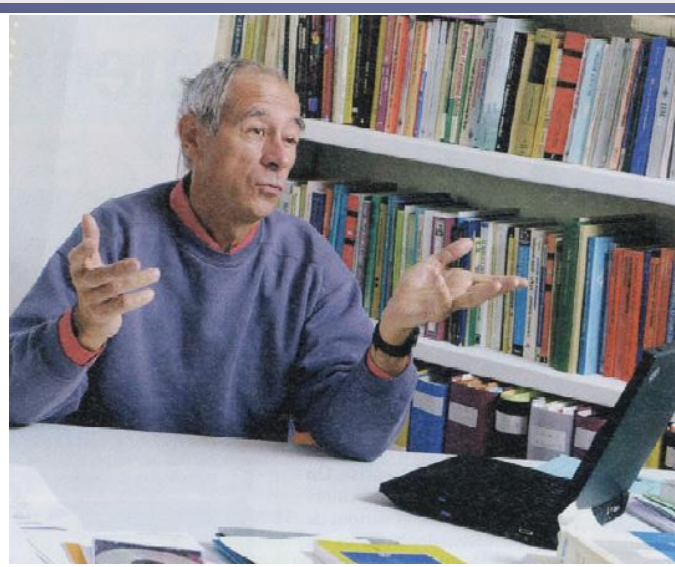
The Big Picture

Thierry Lecomte

thierry.lecomte@clearsy.com

A small history of B

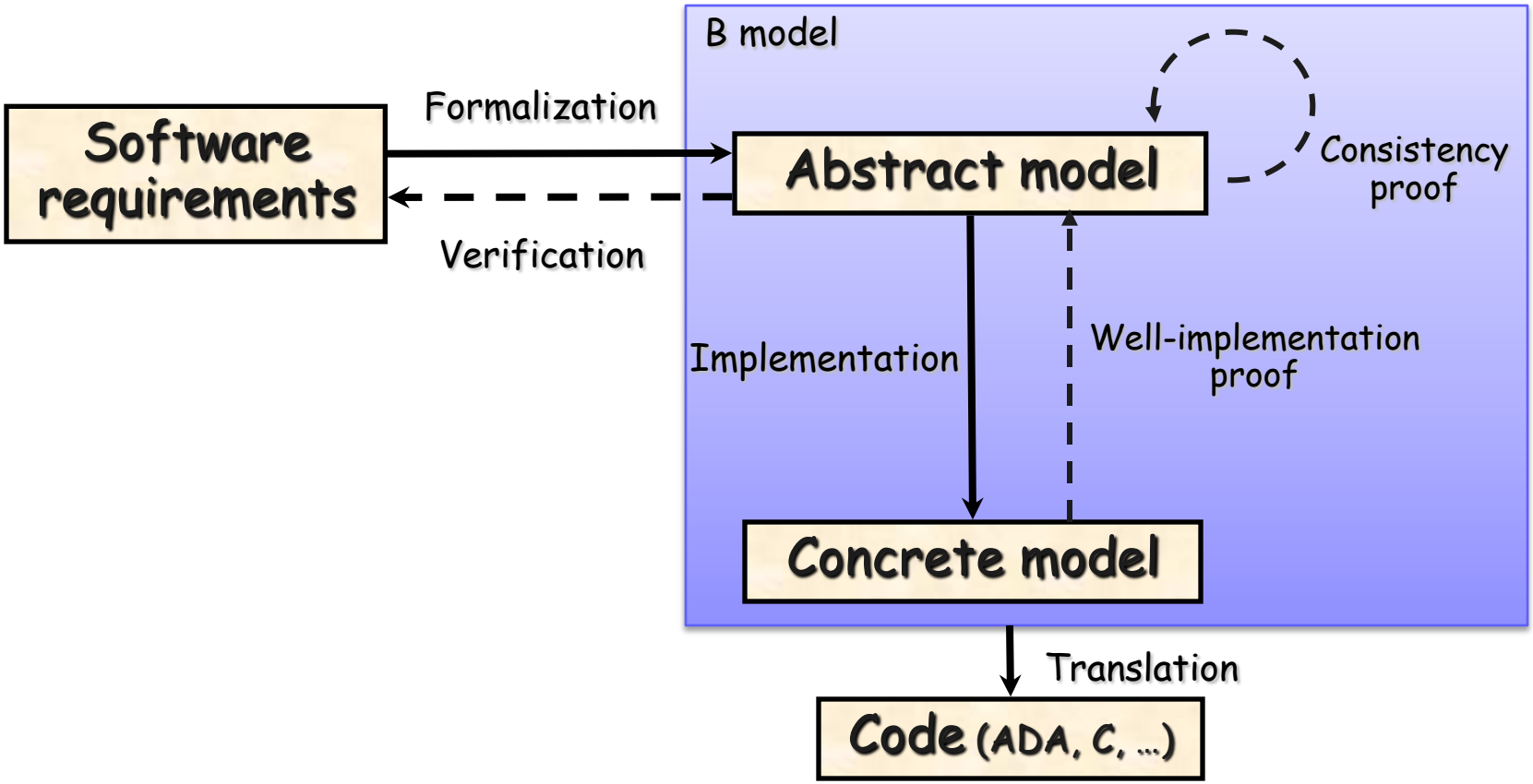
- Born and matured in the 90's
- Based on scientific results
  (Dijkstra, Hoare, Jones, Morgan, Jifeng)
- Features:
  - Abstract specification
  - Refinement
  - Implementable models proved to comply with specifications
- First tool:
  - Developped by Alstom (Mejia)
  - Aimed at safety critical software
  - Translation of models in Ada



Abrial, J.R.

Inventor of the B method

Intrinsics


B model
Software requirements
Formalization
Verification
Abstract model
Consistency proof
Implementation
Well-implementation proof
Concrete model
Translation
Code (ADA, C, ...)

Yet Another Formal Method

- It all started with a failure:
  - Metro Line D in Lyon (initiated in 1979)
  - The line is automated during the development of infrastructures
  - Difficulties to set up a proper Automatic Pilot (SACEM): budget, planning (completed in 1992)
  - RATP decided to go for B, for the first fully automated metro in Paris ….

B into industrial existence

- Support
  - Prototype tool strengthened through a 3M€ programme (RATP, French Railways, INRETS) over 5 years

- METEOR Line 14 (Paris)
  - Automatic refinement to come
  - Released in dec. 1998

- But turned out to be a real success:
  - 86 k loc software
  - still in v1.0 today, no bug detected so far

Some implementations (B)

To come:
- Istanbul
- Lyon
- New York (Flushing)

Metro L1
Paris

Metro L1
Algiers

SHUTTLE
ROISSY AIRPORT
Paris

Metro
L2 L3
Sao Paulo

Metro L
New York

Metro L3
Paris

Metro
Mexico

Metro L9
Seoul

Metro L9
Barcelona

Metro Airport Express
Hong Kong

Metro L2
Budapest

Metro
Toronto

Metro
Madrid

Metro L10
Beijing

Metro
Circle Line
Singapore

KVB
6000 trains
France

Metro
San Juan

Metro
L1 L2
Malaga

METEOR L14
Paris

Metro
Delhi

Metro
Lausanne

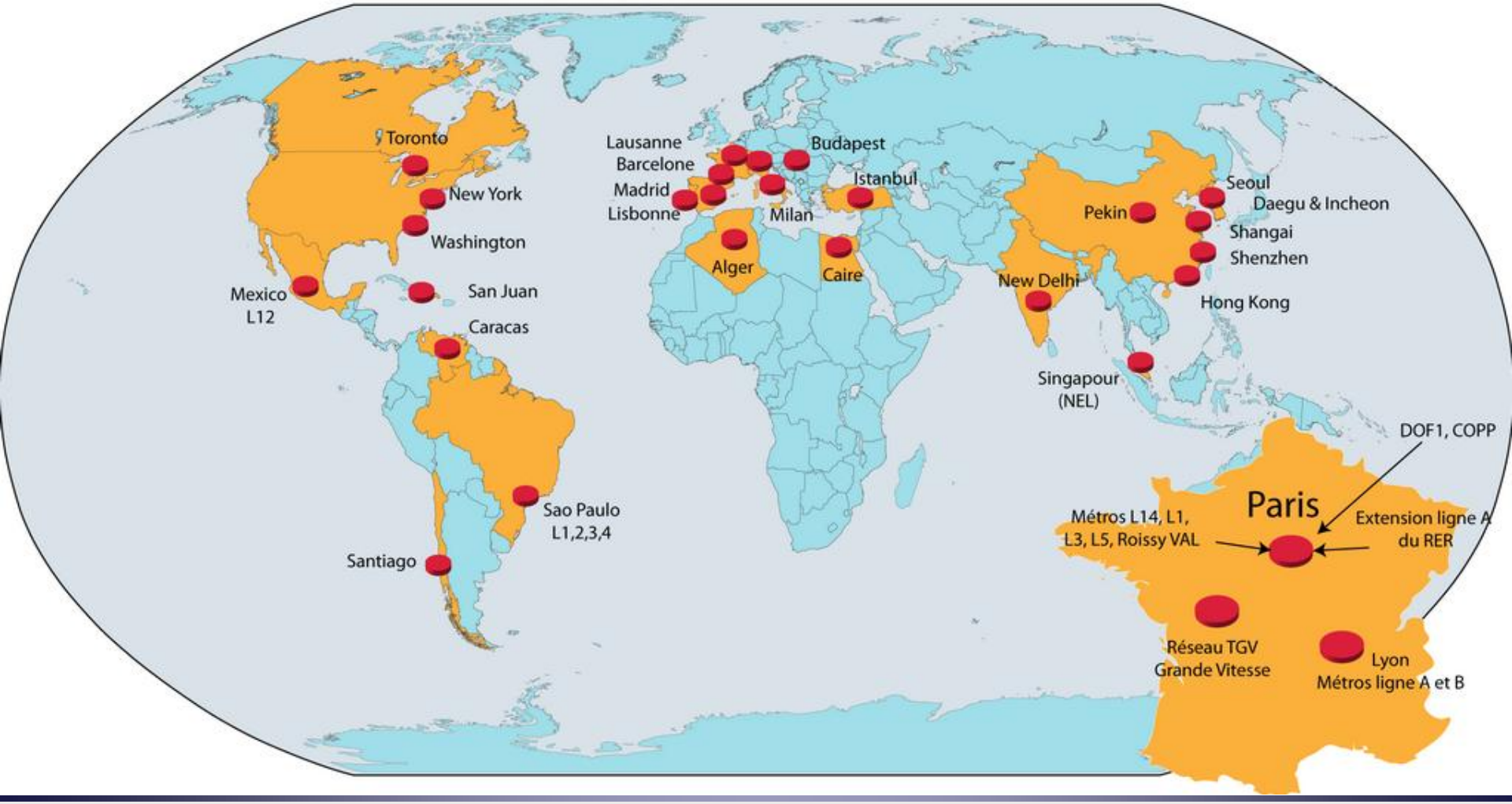
Metro L5
Milano

1990

2000

2010

Current picture: « B inside » metros



B for systems: the reasons

- 100% proved software is not a guaranty *per se*
  - Even if METEOR ATP is still in v1.0 in 2010
  - Ex: ATP reverse-engineered, from existing wired-logic systems to PLC
    - Not able to stop precisely at station
    - Software 100% proved but its specification was not the one that could make the train stopping

- METEOR a success because lot of energy spent at the system level

Event-B was born with the new century

- Building models for systems instead of software
- With events instead of operations/methods
- With one strong objective: to provide a system-level justification for a software specification
- Time for experimenting and researching ….

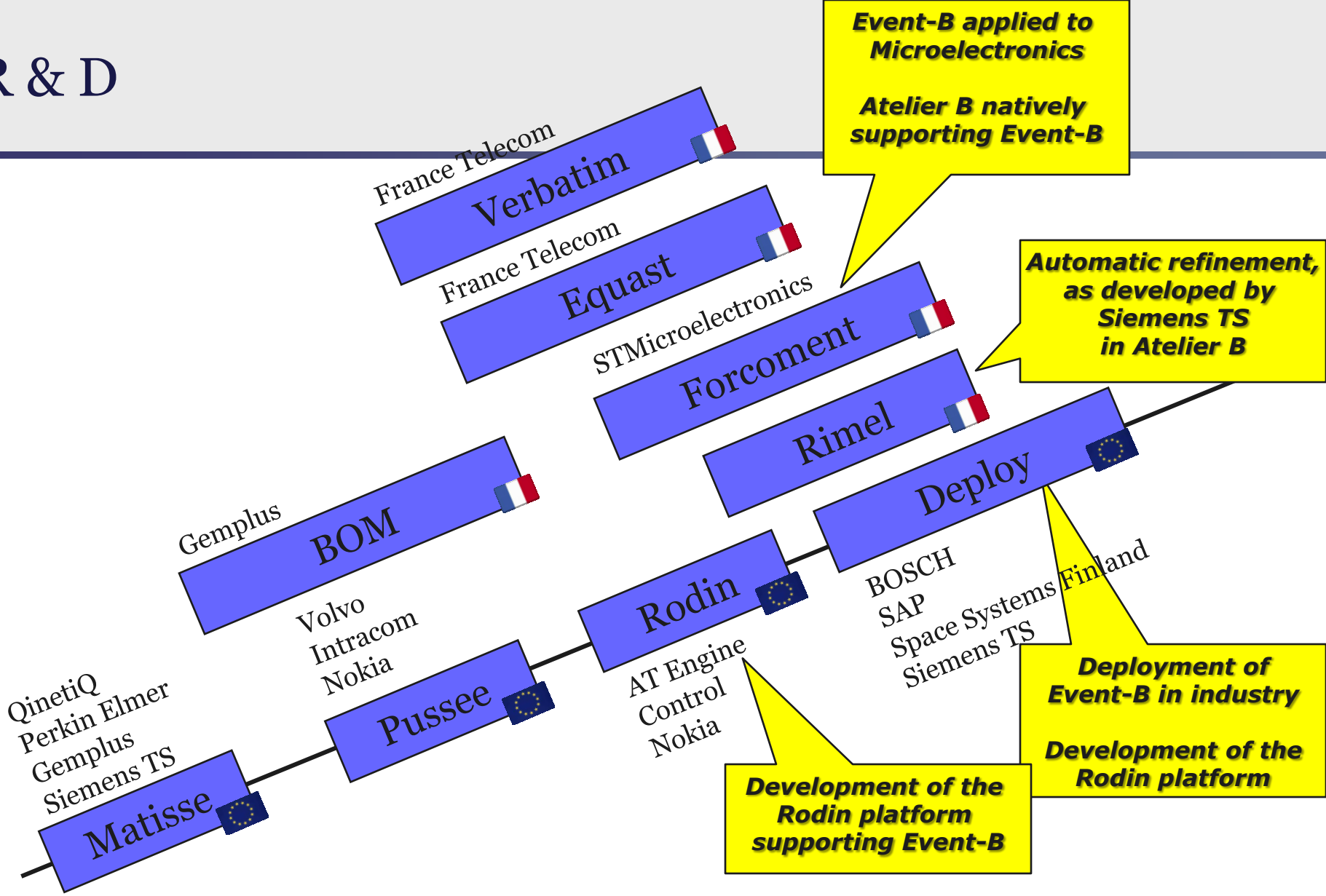
[Foundation papers:]

- J.R. Abrial, « *Extending B without changing it* », 1996
- J.-R. Abrial and L. Mussat, "Introducing Dynamic Constraints in B," 1998

Some 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)

R & D


Event-B applied to Microelectronics
Atelier B natively supporting Event-B
Automatic refinement, as developed by Siemens TS in Atelier B
Deployment of Event-B in industry
Development of the Rodin platform
Development of the Rodin platform supporting Event-B
France Telecom
Verbatim
France Telecom
Equast
STMicroelectronics
Forcoment
Rimel
Deploy
Gemplus
BOM
Volvo
Intracom
Nokia
Rodin
BOSCH
SAP
Space Systems Finland
Siemens TS
AT Engine Control
Nokia
Pussee
QinetiQ
Perkin Elmer
Gemplus
Siemens TS
Matisse

Some implementations (Event-B)

PSD L2 L3
Sao Paulo

Platform Screen Doors
Demonstrator
L13
Paris

PSD L1
Paris

Platform Screen Doors
L13
Paris

L13
Automatic Gap Filler
Paris

1998 **2000** **2002** **2004** **2006** **2008** **2010**

Metro L3
Cairo
2011 ?

Some implementations (microelectronics)

AT90SC12872RCFT	Low-power, high-performance, 8-/16-bit secure cryptocontroller with 128 Kbytes ROM and 72 Kbytes EEPROM. Security Features: OTP (One Time Programmable) EEPROM area, RNG (Random Number Generator), "out of bounds" detectors, side channel attack countermeasures. Hardware DES/TDES, 32-bit Cryptographic Accelerator, CRC, ISO 14443 Type B contactless interface and ISO 7816 contact interface, Common Criteria EAL5+ and EMVCo Certifications.

Secure microcontroler
ST19NA18
ST19NT66A
EAL5+
ST

Secure microcontroler
ST23YR80
SA23YR80
EAL5+
ST

Secure microcontrolers
ATS90SC6404
ATS90SC12872
EAL5+
Atmel

Secure microcontroler
ST23YL80
ST23YL18
EAL5+
ST

Secure microcontroler
ST19WR08
ST19WR66
ST19NR66
EAL5+
ST

Secure microcontrolers
ATS90SC12872R
ATS90SC12836R
EAL5+
Atmel

Microcircuits
ST19WP
ST19WL
EAL5+
ST

Secure microcontrolers
AT90SC20818
AT90SC13612
AT90SC24036
EAL5+
Atmel

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.

Microcircuit
ST22L128
EAL5+
ST

Secure microcontrolers
ATS90SC6404A
ATS90SC12872A
EAL5+
Atmel

1998 **2000** **2002** **2004** **2006** **2008** **2010**

ClearSy

System Engineering