

A « Correct by Construction »  
Realistic Digital Circuit

Marc BENVENISTE  
Formal Methods  
Digital Secure Access Division

Recent Innovations and Applications in RI'2009, November 3rd, 2009, TU Eindhoven

deploy

Digital Secure Access (DSA) Division  
<http://www.st.com/stonline/domains/applications/security/index.htm>

**Smartcard Circuits**

**Mobile Telecom**  
TAM 2008 ~ 3 Bu

**Secure Smartcards**  
TAM 2008 ~ 800 Mu

**Secure Conditional Access**  
TAM 2008 ~ 150 Mu

**SIM USIM NFC Solutions**

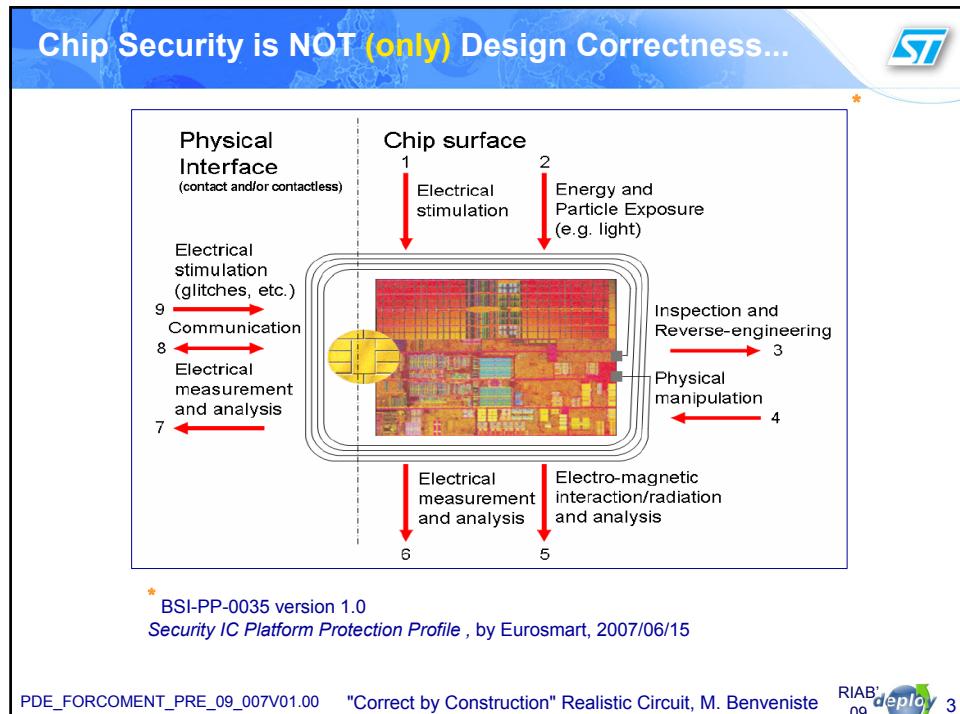
**Gov & ID Banking Transport**

**Pay TV IT & Security**

**Mid Range Security**

**High Range Security**

PDE\_FORCOMENT\_PRE\_09\_007V01.00   "Correct by Construction" Realistic Circuit, M. Benveniste   RIAB'09 deploy 2



**Quoting www.scdsource.com\***

**ARM**'s Bryan Dickman said:

We hope to see a **correct-by-construction design flow** that may also reduce the overall verification burden

We could get there by having designers use the tools from design onwards in the flow to **systematically explore and formally prove their code**

At the moment, we're using formal **rather retrospectively**

\* <http://www.scdsource.com/article.php?id=341>  
*Mixing Formal and Dynamic Verification, Part1 & Part 2*, by Bill Murray, 2009/05/29  
(emphasizing is mine)

PDE\_FORCOMENT\_PRE\_09\_007V01.00 "Correct by Construction" Realistic Circuit, M. Benveniste RIAB'09  5

**Correct by Construction Chip Functionality:  
An advanced R&D feasibility study report**

- ST23 Memory Protection Unit at a Glance
- Traditional Design Flow
- Experimental Design Flow
- Main Construction Steps
- Traditional versus Experimental
- Limitations & Ways Forward

PDE\_FORCOMENT\_PRE\_09\_007V01.00 "Correct by Construction" Realistic Circuit, M. Benveniste RIAB'09  6

**Correct by Construction Chip Functionality:  
An advanced R&D feasibility study report**

**ST**

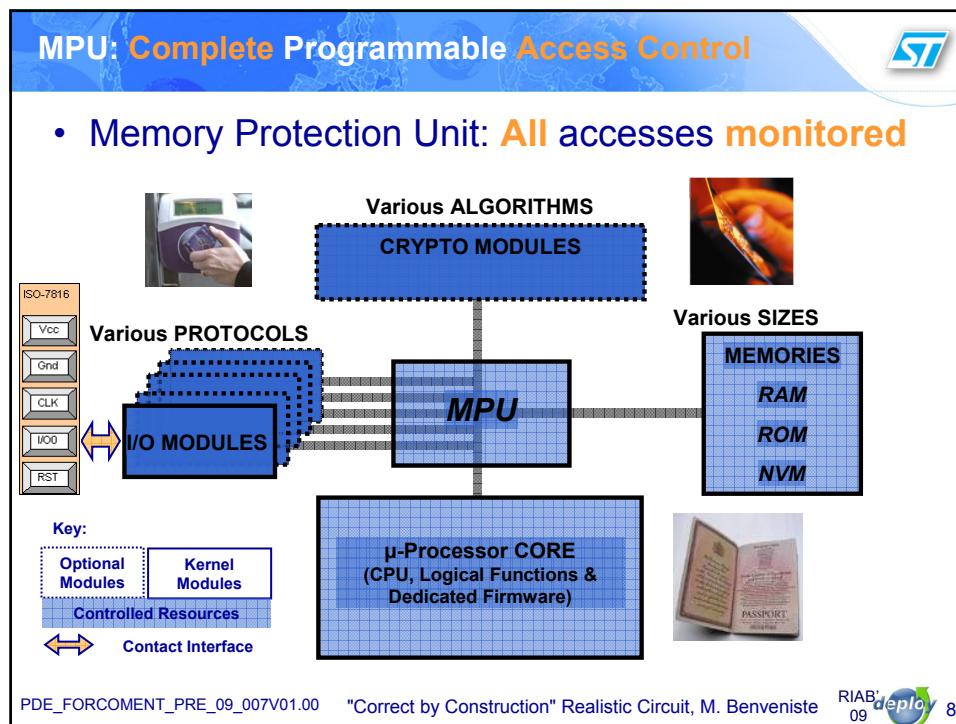
- ST23 Memory Protection Unit at a Glance
- Traditional Design Flow
- Experimental Design Flow
- Main Construction Steps
- Traditional versus Experimental
- Limitations & Ways Forward

PDE\_FORCOMENT\_PRE\_09\_007V01.00 "Correct by Construction" Realistic Circuit, M. Benveniste RIAB'09 

**MPU: Complete Programmable Access Control**

**ST**

- Memory Protection Unit: All accesses monitored



Key:

- Optional Modules
- Kernel Modules
- Controlled Resources
- Contact Interface

PDE\_FORCOMENT\_PRE\_09\_007V01.00 "Correct by Construction" Realistic Circuit, M. Benveniste RIAB'09 

## MPU - Overview

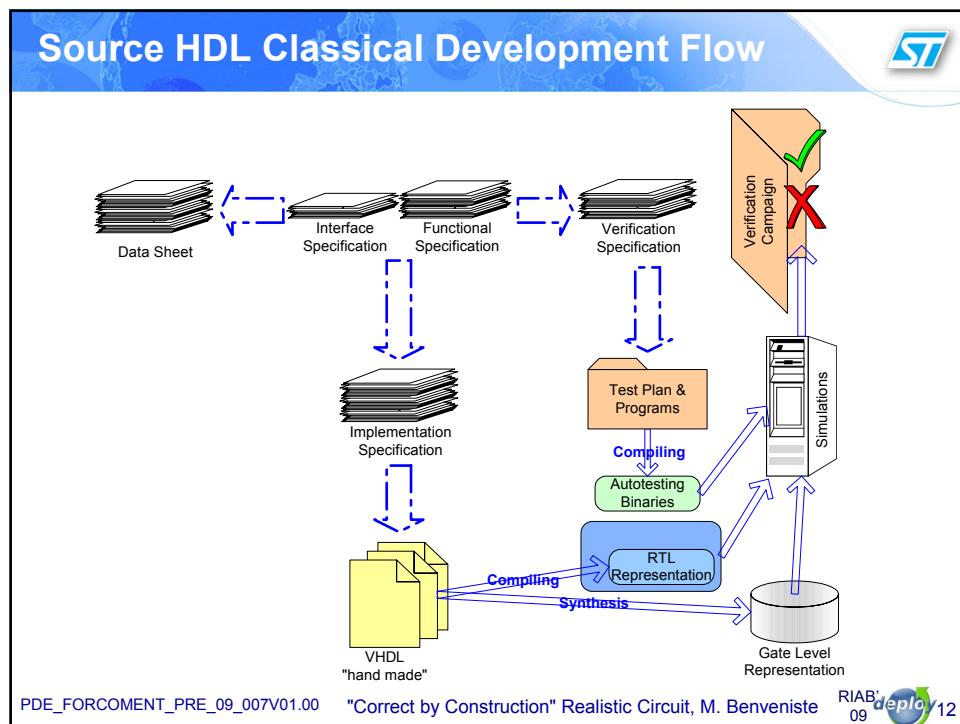
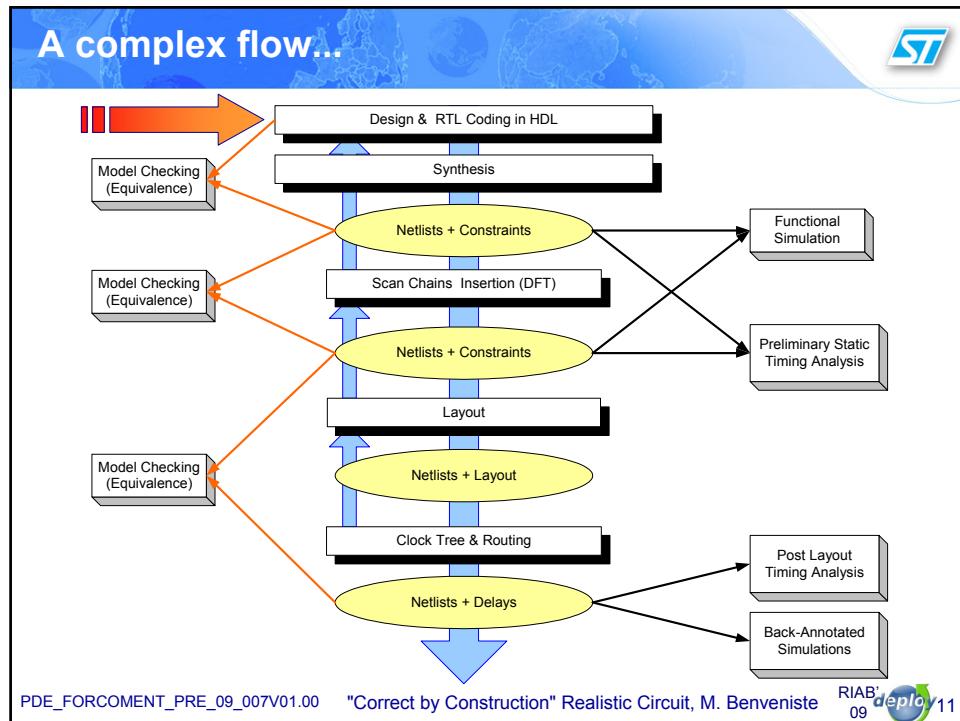
- **Segment:** addressable window in memory, **defined by**
  - Start / End addresses
  - A clearance level
  - Access rights (Read, Write, eXecute)
  - Active status (mapped, not mapped)
- **Clearance level:** privilege level of a program
  - A value in [Supervisor .. Public] (actually [0 .. 3])
  - Each segment is given a clearance level
  - Read & write access to **peripheral registers** are globally denied/granted for each clearance level
  - Program **clearance change** control is enabled/disabled for each clearance level (call gates)
- Access control principles: code (eXecute) & data (Read/Write) controls
  - A program can enforce clearance change control based on **current** and **previous** program clearance levels
  - All needed **data** for a given program must be located in its own **clearance** (or **Public** data) segments

PDE\_FORCOMENT\_PRE\_09\_007V01.00 "Correct by Construction" Realistic Circuit, M. Benveniste RIAB'09 deploy 9

## Correct by Construction Chip Functionality: An advanced R&D feasibility study report

- ST23 Memory Protection Unit at a Glance
- **Traditional Design Flow**
- Experimental Design Flow
- Main Construction Steps
- Traditional versus Experimental
- Limitations & Ways Forward

PDE\_FORCOMENT\_PRE\_09\_007V01.00 "Correct by Construction" Realistic Circuit, M. Benveniste RIAB'09 deploy 10

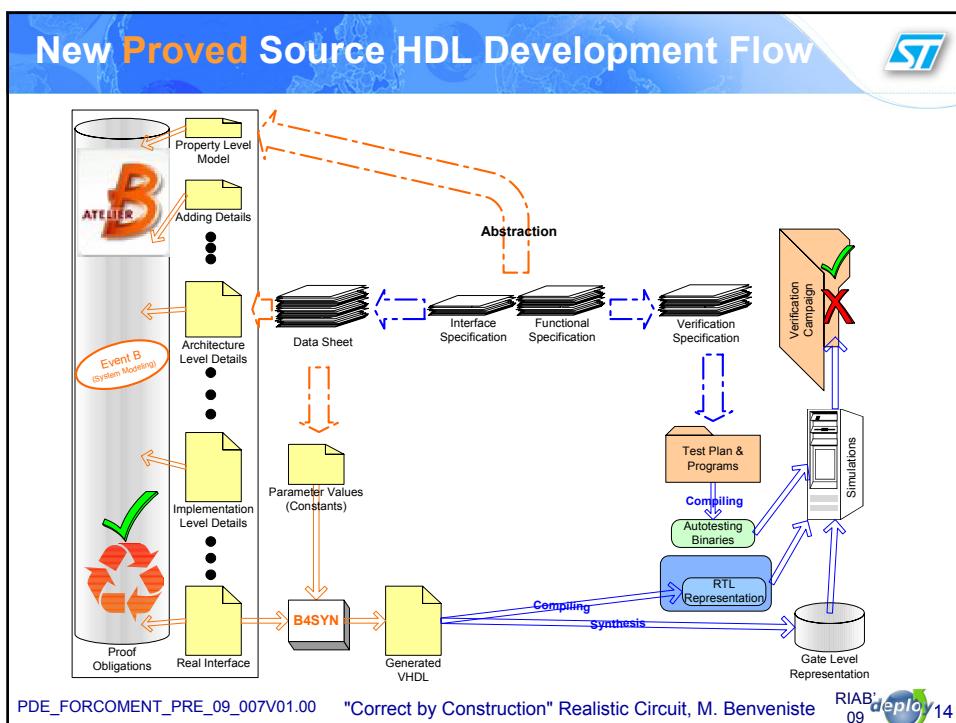


**Correct by Construction Chip Functionality:  
An advanced R&D feasibility study report**

ST

- ST23 Memory Protection Unit at a Glance
- Traditional Design Flow
- **Experimental Design Flow**
- Main Construction Steps
- Traditional versus Experimental
- Limitations & Ways Forward

PDE\_FORCOMENT\_PRE\_09\_007V01.00 "Correct by Construction" Realistic Circuit, M. Benveniste RIAB'09 deploy'13



**Correct by Construction Chip Functionality:  
An advanced R&D feasibility study report**

ST

- ST23 Memory Protection Unit at a Glance
- Traditional Design Flow
- Experimental Design Flow
- **Main Construction Steps**
- Traditional versus Experimental
- Limitations & Ways Forward

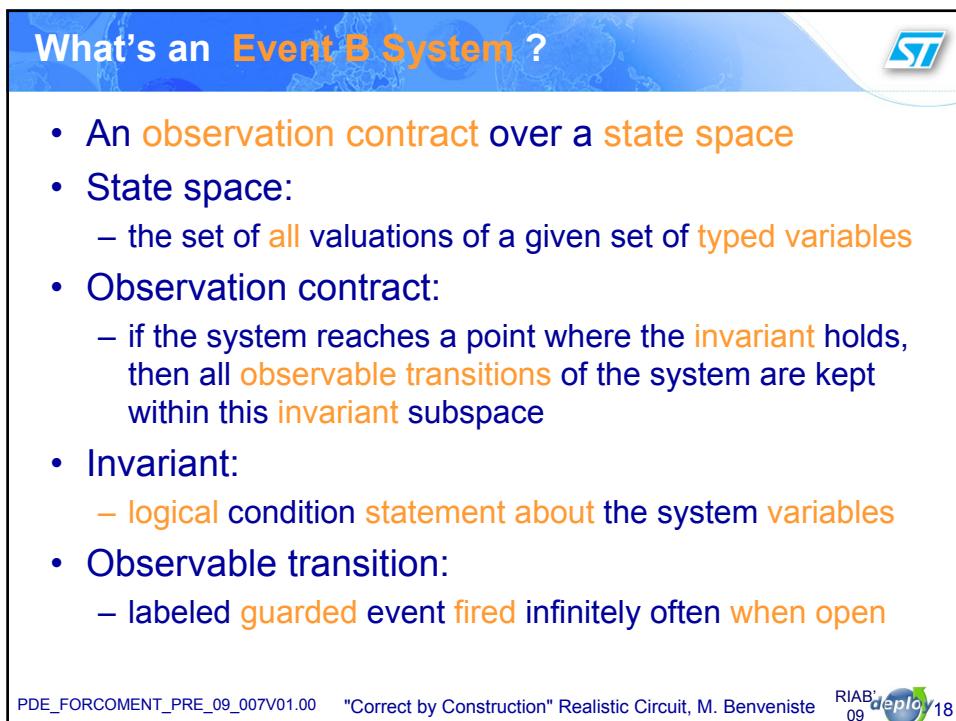
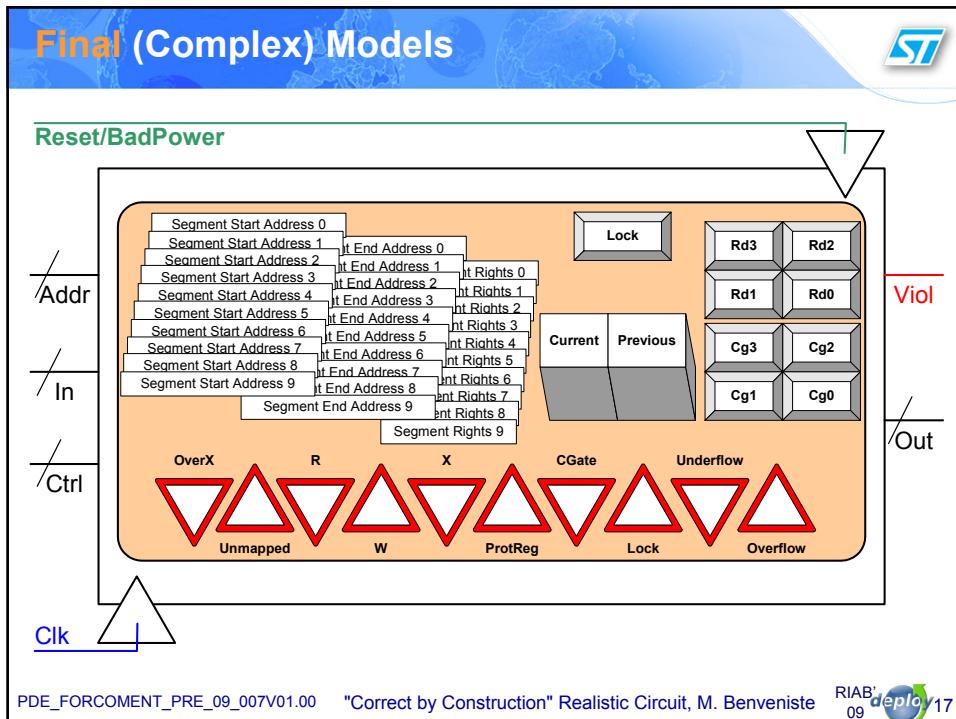
PDE\_FORCOMENT\_PRE\_09\_007V01.00 "Correct by Construction" Realistic Circuit, M. Benveniste RIAB'09 deploy'15

**Initial (Simple) Models**

ST

The diagram illustrates a simple memory model. On the left, a memory controller labeled **c0** contains a register **r0** with a 4x4 matrix of bits. The columns are labeled **a**, **c**, **d**, and **t**. The rows are labeled with colons. Inputs **a0**, **d0**, and **t0** feed into the controller. A red output line **v0** is shown. On the right, a state transition graph shows three states: **m0=0** (yellow), **m0=1** (green), and **m0=2** (light blue). Transitions are labeled **RESET/POR**, **ACCESS**, and **PSI**. The **RESET/POR** transition leads from **m0=0** to **m0=1**. The **ACCESS** transition leads from **m0=0** to **m0=2**. The **PSI** transition leads from **m0=1** back to **m0=0**.

PDE\_FORCOMENT\_PRE\_09\_007V01.00 "Correct by Construction" Realistic Circuit, M. Benveniste RIAB'09 deploy'16



## What's an Event B Refinement ?

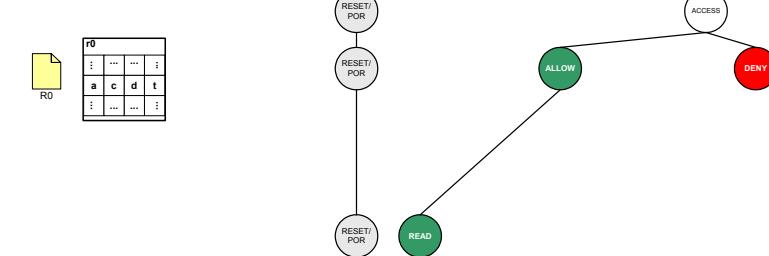
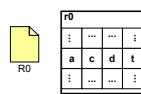
- A change of observation space preserving bound contracts
- State Space usually expands as the represented system becomes more precisely defined
- Observable transitions can be split or joined according to description needs:
  - stretching observation or folding behaviors, for instance
- If “allow” refines “access”, then:
  - “allow” occurs at most as often as “access”  
(guard strengthening)
  - “allow” preserves the expanded invariant  
(everlasting contract)
  - “allow” doesn’t do something “access” would not do  
(no contradiction)

PDE\_FORCOMENT\_PRE\_09\_007V01.00   "Correct by Construction" Realistic Circuit, M. Benveniste   RIAB'09 

## Refining State & Behavior in sync... (1/6)

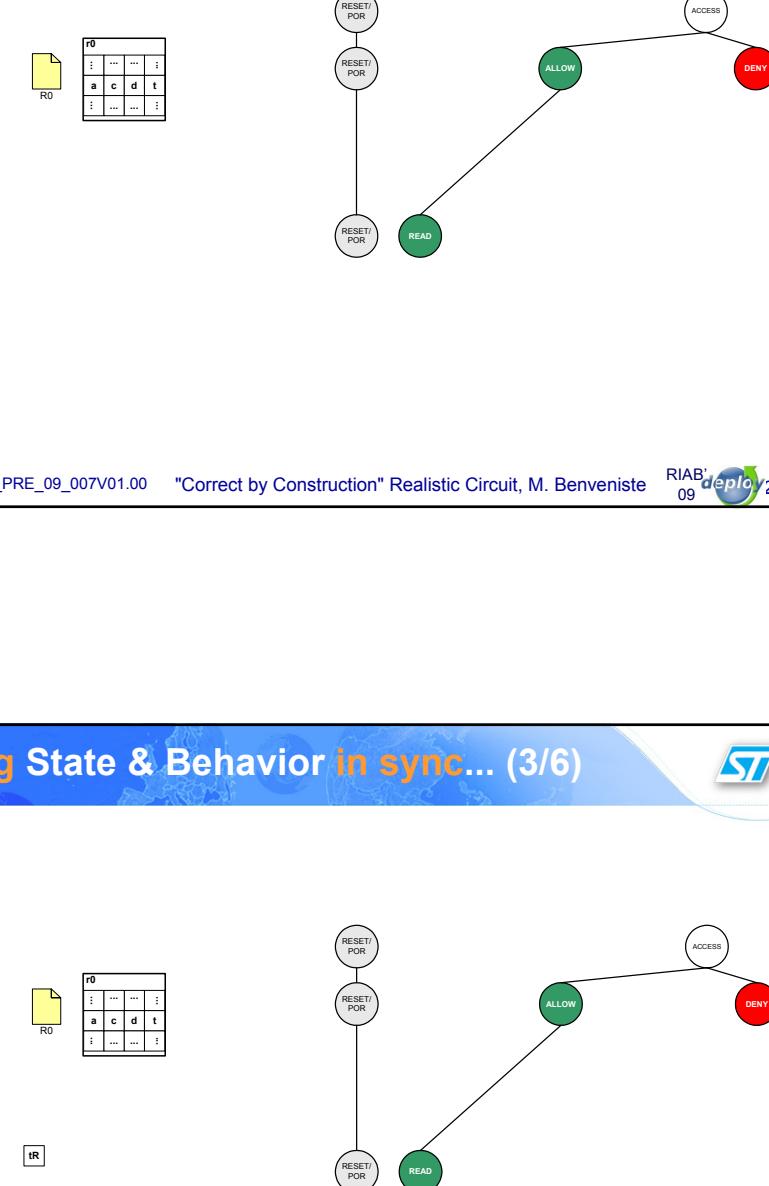
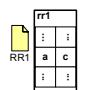
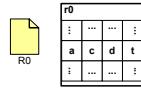
PDE\_FORCOMENT\_PRE\_09\_007V01.00   "Correct by Construction" Realistic Circuit, M. Benveniste   RIAB'09 

## Refining State & Behavior in sync... (2/6)



PDE\_FORCOMENT\_PRE\_09\_007V01.00 "Correct by Construction" Realistic Circuit, M. Benveniste RIAB'09

## Refining State & Behavior in sync... (3/6)



Let's take a closer look at this event...

PDE\_FORCOMENT\_PRE\_09\_007V01.00 "Correct by Construction" Realistic Circuit, M. Benveniste RIAB'09

### Refining State & Behavior in sync... (3/6)

**REFINEMENT**

```

mpu02
...
EVENTS
...
; read
ref allow
=
SELECT
  m0 = 2
  & t0 = TyR
  & a0 |-> c0 : rr1
THEN
  m0 := 0
  || v0 := FALSE
END

```

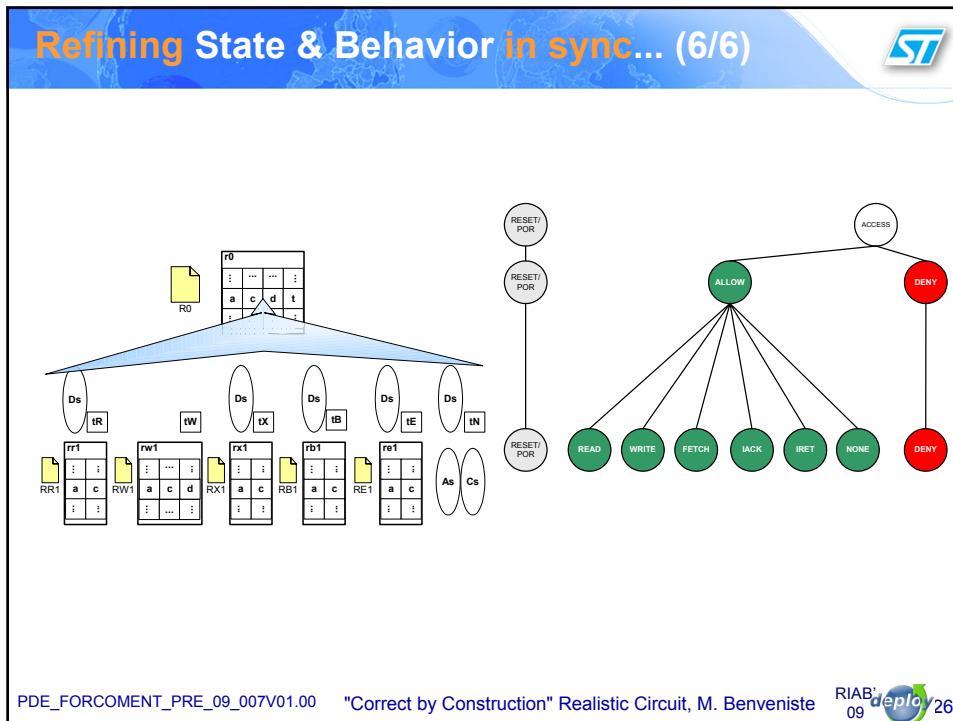
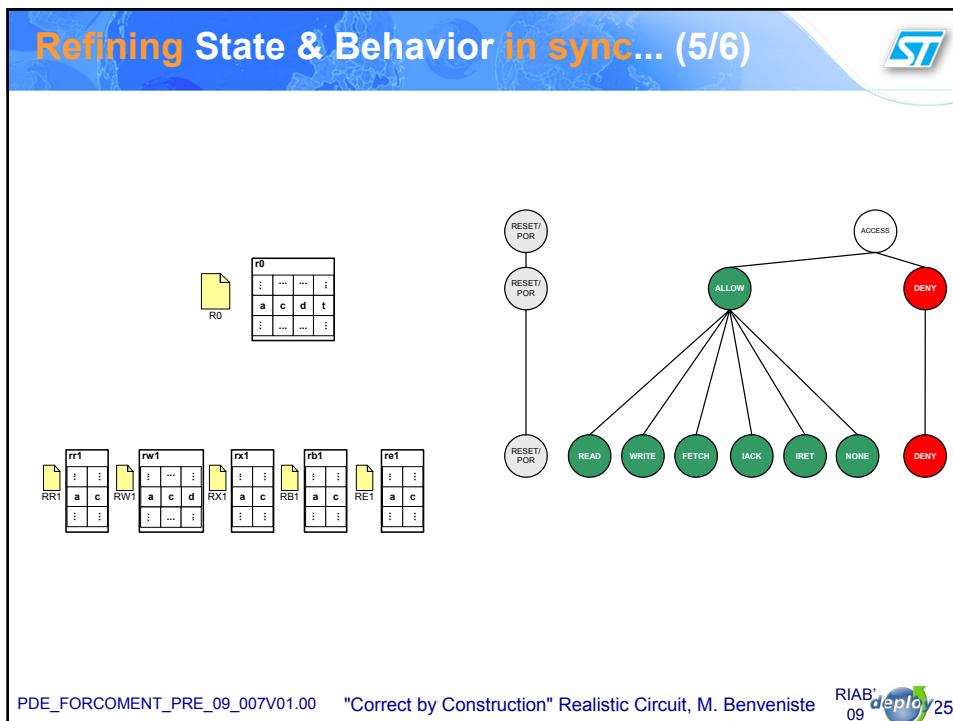
The diagram illustrates the refinement of a memory access. It shows two memory states: **r0** and **rr1**. **r0** contains data [a, b, c, d, e, f, g, h]. **rr1** contains data [a, b, c, d, e, f, g, h]. A yellow document icon labeled **R0** points to **r0**. A blue document icon labeled **rr1** points to **rr1**. An **IR** icon is also present. On the right, a state transition graph shows an **ACCESS** state branching to **ALLOW** (green circle) or **DENY** (red circle). A dotted arrow connects the **ref allow** event to this graph.

PDE\_FORCOMENT\_PRE\_09\_007V01.00 "Correct by Construction" Realistic Circuit, M. Benveniste RIAB'09 deploy'23

### Refining State & Behavior in sync... (4/6)

The diagram continues the refinement process. It shows the same memory states **r0** and **rr1**, and the same access control flow. A blue arrow highlights the **READ** state in the state transition graph. The graph shows **RESET/POR** leading to **READ**, which then leads to **ALLOW** (green circle) or **DENY** (red circle).

PDE\_FORCOMENT\_PRE\_09\_007V01.00 "Correct by Construction" Realistic Circuit, M. Benveniste RIAB'09 deploy'24



### Let's Refine

```

SYSTEM
  mpu00
  ...
EVENTS
  ...
; access =
SELECT
  m0 = 2
THEN
  m0 := 0
END

```

```

REFINES mpu00
...
; allow ref access =
SELECT
  m0 = 2
& a0 |-> c0 |-> d0 |-> t0 : r0
THEN
  m0, v0 := 0, FALSE
|| c0 :: CLs
|| r0 :: ADs * CLs * BYs <-> TYs
END

; deny ref access =
SELECT
  m0 = 2
& a0 |-> c0 |-> d0 |-> t0 /: r0
THEN
  m0, v0 := 0, TRUE
END

```

PDE\_FORCOMENT\_PRE\_09\_007V01.00 "Correct by Construction" Realistic Circuit, M. Benveniste RIAB'09 deploy 27

### “allow” Refines “access”

```

SYSTEM
  mpu00
  ...
EVENTS
  ...
; access =
SELECT
  m0 = 2
THEN
  m0 := 0
END

```

```

REFINES mpu00
...
; allow ref access =
SELECT
  m0 = 2
& a0 |-> c0 |-> d0 |-> t0 : r0
THEN
  m0, v0 := 0, FALSE
|| c0 :: CLs
|| r0 :: ADs * CLs * BYs <-> TYs
END

; deny ref access =
SELECT
  m0 = 2
& a0 |-> c0 |-> d0 |-> t0 /: r0
THEN
  m0, v0 := 0, TRUE
END

```

PDE\_FORCOMENT\_PRE\_09\_007V01.00 "Correct by Construction" Realistic Circuit, M. Benveniste RIAB'09 deploy 28

**“deny” Refines “access”**

```

SYSTEM
  mpu00
  ...
EVENTS
  ...
; access =
SELECT
  m0 = 2
THEN
  m0 := 0
END

```

≡

```

REFINES mpu00
...
; allow ref access =
SELECT
  m0 = 2
  & a0 |-> c0 |-> d0 |-> t0 : r0
THEN
  m0, v0 := 0, FALSE
  || c0 :: CLs
  || r0 :: ADs * CLs * BYs <-> TYs
END

; deny ref access =
SELECT
  m0 = 2
  & a0 |-> c0 |-> d0 |-> t0 /: r0
THEN
  m0, v0 := 0, TRUE
END

```

PDE\_FORCOMENT\_PRE\_09\_007V01.00 "Correct by Construction" Realistic Circuit, M. Benveniste RIAB'09 deploy 29

**Refinement is not enough...**

```

SYSTEM
  mpu00
  ...
EVENTS
  ...
; access =
SELECT
  m0 = 2
THEN
  m0 := 0
END

```

≡

```

REFINES mpu00
...
; allow ref access =
SELECT
  m0 = 2
  & a0 |-> c0 |-> d0 |-> t0 : r0
THEN
  m0, v0 := 0, FALSE
  || c0 :: CLs
  || r0 :: ADs * CLs * BYs <-> TYs
END

; deny ref access =
SELECT
  m0 = 2
  & a0 |-> c0 |-> d0 |-> t0 /: r0
THEN
  m0, v0 := 0, TRUE
END

```

```

m0 = 2 &
not( a0 |-> c0 |-> d0 |-> t0: r0 ) &
m0 = 2 &
a0 |-> c0 |-> d0 |-> t0: r0 &
" `Check refinement exclusivity --companion model` "
=>
bfalse

```

PDE\_FORCOMENT\_PRE\_09\_007V01.00 "Correct by Construction" Realistic Circuit, M. Benveniste RIAB'09 deploy 30

**...exclusive refinement is still not enough...**

```

SYSTEM
  mpu
  ...
EVENTS
  ...
; access =
SELECT
  m0 = 2
THEN
  m0 := 0
END

```

```

REFINES mpu
...
; allow ref access =
SELECT
  m0 = 2
& a0 |-> c0 |-> d0 |-> t0 : r0
THEN
  m0, v0 := 0, FALSE
|| c0 :: CLs
|| r0 :: ADs * CLs * BYs <-> TYs
END

; deny ref access =
SELECT
  m0 = 2
& a0 |-> c0 |-> d0 |-> t0 /: r0
THEN
  m0, v0 := 0, TRUE
END

```

```

m0 = 2 &
not( m0 = 2 & not( a0|-> c0|-> d0|-> t0: r0 ) ) &
"Check refinement liveness - companion model"
=>
a0 |-> c0 |-> d0 |-> t0: r0

```

PDE\_FORCOMENT\_PRE\_09\_007V01.00 "Correct by Construction" Realistic Circuit, M. Benveniste RIAB'09 deploy31

**...now we can be confident it's all there...**

```

SYSTEM
  mpu00
  ...
EVENTS
  ...
; access =
SELECT
  m0 = 2
THEN
  m0 := 0
END

```

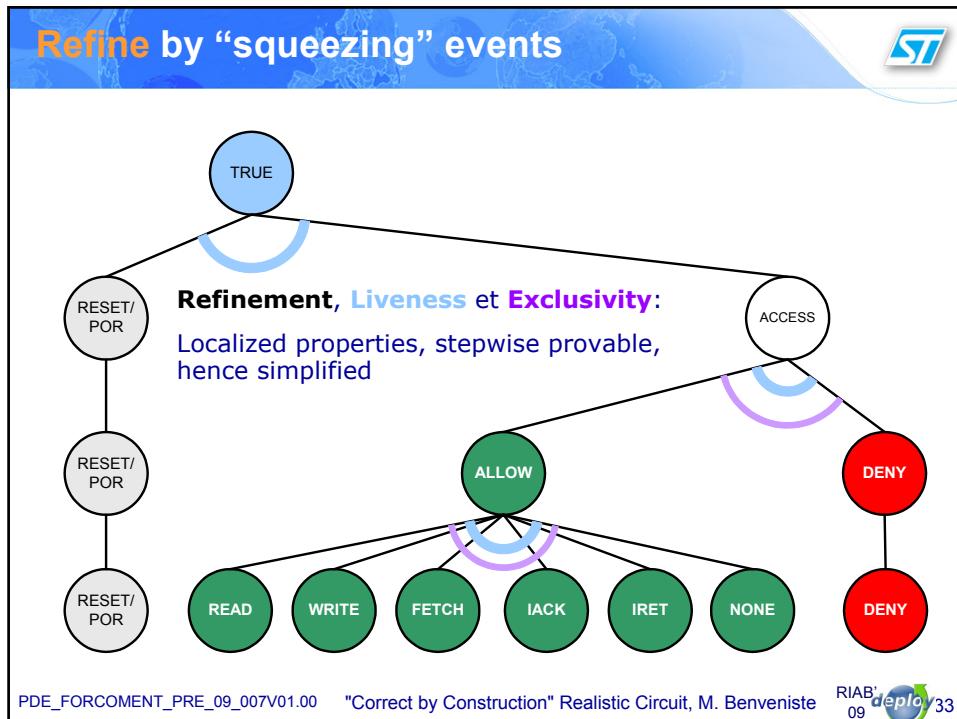
```

REFINES mpu00
...
; allow ref access =
SELECT
  m0 = 2
& a0 |-> c0 |-> d0 |-> t0 : r0
THEN
  m0, v0 := 0, FALSE
|| c0 :: CLs
|| r0 :: ADs * CLs * BYs <-> TYs
END

; deny ref access =
SELECT
  m0 = 2
& a0 |-> c0 |-> d0 |-> t0 /: r0
THEN
  m0, v0 := 0, TRUE
END

```

PDE\_FORCOMENT\_PRE\_09\_007V01.00 "Correct by Construction" Realistic Circuit, M. Benveniste RIAB'09 deploy32



**The Refinement Plan (1/3)**

N°	Step	Main Purpose
1	Host_1	Host execution model
2	Complete Policy	Abstract complete access policy
3	Split Access	Rights matrix split for each access type Allow cases split by access type
4	Exceptions	By-passing checks automata Interrupts & reset management
5	Split Deny	Deny cases split by access type Clearances stack introduced (interrupts)
6	Registers_1	Registers access policy (mem. vs. reg.) Supervisor clearance introduced

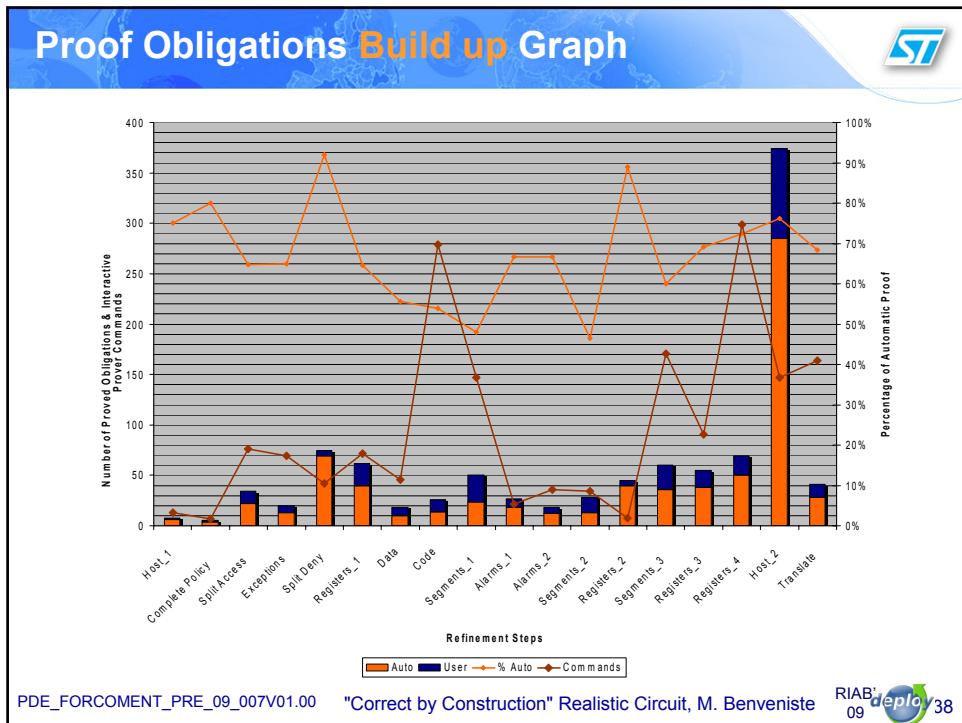
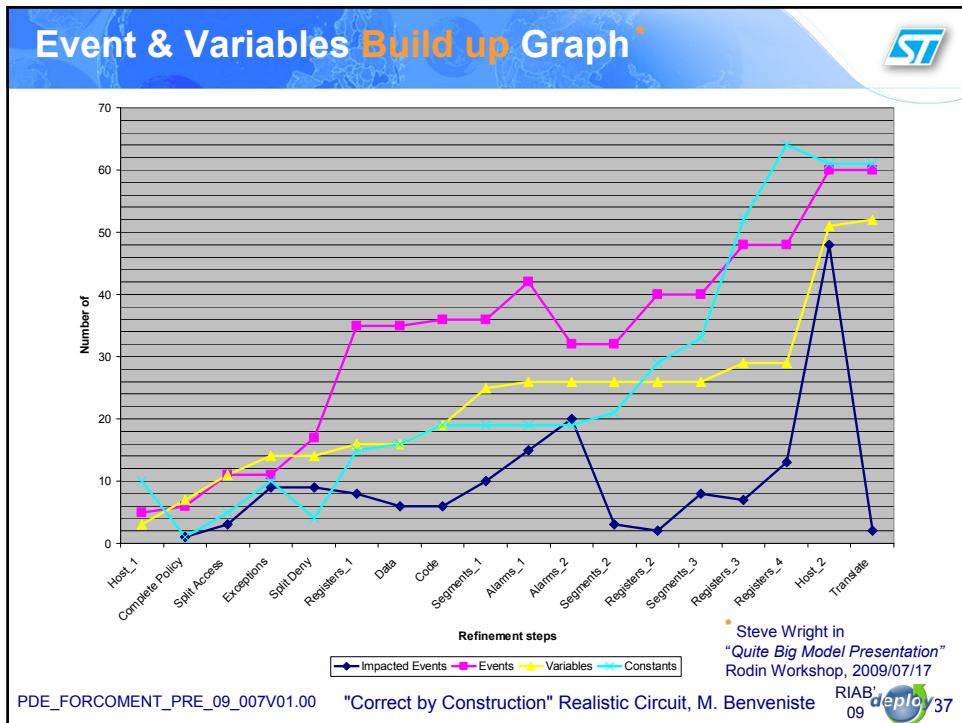
PDE\_FORCOMENT\_PRE\_09\_007V01.00   "Correct by Construction" Realistic Circuit, M. Benveniste   RIAB'09 deploy'34

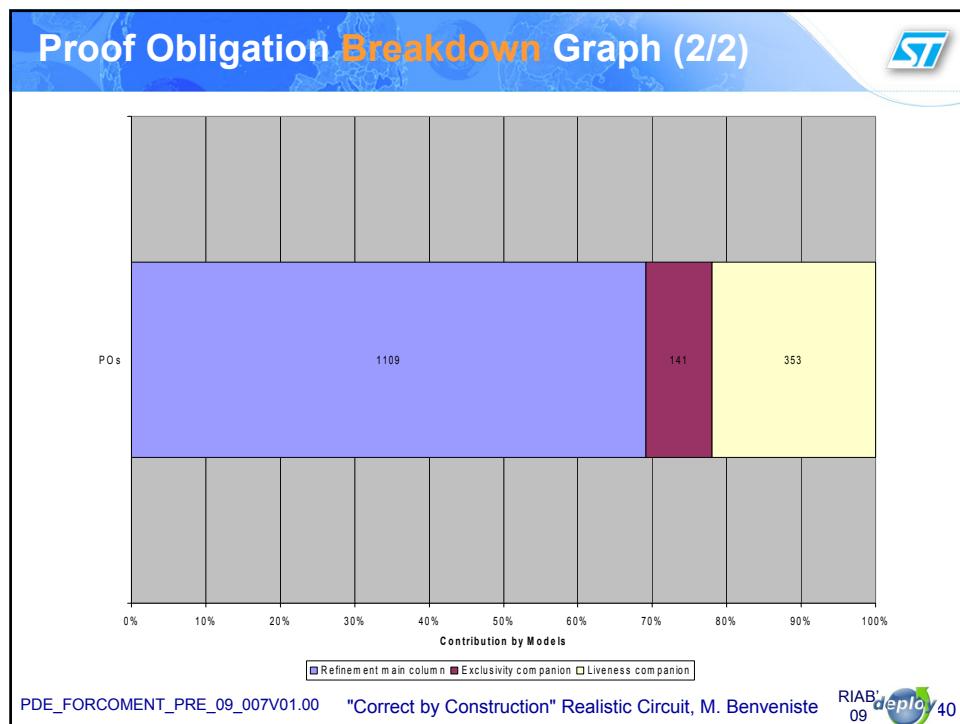
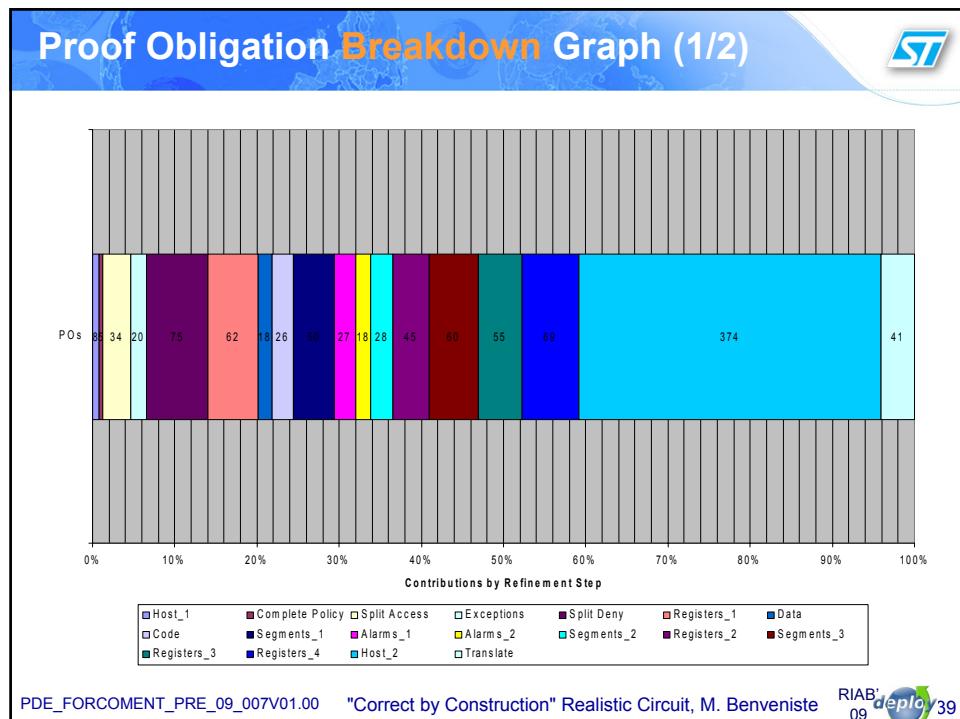
The Refinement Plan (2/3)		
N°	Step	Main Purpose
7	Data	Data access policy Public clearance introduced
8	Code	Code access policy, Call gates introduced
9	Segments_1	Segments as sets of addresses Constructive set expressions defined
10	Alarms_1	Identification of denied accesses Alarm bits introduced
11	Alarms_2	Denied access cases grouped by alarm
12	Segments_2	Segments as address ranges (start & end) Mapped segment bit introduced
13	Registers_2	MPU register access policy Their symbolic addresses introduced

PDE\_FORCOMENT\_PRE\_09\_007V01.00 "Correct by Construction" Realistic Circuit, M. Benveniste RIAB 09 deploy 35

The Refinement Plan (3/3)		
N°	Step	Main Purpose
14	Segments_3	Segments granularity Implementation optimization
15	Registers_3	MPU registers effective read, Output defined Constant read access functions Symbolic addresses are bytes now
16	Registers_4	Effective write of MPU registers Constant write access functions
17	Host_2	Physical interface for meaning (access type) All input cases covered, sampling on "tick"
18	Translate	Expression simplifications for VHDL Prop. not translated, types drive translator

PDE\_FORCOMENT\_PRE\_09\_007V01.00 "Correct by Construction" Realistic Circuit, M. Benveniste RIAB 09 deploy 36





## Observations on resulting implementation

- Built static structure is quite complex  
~60 constants, ~50 variables  
Just imagine if verification had to start at this (RTL) level !  
What would you verify ?
- A lot of individual cases  
56 events
- Although very simple cases  
~12 lines each
- Built with proved exhaustive assurance of:
  - Correctness: no contradiction regarding all specified behaviors
  - Determinism: no overlapping specified behaviors
  - Completeness preservation: no development holes

PDE\_FORCOMENT\_PRE\_09\_007V01.00 "Correct by Construction" Realistic Circuit, M. Benveniste RIAB'09 deploy41

## Correct by Construction Chip Functionality: An advanced R&D feasibility study report

- ST23 Memory Protection Unit at a Glance
- Traditional Design Flow
- Experimental Design Flow
- Main Construction Steps
- Traditional versus Experimental
- Limitations & Ways Forward

PDE\_FORCOMENT\_PRE\_09\_007V01.00 "Correct by Construction" Realistic Circuit, M. Benveniste RIAB'09 deploy42

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

PDE\_FORCOMENT\_PRE\_09\_007V01.00 "Correct by Construction" Realistic Circuit, M. Benveniste RIAB'09 deploy 43

Correct by Construction Chip Functionality: An advanced R&D feasibility study report
<ul style="list-style-type: none"> <li>• ST23 Memory Protection Unit at a Glance</li> <li>• Traditional Design Flow</li> <li>• Experimental Design Flow</li> <li>• Main Construction Steps</li> <li>• Traditional versus Experimental</li> <li>• Limitations &amp; Ways Forward</li> </ul>

PDE\_FORCOMENT\_PRE\_09\_007V01.00 "Correct by Construction" Realistic Circuit, M. Benveniste RIAB'09 deploy 44

## Benefits, Drawbacks & Future work

- Benefits
  - Zero bug macros become feasible
  - Highly parameterized coding is encouraged
  - Focus can safely turn onto security concerns
- Drawbacks
  - No composition mechanism to assemble units
  - Not yet ready for industry (both method & tool)
- Future work
  - Extend to other case studies
  - Propose language support enhancements

PDE\_FORCOMENT\_PRE\_09\_007V01.00 "Correct by Construction" Realistic Circuit, M. Benveniste RIAB'09 deploy45

## Credits & Acknowledgement

The FORmal CO-developMENt Project

**B Models :** L. Mussat, Clearsy  
**B4SYN Translator:** T. Lecomte & A. Requet, Clearsy  
**Screenplay, Direction & Realization :** M. Benveniste, STMicroelectronics  
**Support Design :** D. Chomaud, STMicroelectronics  
**Administration :** R. Petri, STMicroelectronics, J.P. Pitzalis, Clearsy  
**Production :** 4<sup>th</sup> et 5<sup>th</sup> Conventions PACA Regional Council - STMicroelectronics - Clearsy

Please Read Carefully:

Information in this document is provided solely in connection with ST products. STMicroelectronics NV and its subsidiaries ("ST") reserve the right to make changes, corrections, modifications or improvements, to this document, and the products and services described herein at any time, without notice. All ST products are sold pursuant to ST's terms and conditions of sale. Purchasers are solely responsible for the choice, selection and use of the ST products and services described herein, and ST assumes no liability whatsoever relating to the choice, selection or use of the ST products and services described herein. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted under this document. If any part of this document refers to any third party products or services it shall not be deemed a license grant by ST for the use of such third party products or services, or any intellectual property contained therein or considered as a warranty covering the use in any manner whatsoever of such third party products or services or any intellectual property contained therein.

UNLESS OTHERWISE SET FORTH IN ST'S TERMS AND CONDITIONS OF SALE ST DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY WITH RESPECT TO THE USE AND/OR SALE OF ST PRODUCTS INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE (AND THEIR EQUIVALENTS UNDER THE LAWS OF ANY JURISDICTION), OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. UNLESS EXPRESSLY APPROVED IN WRITING BY AN AUTHORIZED ST REPRESENTATIVE, ST PRODUCTS ARE NOT RECOMMENDED, AUTHORIZED OR WARRANTED FOR USE IN MILITARY, AIR CRAFT, SPACE, LIFE SAVING, OR LIFE SUSTAINING APPLICATIONS, NOR IN PRODUCTS OR SYSTEMS WHERE FAILURE OR MALFUNCTION MAY RESULT IN PERSONAL INJURY, DEATH, OR SEVERE PROPERTY OR ENVIRONMENTAL DAMAGE. ST PRODUCTS WHICH ARE NOT SPECIFIED AS "AUTOMOTIVE GRADE" MAY ONLY BE USED IN AUTOMOTIVE APPLICATIONS AT USER'S OWN RISK.

Resale of ST products with provisions different from the statements and/or technical features set forth in this document shall immediately void any warranty granted by ST for the ST product or service described herein and shall not create or extend in any manner whatsoever, any liability of ST.

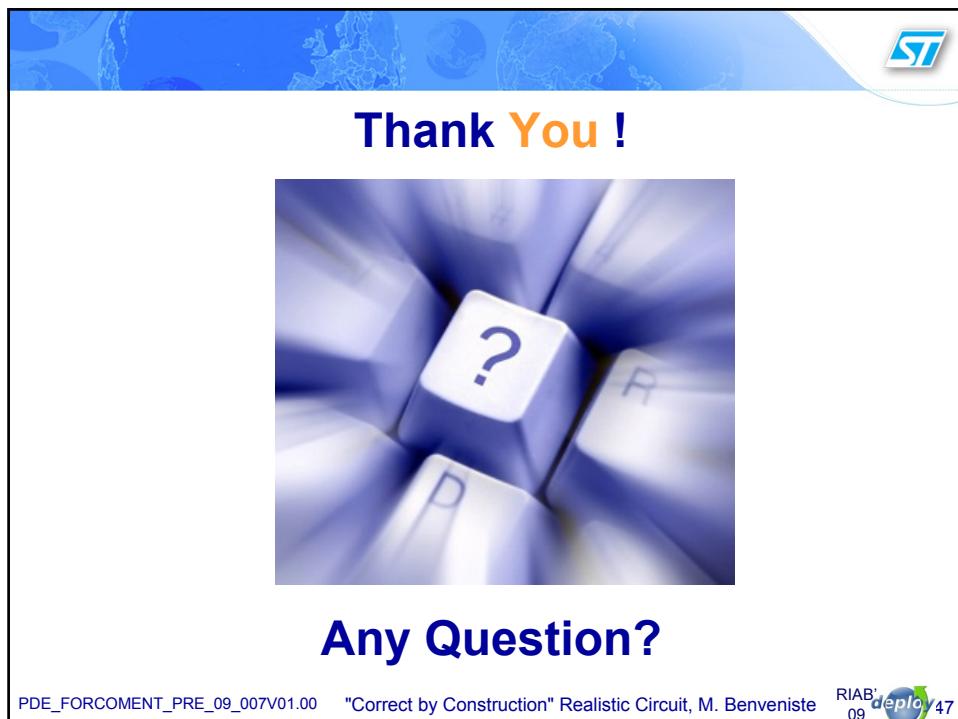
ST and the ST logo are trademarks or registered trademarks of ST in various countries. Information in this document supersedes and replaces all information previously supplied. The ST logo is a registered trademark of STMicroelectronics. All other names are the property of their respective owners.

© 2009 STMicroelectronics - All rights reserved

STMicroelectronics group of companies Australia - Belgium - Brazil - Canada - China - Czech Republic - Finland - France - Germany - Hong Kong - India - Israel - Italy - Japan - Malaysia - Malta - Morocco - Singapore - Sweden - Switzerland - United Kingdom - United States of America

www.st.com

PDE\_FORCOMENT\_PRE\_09\_007V01.00 "Correct by Construction" Realistic Circuit, M. Benveniste RIAB'09 deploy46



PDE\_FORCOMENT\_PRE\_09\_007V01.00 "Correct by Construction" Realistic Circuit, M. Benveniste RIAB'09 deploy47