Esterel et SCADE, de la recherche à l'industrie

2. La vision industrielle

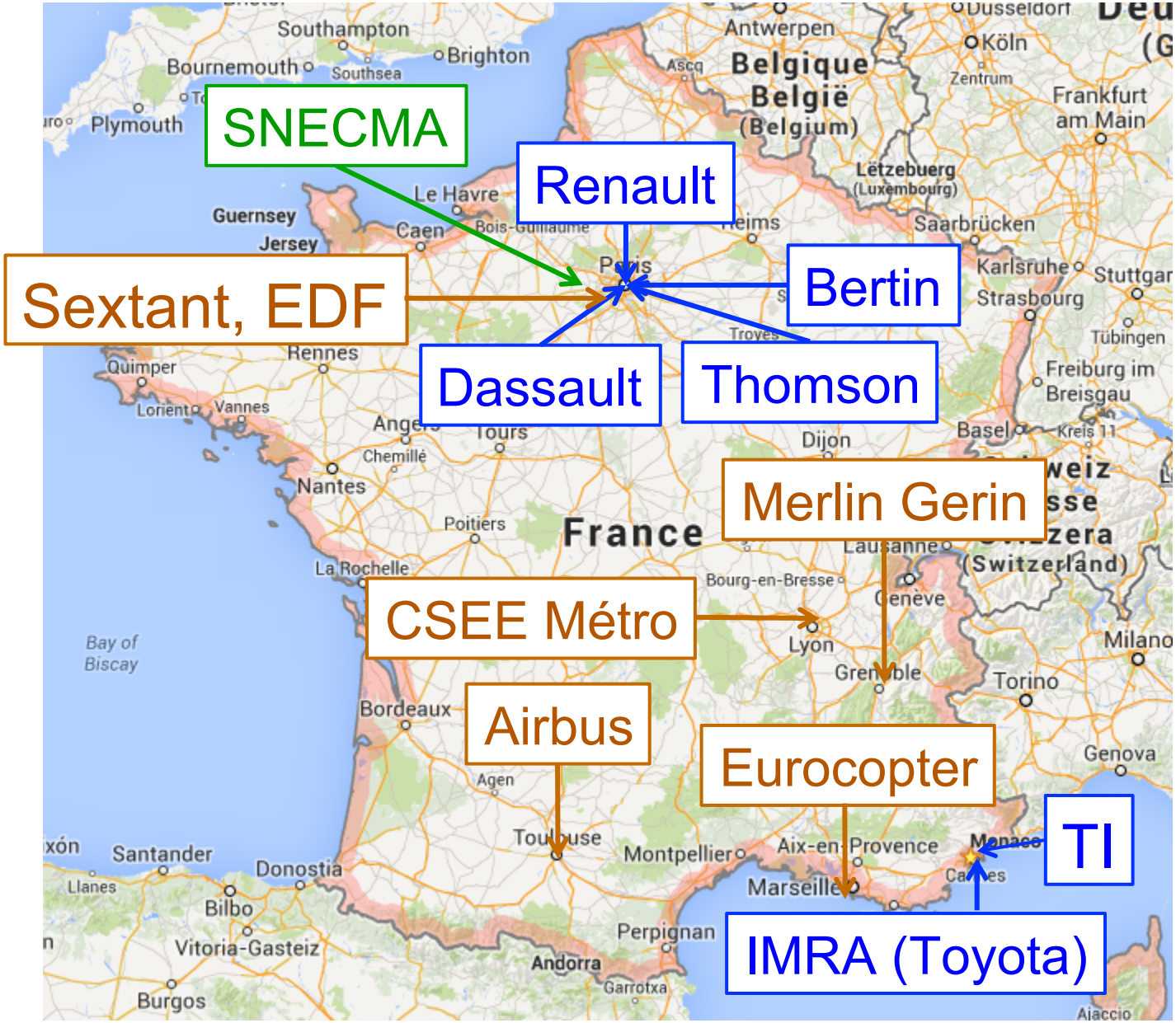
Gérard Berry

Collège de France

Chaire Algorithmes, machines et langages

gerard.berry@college-de-france.fr

Cours 2, Inria Sophia-Méditerranée, 22/01/2014



Esterel
Cisi Ing,Ilog
Simulog

SCADE
Verilog →
Telelogic

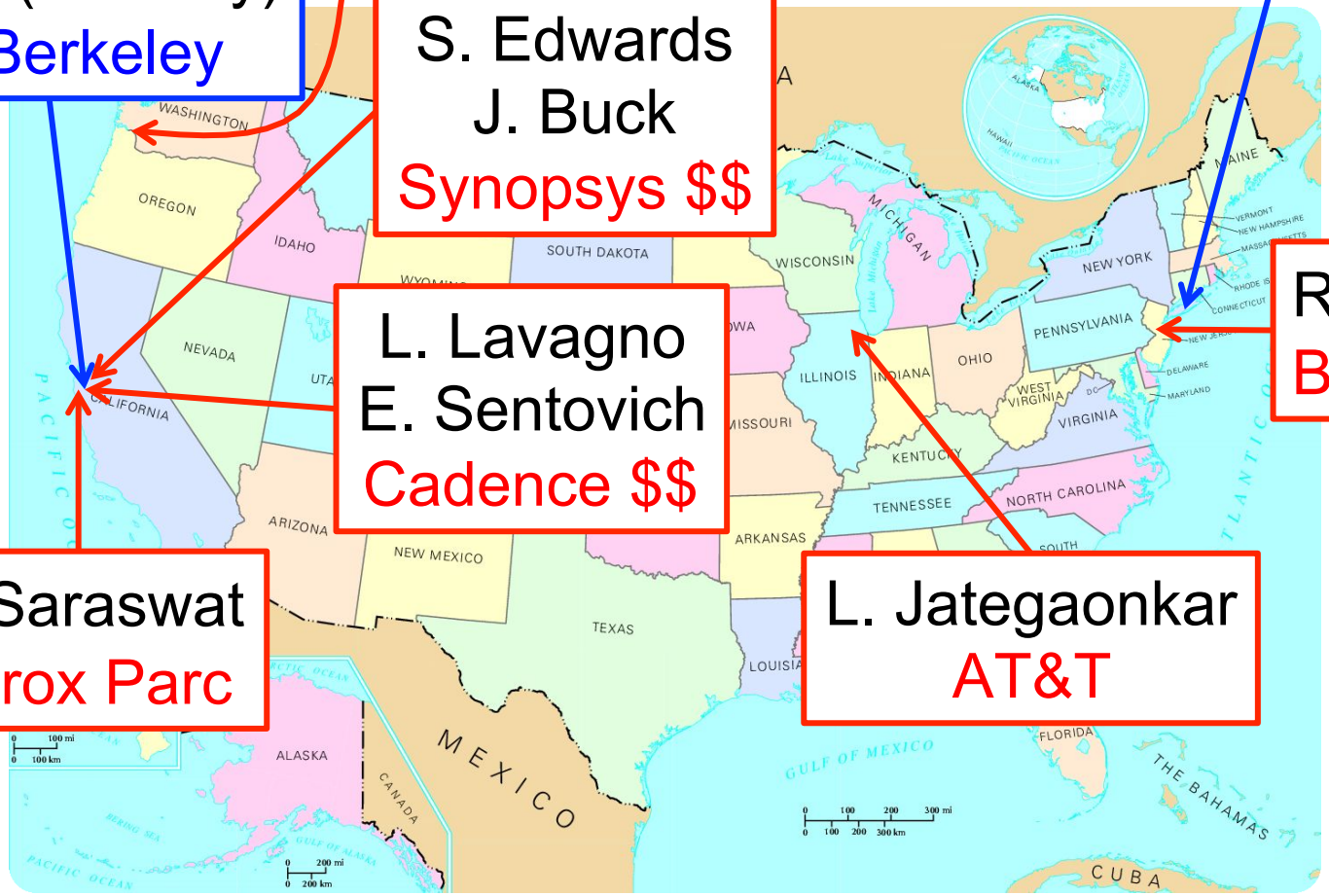
Sildex
TNI

Michael Kishinevsky
Intel $$

S. Edwards
Columbia

E. Lee (Ptolemy)
UC Berkeley

S. Edwards
J. Buck
Synopsys $$



L. Lavagno
E. Sentovich
Cadence $$

Ravi Sethi
Bell Labs

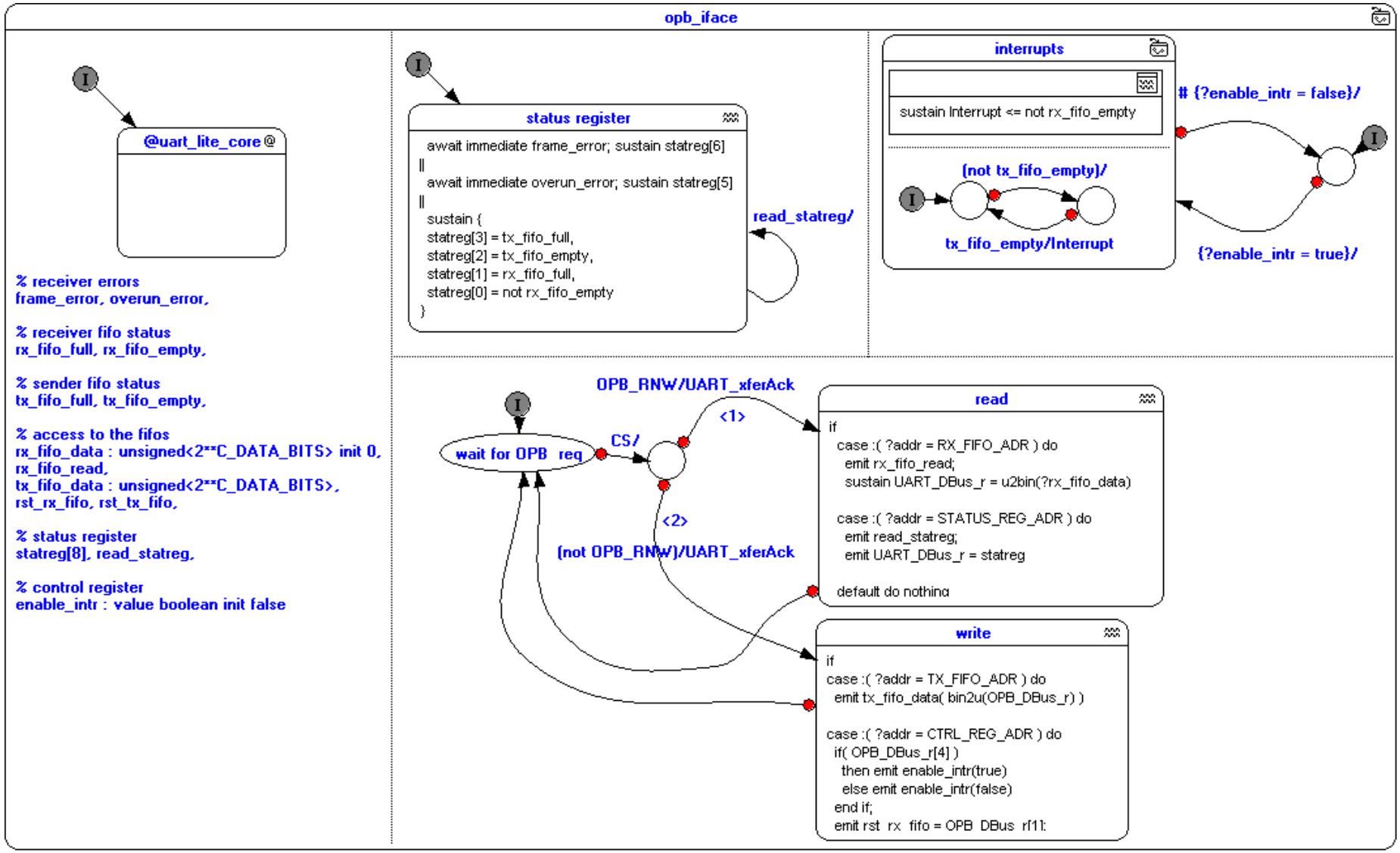
V. Saraswat
Xerox Parc

L. Jategaonkar
AT&T

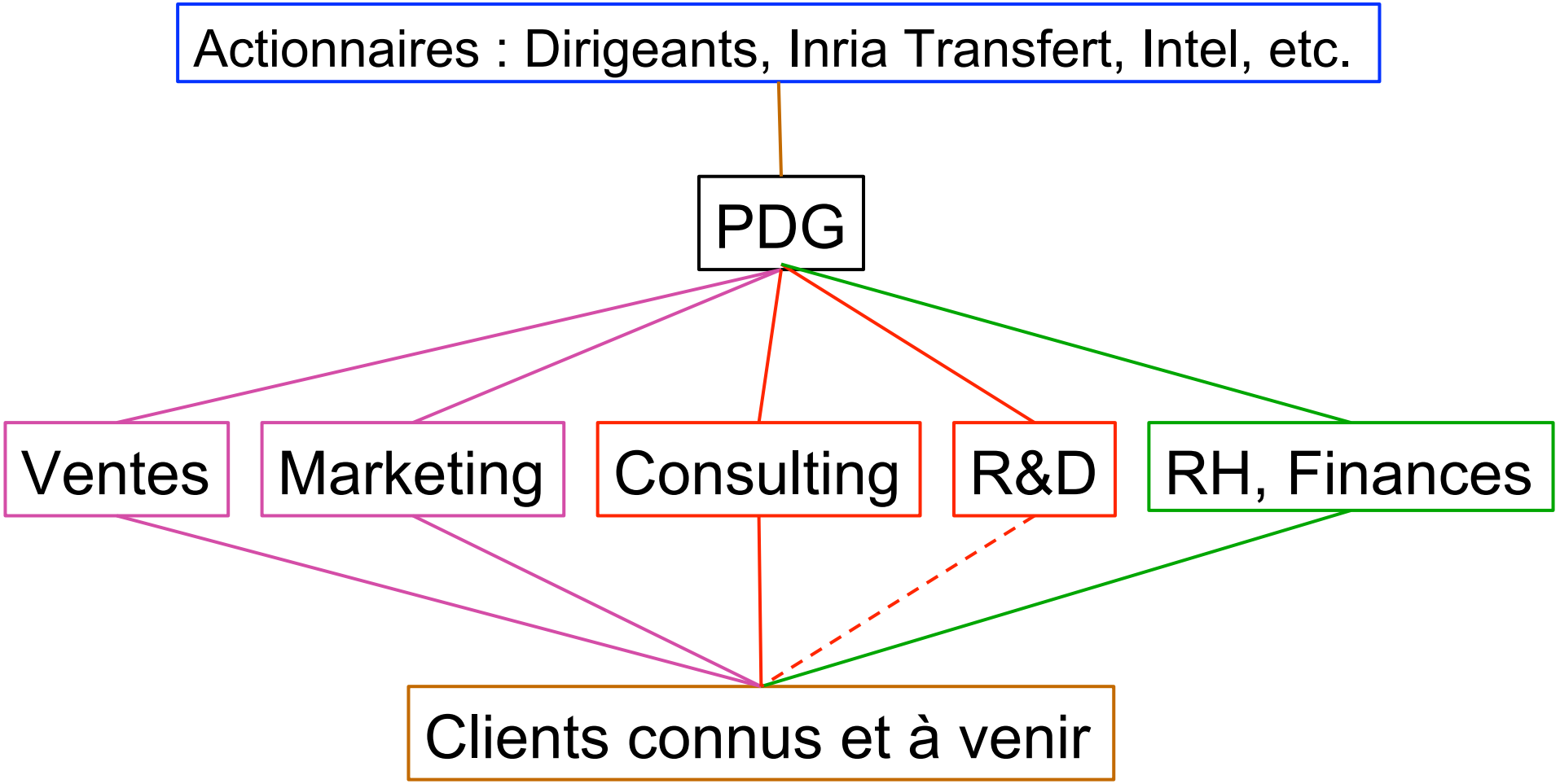
Etat des choses début 2001

- Logiciel : clients actifs (Dassault Aviation, Thomson)
- Circuits : proposition initiale Esterel v7
  avec M. Kishinevsky (Intel SCL)
  ⇒ intègre les chemins de données
- Expérimentations HW et HW / SW avec Esterel v5
  Digital Equipment : J. Vuillemin, carte FPGA Perle 1
  Intel, MK : SATA link layer (efficace, bug trouvé), ILD, etc.
  Motorola, Y. Mathis, A. Chatelain : simulation architecturale
  ST Micro : R. Hersemeule
  Xilinx, S. Singh : protocoles rapides
  Texas Instruments, L. Arditi, G. Clavé : DSP, communication
  Cadence, L. Lavagno, E. Sentovich : HW-SW codesign
  Synopsys, J. Buck : System-Level Design (licence source)

Esterel v7, textuel et graphique

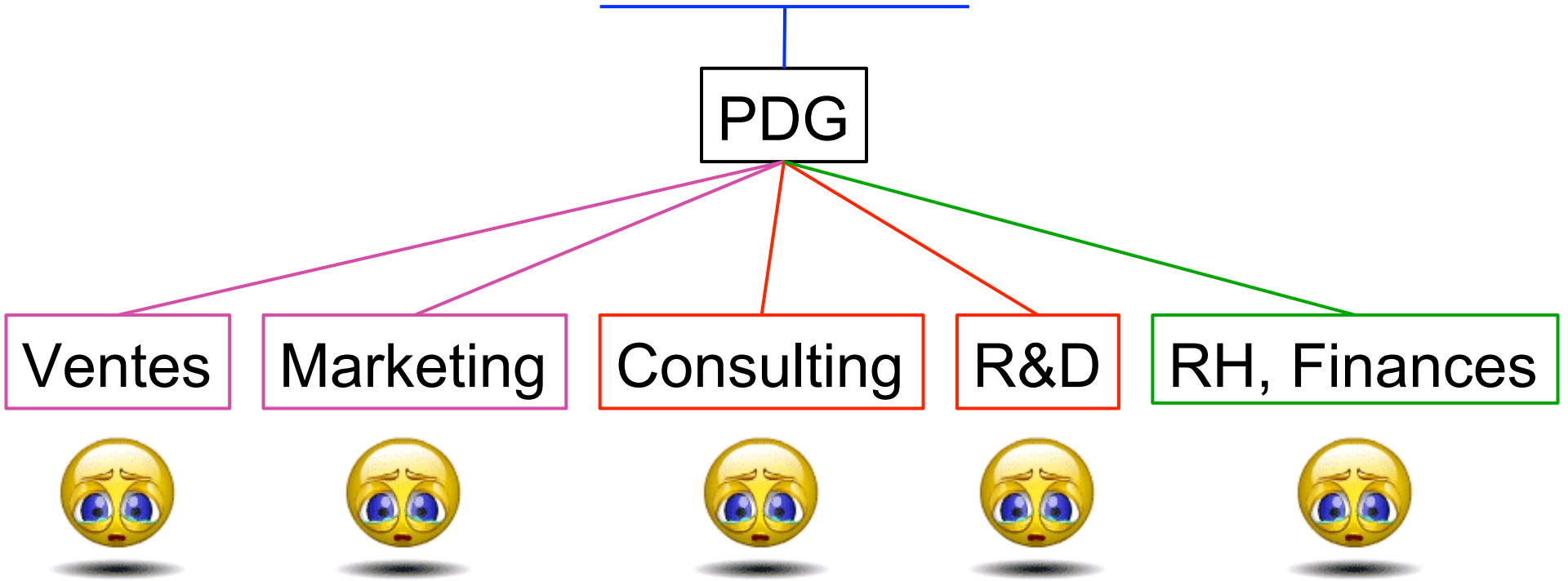


Esterel Technologies – la naissance



Première réunion

Chers amis, de quoi allons nous mourir, et quand ?



Réponses toutes différentes, toutes intéressantes

Industrie ⇒ Flot de développement

Question clef : insertion dans les flots existants

Architecture

Micro-architecture

Design logique RTL

Circuits

DFT (testabilité)

Placement-Routage

$ 1,000,000 Masks

Chips

Design

Vérification

Synthèse

Vérification

Fab

Vérification

Architecture

composants
dimensionnement
communication

Word, Excel, Visio
System C

Micro-architecture

parallélisme
pipeline
partage de ressources

Word, Visio, C

ESTEREL V7

Design logique RTL

portes, horloges
registres, RAMs
chemin critique

VHDL, Verilog

Circuits

cellules standard
arbres d'horloges,
surface, vitesse

netlists

DFT (testabilité)

scan insertion

netlists

Placement-Routage

contraintes électriques
& physiques

P&R netlists

$ 1,000,000

Masks

impression

pseudo-rectangles

Chips

fabrication

die, wafer

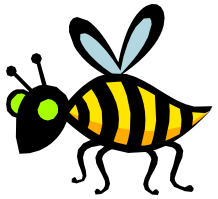
Architecture

$$ 

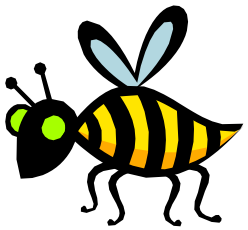
Micro-architecture

$$ 

Design logique RTL

$$ 

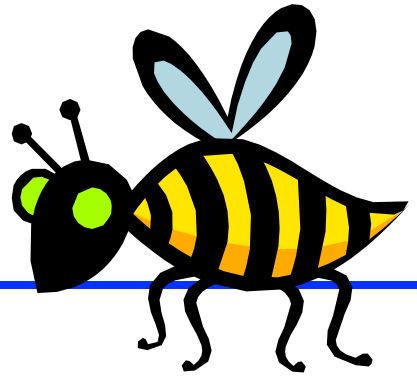
Circuits

$$ 

DFT (testabilité)

Placement-Routage

$ 1,000,000 Masks

$$ 

Chips

Architecture

fonctionnalité ?
performances ?
marché ?

Expérience
Revues

Micro-architecture

découpage ?
performance ?

modèles SystemC

ESTEREL V7

Design logique RTL

fonctionnalités ?
taille / vitesse ?
chaleur ?

test aléatoire dirigé
vérification formelle

Circuits

identique au RTL ?

équivalence formelle
(model checking)

DFT (testabilité)

couverture de tests
~100% ?

ATPG

Placement-Routage

connexions?
contraintes
électriques ?
timing?

Design Rules
Checking (DRC)

$ 1,000,000 Masks

Chips

fonctionnent?

Scan test

Architecture

Micro-architecture

ESTEREL V7

Design logique RTL

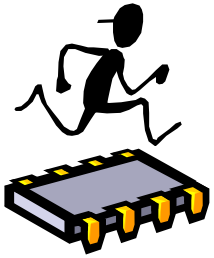
Circuits

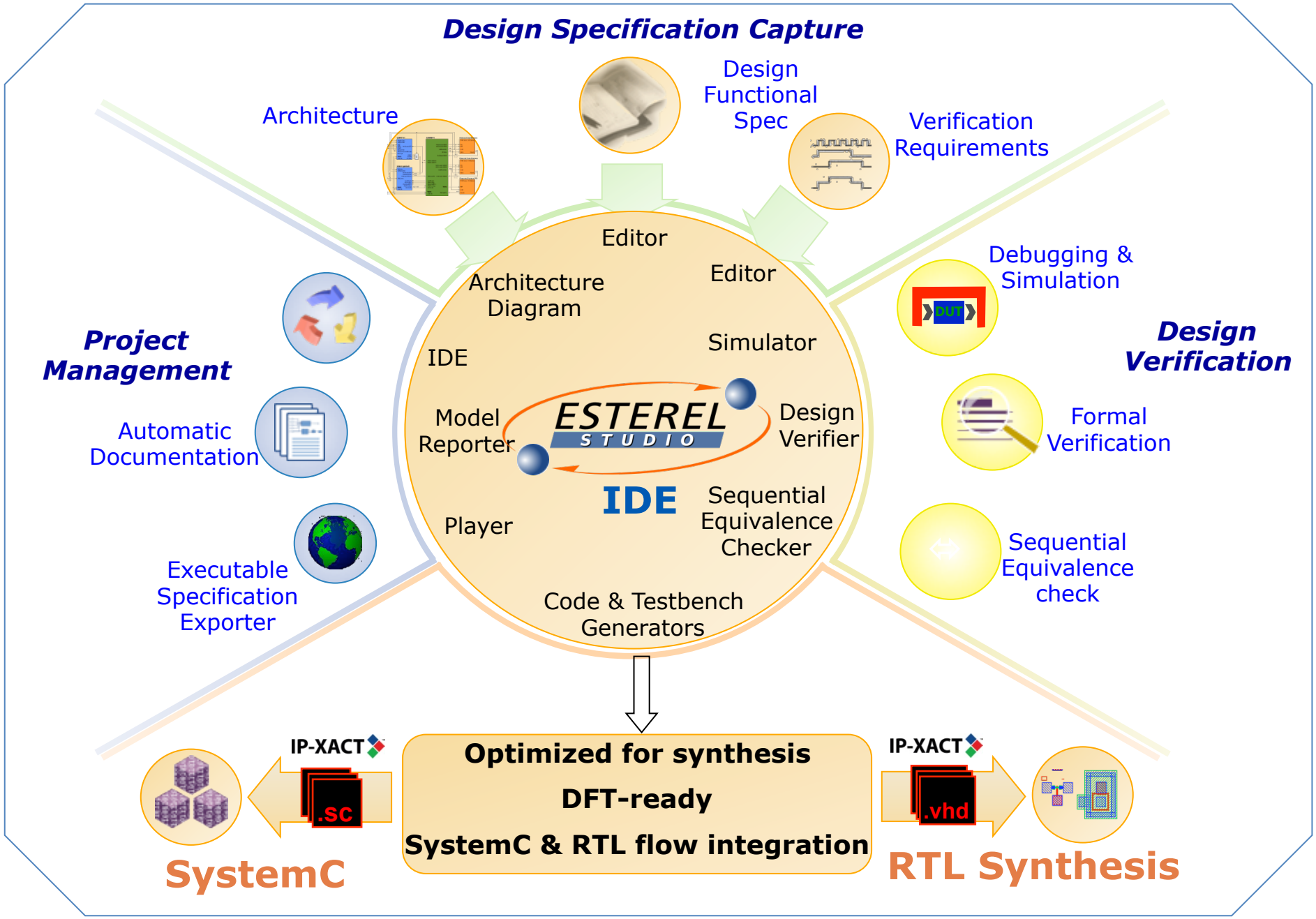
DFT (testabilité)

Placement-Routage

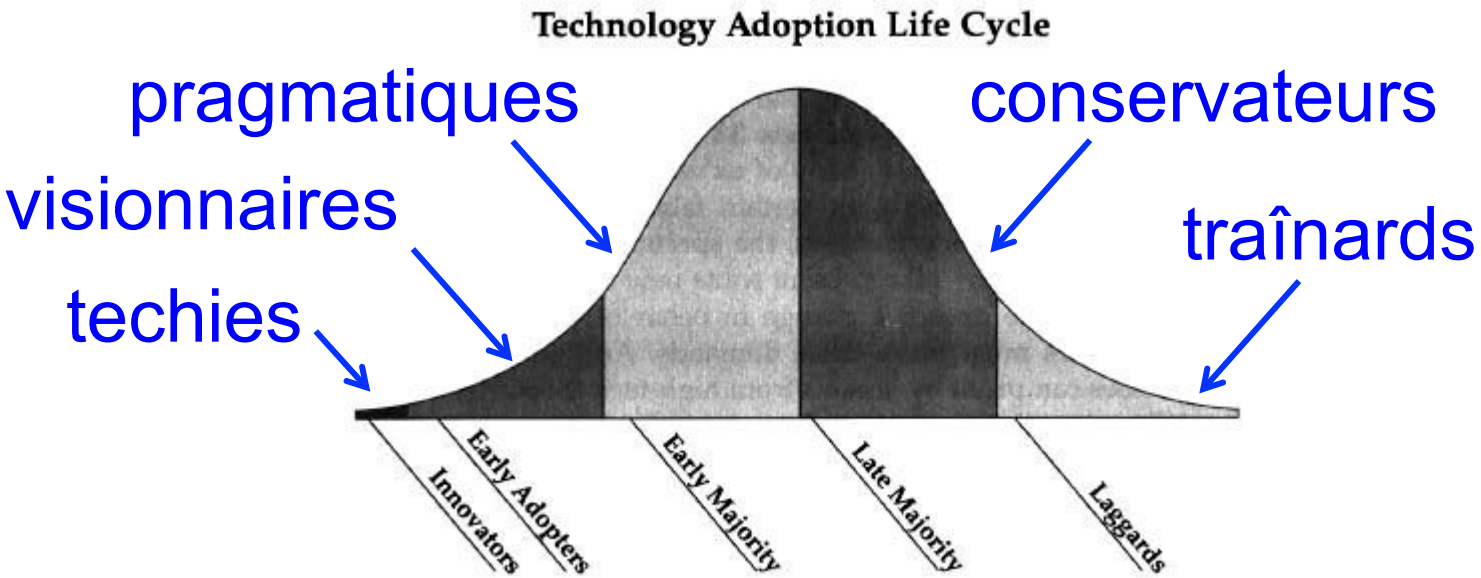
$ 1,000,000 Masks

Chips



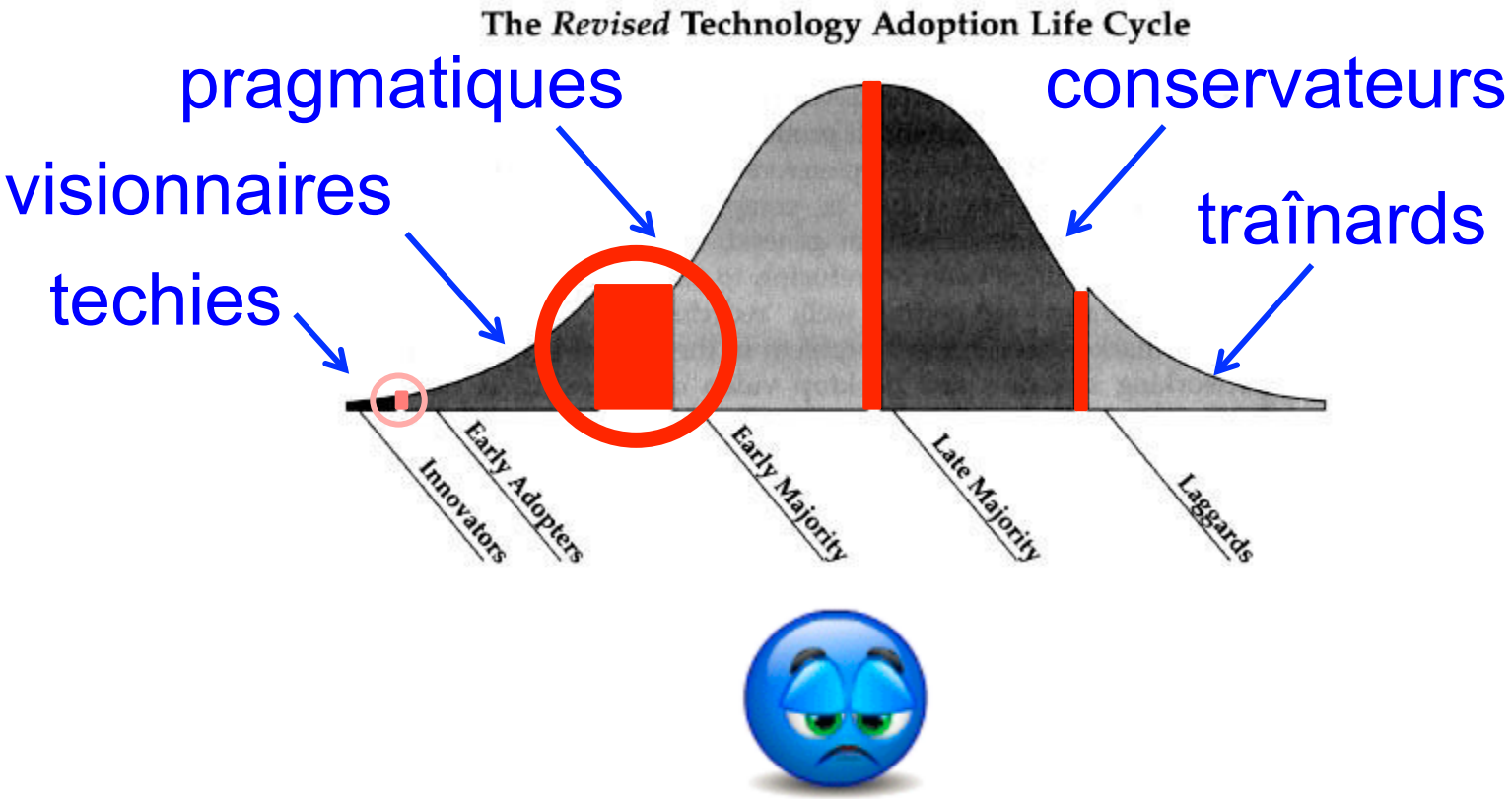

Design Specification Capture
Architecture
Design Functional Spec
Verification Requirements
Editor
Editor
Architecture Diagram
Simulator
IDE
Model Reporter
ESTEREL STUDIO
Design Verifier
IDE
Player
Sequential Equivalence Checker
Code & Testbench Generators
Project Management
Automatic Documentation
Executable Specification Exporter
Debugging & Simulation
DUT
Design Verification
Formal Verification
Sequential Equivalence check
IP-XACT
.sc
SystemC
Optimized for synthesis
DFT-ready
SystemC & RTL flow integration
IP-XACT
.vhd
RTL Synthesis

Crossing the Chasm – Geoffrey A. Moore



- techies ⇒ référence technique
- visionnaires ⇒ début de la crédibilité industrielle
- pragmatiques, conservateurs ⇒ le vrai marché

Où sont les fossés ?



Les arguments qui peuvent convaincre les uns sont inefficaces ou contre-productifs pour les autres

Trois marchés distincts

- Techies : aiment la technique pour la technique
  apprécient la nouveauté et l'élégance
  tolèrent les bugs et trous initiaux
  pensent que les pragmatiques sont ignares

- Visionnaires : vrais projets, avec prise de risques
  cherchent l'avantage compétitif (*breakthrough*)
  écoutent certains techies
  sont très exigeants, mais encore tolérants

- Pragmatiques / conservateurs :
  n'aiment pas le risque cherchent des solutions
  déjà confirmées par les autres pragmatiques
  pensent que les techies sont des
  pique-assiettes inefficaces

Attention :
chacun d'entre nous occupe une position variable selon le sujet traité !

GB : techie en photo
visionnaire en programmation (?)
pragmatique en matériel informatique
conservateur en design de transparents
traînard en programmation par threads

Taille des marchés

Taille : techies < visionnaires << pragmatiques
= conservateurs

Sous : techies << visionnaires <<< pragmatiques
= conservateurs

Convaincre les techies

Facile, ils vont aux mêmes congrès que vous !

- Prêts à essayer eux-mêmes
- Admirateur des qualités, tolérants sur les défauts si dérivée positive (comme vous)
- Prêts à dialoguer, à co-écrire des applis ou des papiers - voire à se faire embaucher chez vous!

Intel : M. Kishinevsky (co-auteur Esterel v7)
Texas Instruments : L. Arditi, G. Clavé, Y. Leduc, E. Badi, etc. (Villeneuve-Loubet)
Philips / NXP : M. Duranton et son équipe (Eindhoven)
ST Micro : M. Borgatti (Milan), J.P Cousin (Grenoble)

Impératif : détecter les techies reconnus en interne

Convaincre les visionnaires

Ils vont aux mêmes congrès généraux que vous (DAC, DATE), mais pas aux mêmes sessions

Méthode : projet coopératif proche de la production, financé, et effectué en collaboration

⇒ consultants dédiés + lien avec la R&D

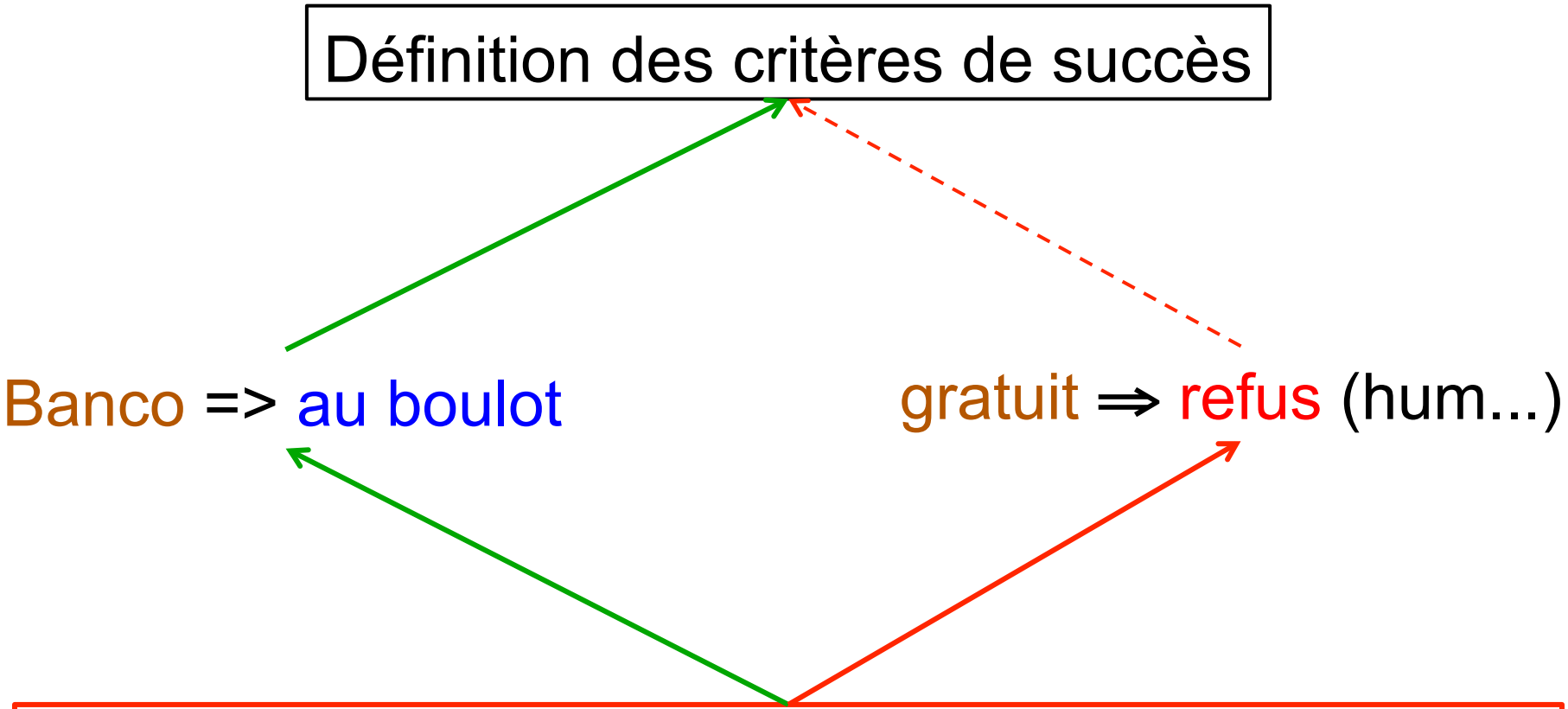
Texas Instruments : gestion mémoire, DMAs vidéo

L. Six, P. Voultoury, etc.

ST micro : ST bus (réseau sur puce, Catane + Delhi)

C. Pistritto, *et. al.*

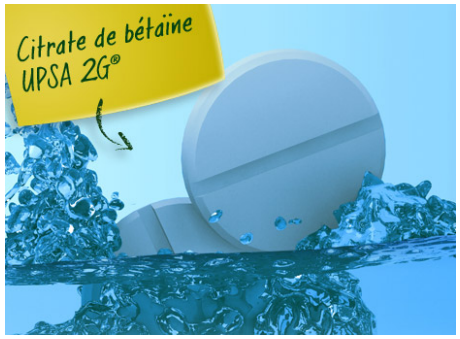
Le projet d'évaluation, moment crucial

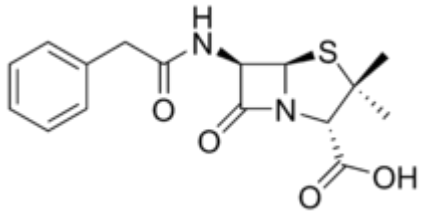


Principe: ne conduire que des évaluations payantes, obligatoirement suivies par un consultant dédié

Convaincre les conservateurs ?

On ne peut leur vendre que des médicaments,
et uniquement s'ils se savent déjà malades
pas de la prévention (= manque à perdre)...





✓ ✓ ✓ X

... sauf en cas de plantage industriel majeur !
(cf Bell Labs, Intel, etc.)

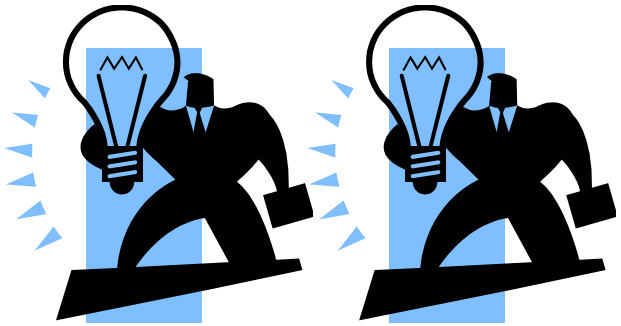
Convaincre les conservateurs

1. Le client ne veut pas savoir qu'il est malade
   We don't have this kind of problem !
   Our current method is good enough
   We have workarounds for the difficulties you mention
   Sans espoir ! Ne jamais dépenser d'énergie sur quelqu'un qui ne sera jamais convaincu (> /dev/null)

2. Le client ne se sort pas d'un problème urgent
   do whatever you want, but solve it **NOW** (I mean 2 weeks)!
   peu d'espoir, techno pas encore prête pour ça

3. Le client accepte une réunion technique
   concentration maximale !

Réunion client : les questions centrales



- What is your positioning, your value proposition?

  You will take more time to design, but less to verify

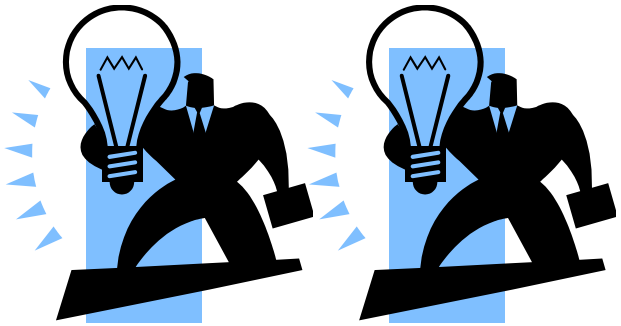
  This will improve your time to market, which is very important

  Esterel is formal and so much better than Verilog / VHDL !

  You will make less bugs, save their costs, etc. etc.

- Hmmm.... But your product is quite expensive, what will be my ROI? How do you quantify it?

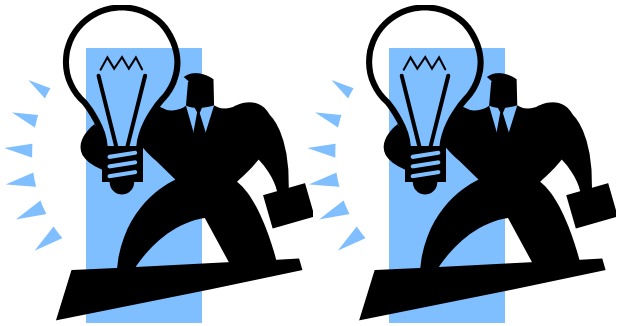
Réunion client : les questions centrales



- What is your market share ? How solid are you?
  ....committed shareholders...fast growth ... ...
- How are your training and maintenance organized?
  ... pilot projects...consultants...immediate fix by R&D...
- How will I hire already trained engineers ?
  ... free academic license...international universities...

Can you summarize your value proposition?

Interprétation sémantique



En quoi pouvez-vous m'aider à résoudre mes problèmes?

aux faits!

doit être votre seul objectif

et pas les vôtres

parler beaucoup de lui et un peu de nous

⇒ construction de la confiance

(structure, techno, engagement)

La question qui tue : Why a new language ?

Esterel : syntaxe ADA

```
loop
   abort
      every A do emit X end
   ||
      pause ;
      V := 1 ;
      emit ?T <= V if B
   when S
end loop
```

ECL (1999)
L. Lavagno
E. Sentovich

norme de fait : syntaxe C

```
while (1) {
   do {
      par {
         {
            every (A) emit X;
         }
         {
            pause ;
            V = 1;
            if (B) emit(T, V);
         }
      }
   } abort (S)
```

Contact avec la recherche

.... nettement affaibli

Ancien chercheur Chercheur

J’ai des idées intéressantes pour toi !

Mais pourquoi ça m’intéresserait?
Il ne me demande pas ce qui peut m’intéresser...

Esterel v7 : du succès technique à l'arrêt

- 2001-2004 : la naissance des outils, les techies
  - définition 1 du langage
  - développement de l'outillage : compilateur, Esterel Studio
  - expérimentations : Intel, TI Villeneuve-Loubet, ST Milan, ST Grenoble
- 2004-2006 : la maturité, les visionnaires
  - passage au multi-horloges
  - expérimentations lourdes : TI VL, ST, Philips / NXP
- 2006-2008 : passage en production, les pragmatiques
  - TI VL, contrat majeur : contrôleurs mémoires, DMA vidéo, etc.
  - ST Catane : ST Bus (réseau sur puce)
  - travail de standardisation IEEE
  - établissement de coopérations avec d'autres fournisseurs
- 2009 : arrêt global du domaine HW après la crise bancaire...
- 2009-2012 : SCADE s'impose sur le marché
- 2012: Esterel Technologies racheté par ANSYS

SCADE : une approche pragmatique

- mi-1980 : Paul Caspi, CR CNRS en automatique
  en contact direct avec les ingénieur (Merlin-Gerin, Airbus)
  et avec les informaticiens (N. Halbwachs, labo commun)

Paul Caspi Daniel Pilaud

SCADE : une approche bien différente

- Problèmes, méthodes et contraintes différents

  contrôle continu ≠ contrôle discret (Esterel)

  il est connu que les langages classiques ne conviennent pas

  ⇒ block diagrams graphiques, simulation en Simulink

  exigences de sûreté >>> time-to-market

  ⇒ certification des logiciels (DO-178B ou autre)

- Les industriels développent leurs propre langages

  et leurs propres bibliothèques métier

  ... mais peinent à les maintenir et les trouvent trop coûteux

La proposition de valeur de Lustre (P. Caspi, N. Halbwachs, J.L. Bergerand, etc.)

- Langage très simple et allant droit au but
  - peu de primitives
  - textuel ou graphique (block diagrams classiques)
  - sémantique mathématique claire: réseaux de Kahn synchrones
  - bibliothèques développées en Lustre ⇒ meilleure sûreté
- compilation simple
  - donc compilateur certifiable
  - ⇒ temps de recertification des modifications bien plus court
  - efficacité comparable à celle des méthodes classiques
  - meilleure prédictibilité temporelle (scheduling statique)

Et, surtout, pas besoin de changer les habitudes !

Lustre : réseaux de Kahn synchrones

EventCounter

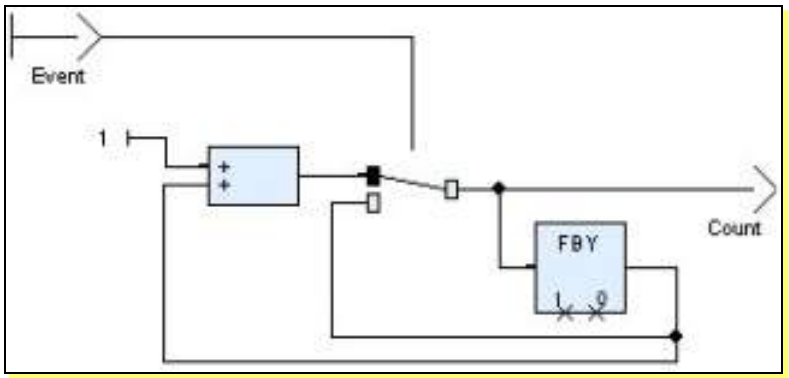
Event = false true false true true false false false true true false

Count = 0 1 1 2 3 3 3 3 4 5 5

$$\begin{cases} Count(0) = 0 \\ \forall t > 0,\ Count(t) = \begin{cases} Count(t-1) + 1, & if\ Event(t) = true \\ Count(t-1), & otherwise \end{cases} \end{cases}$$

```
Count = 0 → (if Event
              then pre(Count)+1
              else pre(Count))
```

Lustre textuel



Block Diagram SCADE

Horloges et sous-échantillonnage

Sous-échantillonnage

C	true	false	true	false	false	true
X	x1	x2	x3	x4	x5	x6
X when C	x1		x3			x6
pre(X when C)	nil		x1			x3
current(X when C)	x1	x1	x3	x3	x3	x6

Opérations sur flots sous-échantillonnés

C	true	false	true	false	false	true
X	x1	x2	x3	x4	x5	y6
Y	y1	y2	y3	y4	y5	y6
Z = X when C	x1		x3			x6
T = Y when C	y1		y3			y6
Z + T	x1 + y1		x3 + y3			x6 + y6

La recherche sur Lustre

- Compilation efficace
  J. Plaice, P. Raymond
- Traitement des tableaux
  F. Rocheteau (Digital Equipment PRL)
- Vérification formelle, génération de tests
  N. Halbwachs, A-C. Glory, C. Ratel, B. Jeannet
- Distribution physique, lien avec l'asynchrone
  A. Girault, P. Caspi, R. Salem
- Compilation des automates, automates hiérarchiques
  P. Raymond, F. Maraninchi (ARGOS)
- Worst Case Execution Time (WCET)
  R. Wilhelm (AbsInt GMBH)

L'industrialisation de SCADE

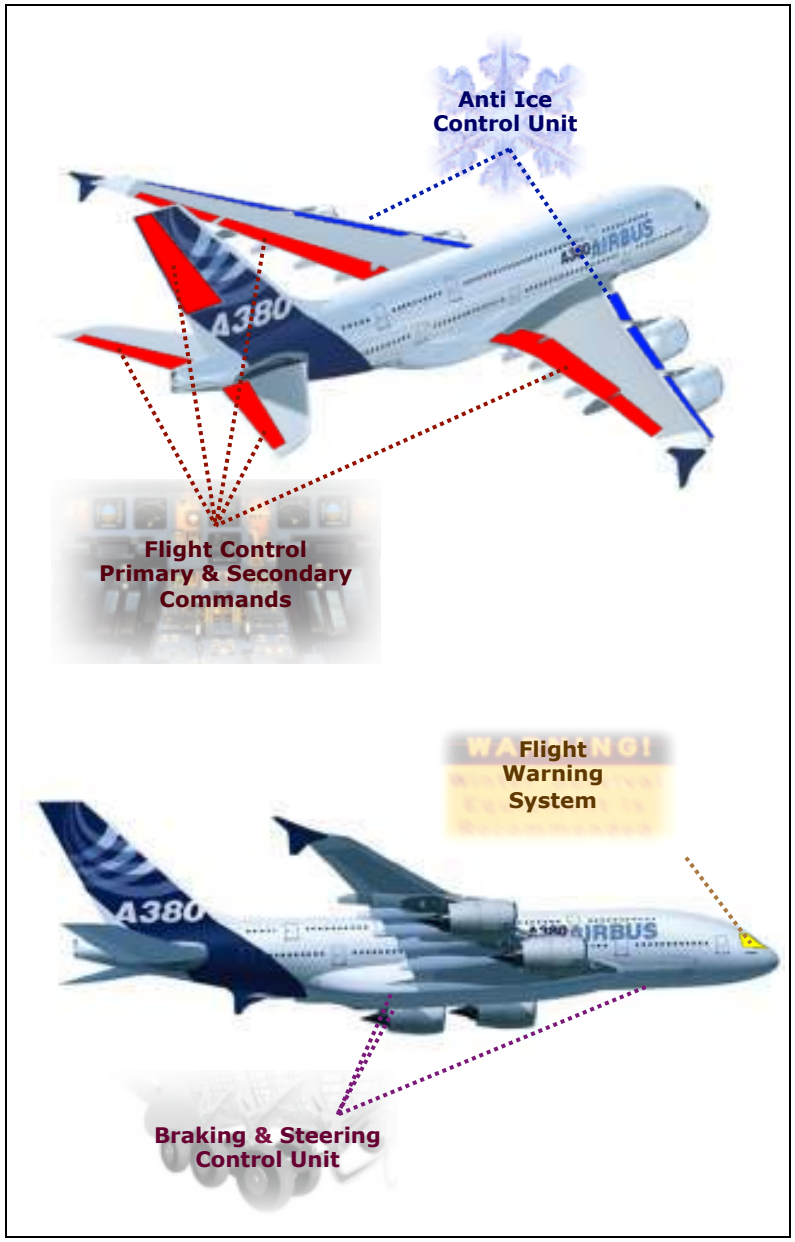
- Collaboration Merlin-Gerin (→ Schneider Electric)
  - migration de E. Pilaud et JL. Bergerand
  - développement du système SAGA
  - passage de SAGA chez Verilog
- Contacts avec Aérospatiale
  - outil interne SAO similaire, mais moins formel
  - Verilog : SAGA + SAO → SCADE, D. Pilaud
  - génération de code (KCG), certifiabilité DO-178B
  - développements A340-600 / A380
- Extension de la clientèle
  - métros, trains, hélicoptères (Eurocopter)
- Rachat par Telelogic (télécoms)
  - stagnation des développements et des ventes...

Certifiabilité DO-178B (avionique)

- Certification du processus de développement par une autorité indépendante (FAA, CEAT, JAA, etc.), mondialement requise
- But: détecter et rapporter les erreurs introduites durant le développement du logiciel
- Pas de préconisation de technique de vérification particulière
- Pas seulement du test, mais aussi des revues et des analyses du processus complet fondées sur sa traçabilité
- La vérification de la vérification est obligatoire

DO 178C : introduction de la conception par modèles, de la programmation objet et des méthodes formelles

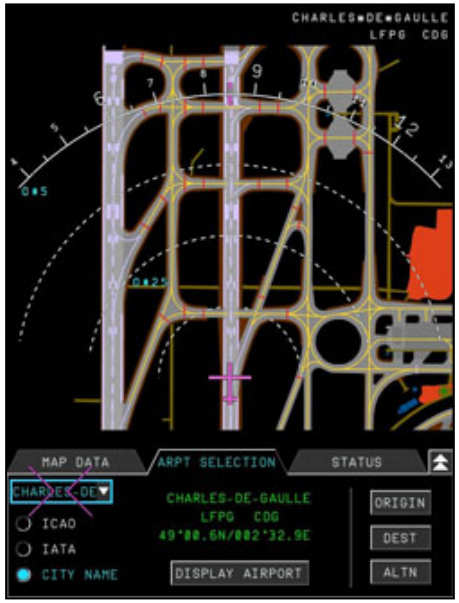
SCADE dans l'Airbus A380



- Contrôle de vol
- FADEC (contrôle moteur)
- Freinage et direction
- Gestion électrique
- Anti-givrage
- Système d'alarmes
- Cockpit:
  - PFD : Primary Flight Display
  - ND : Navigation Display
  - EWD : Engine Warning Display
  - SD : System Display
- ...

Thomson : IHM certifiable DO-178B

- Control and Display System (CDS)
  - 8 écrans, deux claviers / souris
- Head-Up Display (HUD)
  - Techno LCD
- On-board Airport Navigation System (OANS)

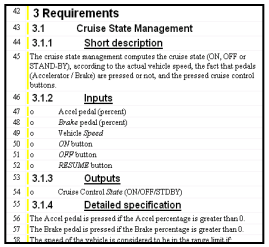


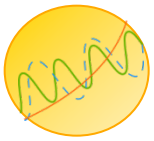
Rachat par Esterel Technologies (2003)

- Rachat de SCADE et IHM Thomson → SCADE Display
  et couplage avec SCADE pour la programmation des IHM
- Conquête de nouveaux marchés
  avionique dans le monde entier
  trains métros, spatial, industrie lourde, simulateurs, etc.
  automobile ? Encore trop dominé par les coûts...
- Développement de SCADE 6
  fusion contrôle continu / contrôle discret (Lustre / Esterel)
  fusion block-diagrams / automates
  ajout de tableaux fonctionnels
  couplage avec SCADE Display, SysML, etc
  codage en OCaml, certification

L'atelier SCADE en 2008

SYSTEM SPEC

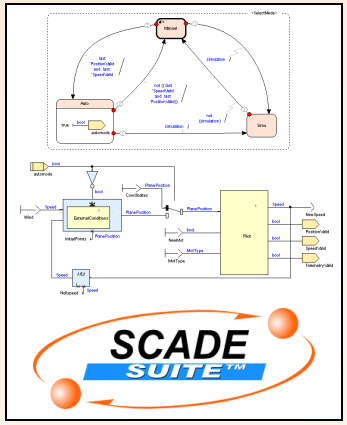


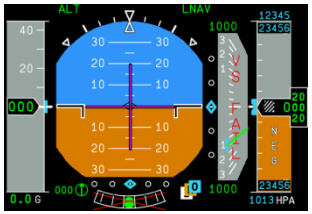


Algorithm Design Capture

Architecture Design Capture

DESIGN





VERIFY

Debugging & Simulation

Formal Verification

Model Coverage Analysis

Object Code Verification

SCADE Suite/SCADE Display Integration

Graphical Animation

Ergonomics Checking

GENERATE

SCADE Suite KCG

RTOS Wrappers

SCADE Display KCG

OpenGL|SC Compliant

SYSTEM TEST

MANAGE & TRACE

Requirements Management Gateway

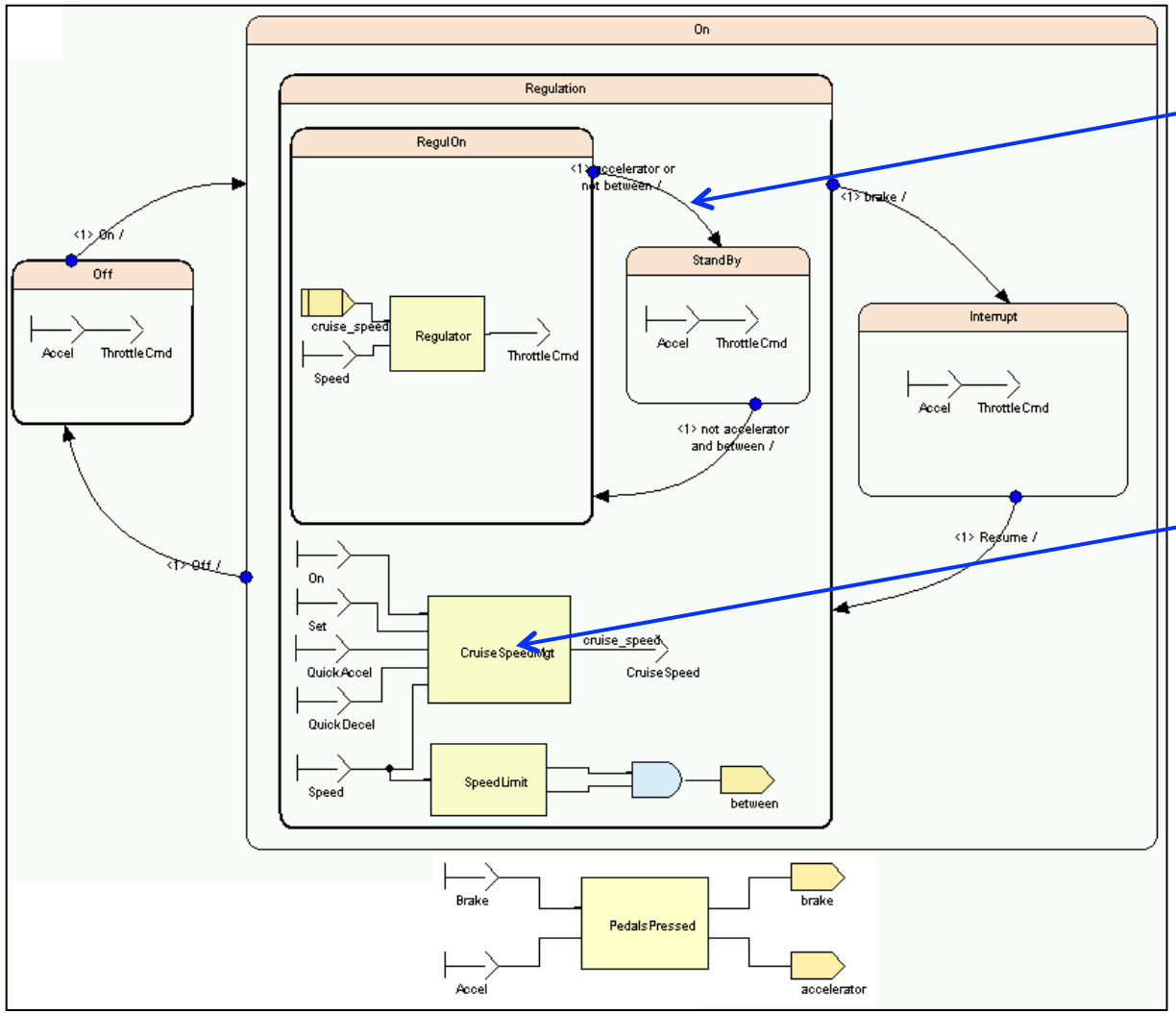
Integrated Configuration Management

Automatic Design Documentation

DO-178B
IEC 61508
EN 50128

Qualification Kits, Certificates & Handbooks

SCADE 6 : unification Lustre / Esterel



automates hiérarchiques

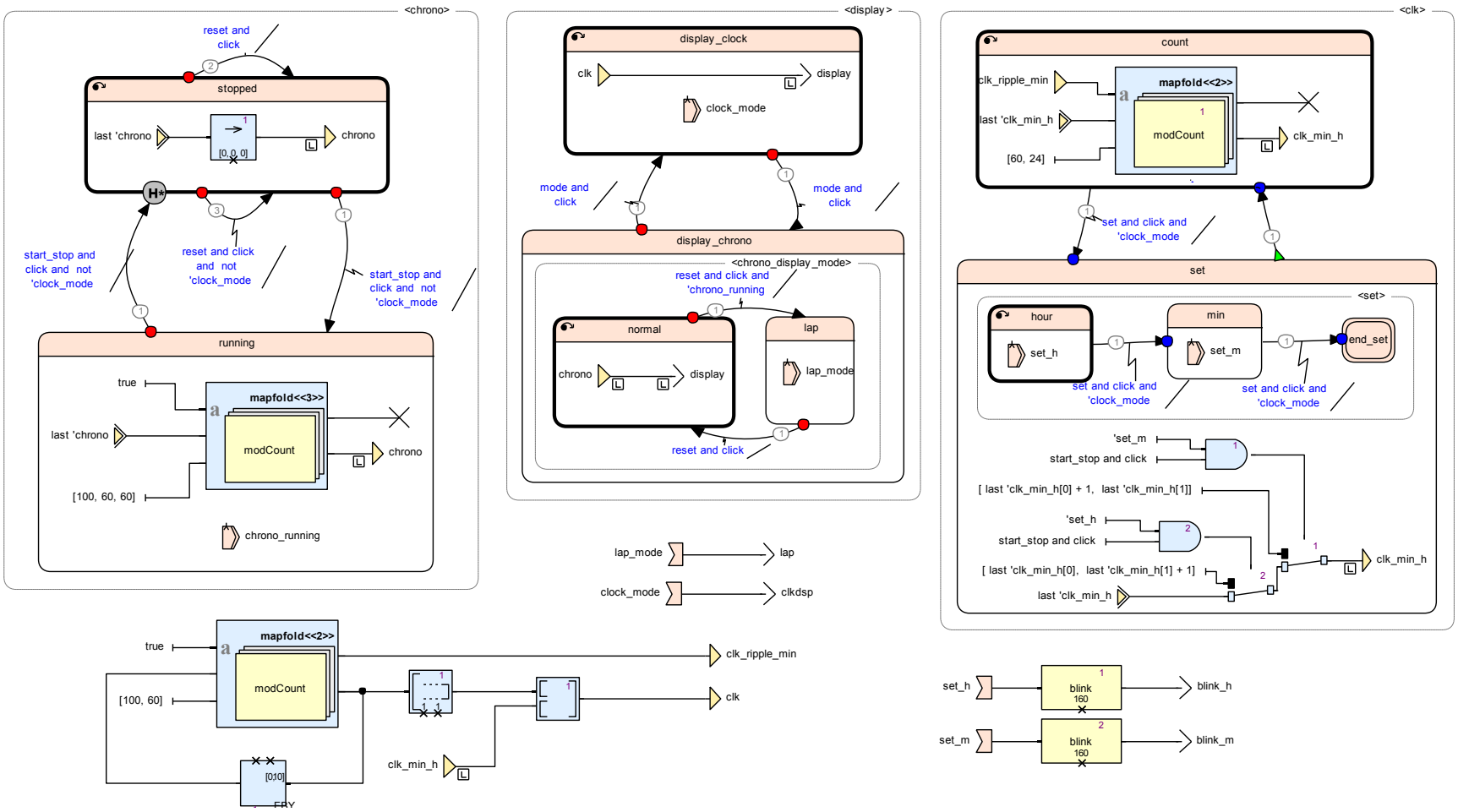
unification

block diagrams

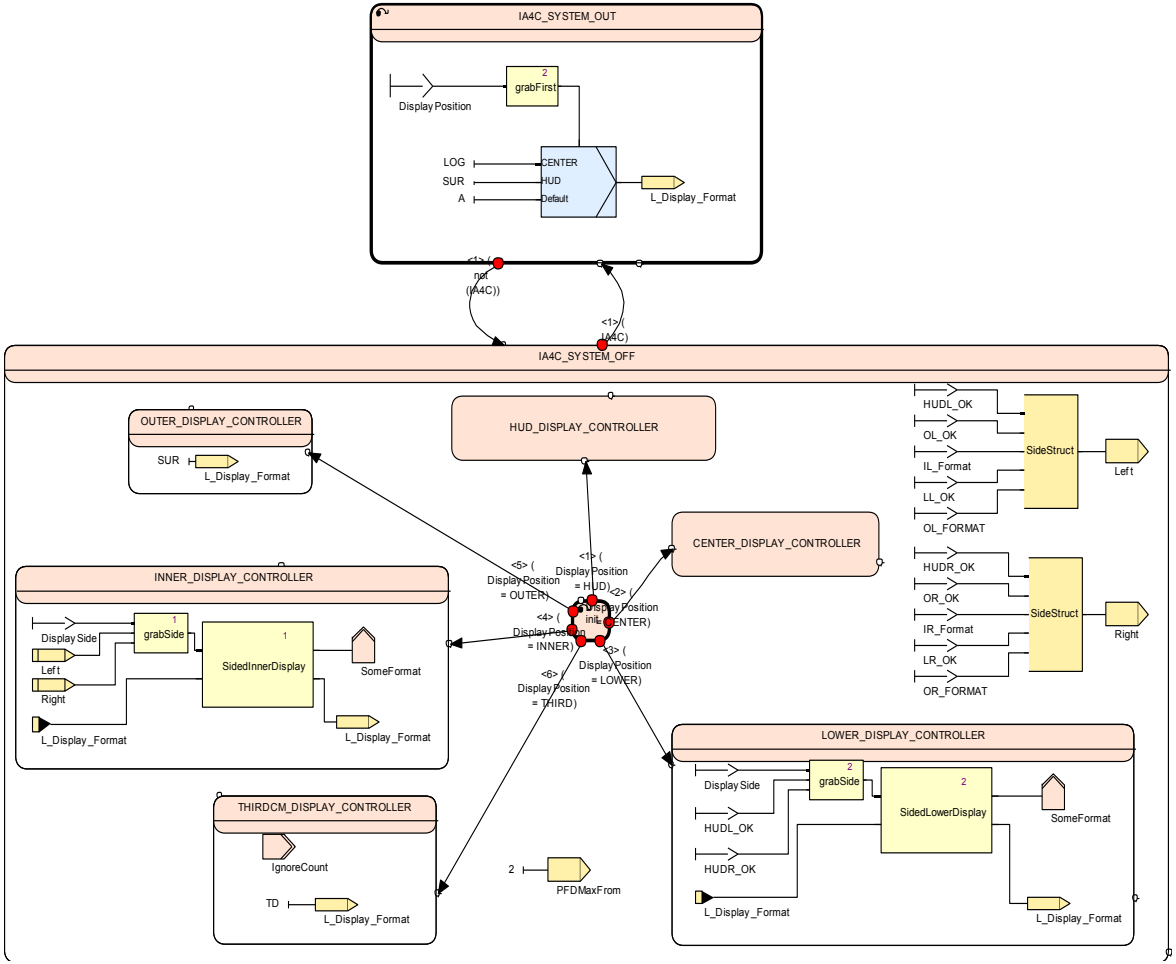
Langage fonctionnel
Tableaux fonctionnels
Sémantique formelle
Compilateur certifiable

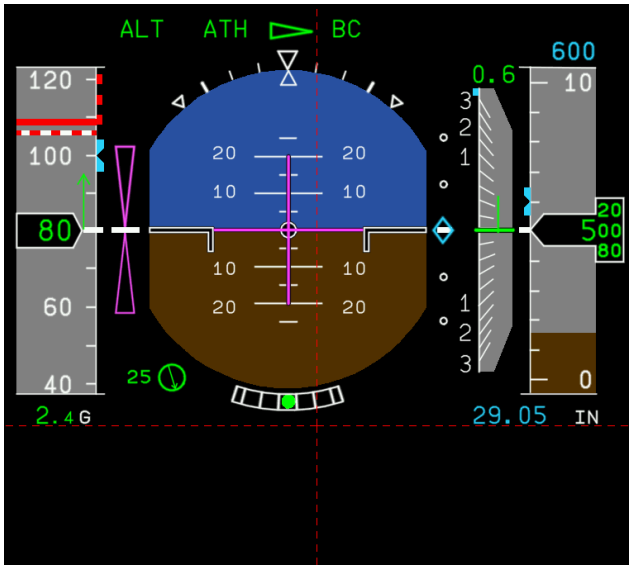
cf séminaire de Bruno Pagano, 23/04/2013

La montre digitale, version SCADE 6



Interfaces hommes-machines certifiables





Les grandes questions actuelles

- Liaison intime avec les outils architecturaux
  SYSML etc.
- Liaison avec vérification formelle / génération de tests
  Prover SL de Prover Technologies
- Génération de codes multiprocesseurs / multicœurs
- Intégration dans les grands systèmes plus asynchrones
- De la simulation à l'objet final
  Intégration avec les simulateurs temps continu
  certification sur la maquette logicielle

Conclusion

- Aller en vrai de la recherche vers l'industrie n'est pas qu'un simple transfert d'idées et de logiciel mais demande un vrai changement de mentalité :
  - compréhension des flots industriels, des clients, de leurs façons de penser, de leurs besoins
  - des arguments qui les convainquent réellement ... et donc de leur économie (value proposition, ROI, etc.)
  - du besoin de produits qui marchent de A à Z (pas de A à Y) et s'insèrent dans les flots existants
  - et de tous les métiers de la société, dont marketing et vente

Bibliographie

The Foundations of Esterel

G. Berry. *In Proof, Language and Interaction: Essays in Honour of Robin Milner,* G. Plotkin, C. Stirling and M. Tofte, editors, MIT Press, Foundations of Computing Series, 2000.

The synchronous dataflow programming language Lustre

N. Halbwachs, P. Caspi, P. Raymond et D. Pilaud.
Proceedings of the IEEE, volume 79(9), pp. 1305–1320 (1991)
séminaire de N Halbwachs sur Lustre :
http://www.college-de-france.fr/site/gerard-berry/seminar-2010-01-13-11h00.htm

SCADE: Synchronous design and validation of embedded control software

G. Berry. G. Berry. *Next Generation Design and Verification of Distributed Embedded Systems*, S. Ramesh and P. Sampath Ed., Springer Verlag (2007).

The synchronous languages twelve years later

Albert Benveniste, Paul Caspi, Stephen A. Edwards, Nicolas Halbwachs,
Paul Le Guernic et Robert de Simone.
Proceedings of the IEEE, Special issue on Embedded Systems, 91(1): 64-83, 2003.

La certification, ou comment faire confiance au logiciel pour l'avionique critique

G. Ladier, Séminaire du cours n° 4 du cycle *Pourquoi et comment le monde devient numérique*, 15 février 2008
http://www.college-de-france.fr/site/gerard-berry/seminar-2008-02-15-11h30.htm

Pardon à tous ceux que j'ai oubliés....

Et merci à l'Inria, à l'Ecole des mines et au CNRS
d'avoir constamment soutenu nos projets