : 04.42.37.12.70
Télécopie : 04.42.37.12.71

www.ClearSy.com

CLEARSY
System Engineering