Ten Years Disseminating
The B Method

Thierry Lecomte
thierry.lecomte@clearsy.com
A quick summary of the last 15 years

1994

1998

METEOR
MATRA

2000

Clic’n’prove
ROISSY
SIEMENS

PEKIN
ALSTOM

2010

Bart
AREVA

COPPILOT

PARIS, SAO PAULO

na Bama F

ATELIER

4.0

Comenc

4.0

ATELIER

2
Industrial dissemination and exploitation
Some implementations (B)
Current picture: « B inside » metros
Some (external) experimentations

- **Automotive:**
  - Diagnosis (Peugeot)
  - Contactless keycard (Renault)

- **Banking:**
  - Reconciliation (Société Générale)

- **Space:**
  - Ariane 5 flight software (EADS)

- **Microelectronics**
  - Smartcard (STMicroelectronics)

- **Nuclear**
  - Control System Design (EDF)

- **Industry**
  - Pneumatic Press (CNAM)
Some (external) experimentations: REX

- **Automotive:**
  - Diagnosis (Peugeot)
  - Contactless keycard (Renault)

- **Banking:**
  - Reconciliation (Société Générale)

- **Space:**
  - Ariane 5 flight software (EADS)

- **Microelectronics**
  - Smartcard (STMicroelectronics)

- **Nuclear**
  - Control System Design (EDF)

- **Industry**
  - Pneumatic Press (CNAM)
Some implementations (microelectronics)

<table>
<thead>
<tr>
<th>Year</th>
<th>Secure microcontrollers</th>
<th>Secure microcontrollers</th>
<th>Secure microcontrollers</th>
</tr>
</thead>
<tbody>
<tr>
<td>1998</td>
<td>ST22L128</td>
<td>ST19NA18</td>
<td>ST23YR80</td>
</tr>
<tr>
<td>2000</td>
<td>32-bit secure microcontroller</td>
<td>ST19NT66A</td>
<td>SA23YR80</td>
</tr>
<tr>
<td>2002</td>
<td>ST19WP</td>
<td>EAL5+</td>
<td>EAL5+</td>
</tr>
<tr>
<td>2004</td>
<td>ST19WL</td>
<td>ST</td>
<td>Atmel</td>
</tr>
<tr>
<td>2006</td>
<td>ST22L128</td>
<td>ST19WR08</td>
<td>ST23YL80</td>
</tr>
<tr>
<td>2008</td>
<td>EAL5+</td>
<td>ST23YL18</td>
<td>EAL5+</td>
</tr>
<tr>
<td>2010</td>
<td>ST</td>
<td>ST</td>
<td>Atmel</td>
</tr>
</tbody>
</table>

Secure microcontrollers
- ST22L128
- ST19WP
- ST19WL
- ST22L128

Microcircuits
- ST22L128
- ST19WP
- ST19WL

STMicroelectronics announced that the established ST22L128 32-bit secure microcontroller has received 'Common Criteria' security certification at Evaluation Assurance Level EAL5+ (Augmented). The formal recognition will now enable 3G network operators to extend their secure mobile services with M-commerce and digital signature applications, and will provide new opportunities in banking and ID market segments.
Some (internal) experimentations

- Platform screen doors
- Safety critical systems (SIL3/SIL4)
- Opening and closing doors

- Event-B system level specification
- PLC code generated
- Specific to a PLC (Siemens S7)
Development cycle

Statement of work → Specification → Refinement → Implementation

Animation (Internal verification) → Proof → Validation Guide (External verification)

Manual code (LADDER) → Safety demonstration

Safety case → Experiment → Verification of hypotheses

Qualified for SIL3/SIL4 systems
Some implementations

- Platform Screen Doors Demonstrator
  - L13
  - Paris
- Platform Screen Doors
  - L13
  - Paris
- L13 Automatic Gap Filler
  - Paris
- PSD L1
  - Paris
- PSD L2 L3
  - Sao Paulo
- Metro L3
  - Cairo
  - 2011?
R & D
Source HDL Classical Development Flow
New Proved Source HDL Development Flow

Property Level Model

Adding Details

Architecture Level Details

Implementation Level Details

Real Interface

Proof Obligations

Event B (System Modeling)

Abstraction

Data Sheet

Interface Specification

Functional Specification

Verification Specification

B4SYN

Generated VHDL

Test Plan & Programs

Compiling

Autotesting Binaries

RTL Representation

Gate Level Representation

Verification Campaign

Simulations

Compiling

Synthesis
<table>
<thead>
<tr>
<th>Criteria</th>
<th>Classical Flow</th>
<th>Experimental Flow</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effort person.days</td>
<td>~145</td>
<td>~145 (~200 translator)</td>
</tr>
<tr>
<td>Volume commented source lines</td>
<td>~3 600 VHDL</td>
<td>~7 500 B  ~3 500 VHDL</td>
</tr>
<tr>
<td>Proof number of items</td>
<td>-</td>
<td>~1 600 obligations ~600 with ~4000 cmds</td>
</tr>
<tr>
<td>Structure module number</td>
<td>~15 tightly linked</td>
<td>4 loosely linked (only 1 generated module)</td>
</tr>
<tr>
<td>Simulation RTL &amp; gate level</td>
<td>~30 patterns Ok</td>
<td>~30 patterns Ok (better debug signals)</td>
</tr>
<tr>
<td>Size equivalent nand gates</td>
<td></td>
<td>~5 Kgates</td>
</tr>
</tbody>
</table>
Tooling

**Convention B**

- Automatic Prover
- Predicate Prover

- Automatic Prover
- Predicate Prover
Tooling

Rodin

Automatic Prover
Predicate Prover
Brama Animator

Automatic Prover
Predicate Prover
Brama Animator
Tooling

ANR Rimel

Automatic Prover
Predicate Prover
Bart Automatic Refiner
Brama Animator

Automatic Prover
Predicate Prover
Brama Animator
Tooling

RNTL BOM

- Automatic Prover
- Predicate Prover
- ComenC Code Generator
- Bart Automatic Refiner
- Brama Animator

- Automatic Prover
- Predicate Prover
- Brama Animator
Tooling

Forcoment

B₄SYN Code Generator

ComenC Code Generator

Automatic Prover

Predicate Prover

Bart Automatic Refiner

Brama Animator

Automatic Prover

Predicate Prover

Brama Animator
Downloads

monthly downloads since January 2009

# downloads (samples)
Rodin 1.0: 608
Rodin 1.3: 449
Atelier B 4.0: 3877
Specific Events: B Dissemination Days

- **Rodin Industry Day**
  - Aix en Provence
  - Apr 2006

- **Rodin Industry day**
  - Paris
  - Sep 2007

- **B Dissemination day**
  - Salvador de Bahia
  - Aug 2008
  - Satellite event of SMBF conference

- **B Dissemination day**
  - Sao Paulo
  - Aug 2008
  - First technical workshop organised by IPT new lab on Requirements

**23**
Specific Events: B Dissemination Days

- **RIAB**
  - Eindhoven, Nov 2009
  - Satellite event of FM conference

- **B Dissemination Day**
  - Tokyo, Mar 2010
  - Satellite event of GRACE symposium on advanced software engineering

An original book on SW development in B
Specific Events: B Dissemination Days

Satellite event of SBMF 2010

- Day 1: DEPLOY speakers
- Day 2: external papers (Cfp)

Day 1
- Session 1: Tools
- Session 2: Tools and extensions
- Session 3: Modelling
- Session 4: Industrial applications

Day 2
- Session 1
- Session 2
- Session 3
- Session 4

Courses
Courses

- « Applications industrielles de B »
  IRIT Toulouse – master 2

- « Spécification et conception sécurisées »
  ENSI Bourges – 3ème année option sécurité logicielle

- « Méthodes formelles »
  ENSMSE Gardanne – 3ème année

- « Développement de logiciels critiques »
  ESIL Marseille – 3ème année
Courses

- Specification in B and Event-B
- Design and software development in B

Examples issued from/inspired by industrial applications:
- Smartcard security policy
- Railway Switch
- Fuel level
- Block
- Virtual machine
- Stack

- Event-B specification
- B specification and design
- B specification and design
- B specification
**Smartcard security policy**

### Security property

\[
\text{MEMORY\_TYPE(currentCell)} = \text{ROM\_SECURE} \land \\
\text{currentOperation} = \text{OP\_READ} \land \\
\text{currentMode} = \text{USER}
\]

\[=>
\text{currentResult} = \text{NOT\_GRANTED}
\]

### RAM read access control

\[
\text{executeRAM} = \\
\text{SELECT} \\
\text{MEMORY\_TYPE(currentCell)} = \text{RAM} \land \\
\text{MEMORY\_CONTENT(currentCell)} = \text{CODE} \land \\
\text{currentOperation} = \text{OP\_EXECUTE}
\]

\[\text{THEN}
\text{currentResult} := \text{GRANTED}
\]

\[\text{END}\]
Fuel level

Services: compute_initial_level, estimate_remaining_fuel

safety property: « make the pilot aware of any fuel shortage »

Complete development: specification, design, implementation (including context machine), basic machine, code generation (ComenC) and execution
Fuel level

VARIABLES
estimated_level, estimated_consumption, status

CONCRETE_VARIABLES
estimated_level, estimated_consumption, status

ctx
ctx_i

fuelo
fuel_i

measure

utils
utilsi

sees
sees
imports
Block
Block

down exit detector  down border detector  block  up border detector  up exit detector

Trackside Detector
Services: specify which blocks are occupied and which are free, according to (faulty) sensors

Simplification: no switch

Unmask_blocks:

This function unmasks some blocks (for TDL alarm). Blocks which do not become unmasked remain unchanged.
A block is unmasked when the block is free or when all of the following conditions are true:
1) The upward block has a free trackside detector or the upward block is free.
2) The downward block has a free trackside detector or the downward block is free.

\[
mb := mb - (d_{free}\_b \cup (cfg\_b2b\_up^{-1} [d_{free}\_td \cup d_{free}\_b] \cap cfg\_b2b\_down^{-1} [d_{free}\_td \cup d_{free}\_b]))
\]
Return of experience

- Easier to teach B when code is generated
  - First exercise was guided, following almost unguided

- Students admit that proof is valuable
  - When discovering errors, even if a.k.o. black box

- ... but are puzzled when a 100% model is faulty
  - Miracles, copy/paste specification and design
  - Model animation

- Data or algorithmic refinement difficult to handle
Future

Directions
Future directions

- **Dedicated modelling environments**
  - **PLC based system development**
    - Safety critical products
    - Tool qualification
    - Automatic refinement
    - Code generation
    - Test case generation
  - **Microelectronics**
    - Smartcard domain
    - Automatic refinement
    - Code generation
Future directions (cnt’d)

- Improvements
  - Provers (last major step in 1999)
    - ProB fine-grain integration
    - Distributed processing (cloud)
  - Code generation
    - C (without safety critical constraints)
    - VHDL, Ladder
  - Support for real numbers & floating point
  - Generic proof obligation generator
    - Required for new application domains
Thank you for your attention
Tools (alphabetical order)

- Atelier B tool
- Batcave A Proof Obligation Generator
- B-Core (UK) Ltd
- B2EXPRESS Animator
- B4free freeware tools
- BRILLANT open source platform
- DumBeX B notation to \LaTeX
- ProB Animator and Model Checker
- Rodin event-B open source platform