iha.dk

Industrial applications of VDM and other formal methods and future perspectives

Professor Peter Gorm Larsen

Engineering College of Aarhus

(pgl@iha.dk)

Personal Background

- **Theoretical Work**
  - VDM-SL Semantics (ISO standard)
  - VDM-SL Proof Rules (PhD work)
- **More Practical Work**
  - VDM and Structured Analysis in combination
  - VDMTools architect
  - Transfer VDM to Industry
  - Intensive use Industrially
- **Employed by**
  - For 13 years: IFAD A/S
  - For 3,5 years: Systematic Software Engineering A/S
  - For 3 years:
    - Engineering College of Aarhus
    - PGL Consult

Overview of Formal Methods

iha.dk

- **Selected Industrial VDM Projects**
- A Survey of Industrial FM Applications
- Expected Future use of Formal Methods

ConForm (1994)

iha.dk

- Organisation: British Aerospace (UK)
- Domain: Security (gateway)
- Tools: The VDM-SL Toolbox
- Experience:
  - Prevented propagation of error
  - Successful technology transfer
  - At least 4 more applications without support
- Statements:
  - “Engineers can learn the technique in one week”
  - “**VDMTools**® can be integrated gradually into a traditional existing development process”

DustExpert (1995-7)

iha.dk

- Organisation: Adelard (UK)
- Domain: Safety (dust explosives)
- Tools: The VDM-SL Toolbox
- Experience:
  - Delivered on time at expected cost
  - Large VDM-SL specification
  - Testing support valuable
- Statement:
  - “Using **VDMTools**® we have achieved a productivity and fault density far better than industry norms for safety related systems”

Adelard Metrics

iha.dk

Initial requirements	450 pages
VDM specification	16kloc (31 modules) 12kloc (excl comments)
Prolog implementation	37kloc 16kloc (excl comments)
C++ GUI implementation	23kloc 18kloc (excl comments)

- 31 faults in Prolog and C++ (< 1/kloc)
- Most minor, only 1 safety-related
- 1 (small) design error, rest in coding

CAVA (1998-)

- Organisation: Baan (Denmark)
- Domain: Constraint solver (Sales Configuration)
- Tools: The VDM-SL Toolbox
- Experience:
  - Common understanding
  - Faster route to prototype
  - Earlier testing
- Statement:
  - "**VDMTools**® has been used in order to increase quality and reduce development risks on high complexity products"

Dutch DoD (1997-8)

iha.dk

- Organisation: Origin, The Netherlands
- Domain: Military
- Tools: The VDM-SL Toolbox
- Experience:
  - Higher level of assurance
  - Mastering of complexity
  - Delivered at ***expected cost*** and ***on schedule***
  - ***No errors detected in code after delivery***
- Statement:
  - “We chose **VDMTools**® because of high demands on maintainability, adaptability and reliability”

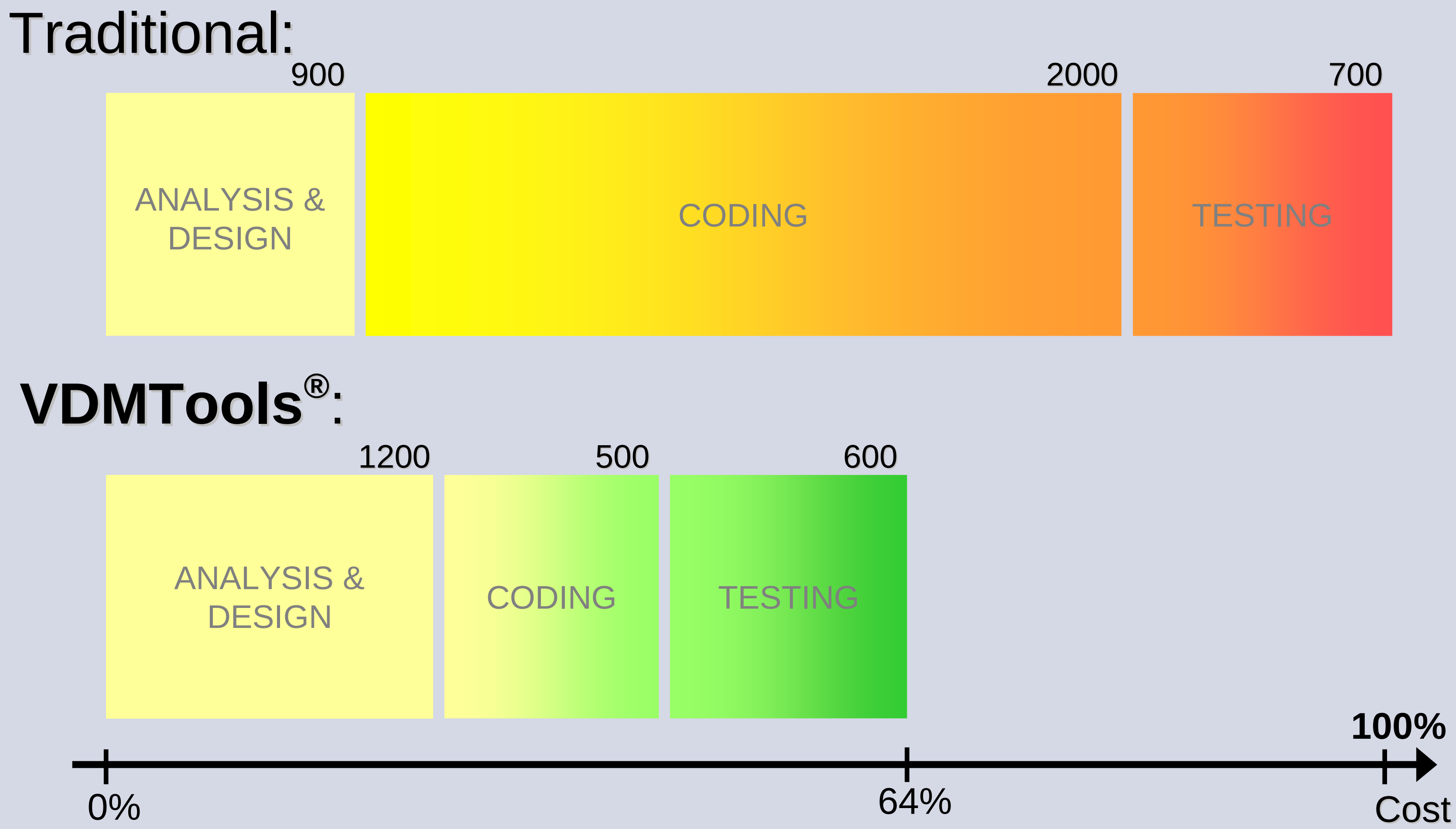
DoD, NL Metrics (1)

iha.dk

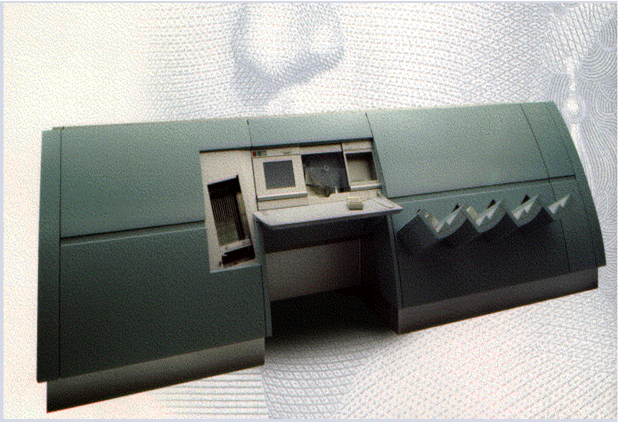
	kloc	hours	loc/hour
spec	15	1196	13
manual impl	4	471	8.5
automatic impl	90	0	NA
test	NA	612	NA
total code	94	2279	41.2

- Estimated 12 C++ loc/h with manual coding!

DoD - Comparative Metrics



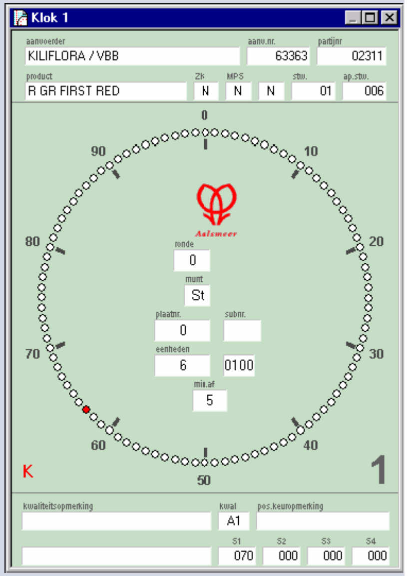
BPS 1000 (1997-)



- Organisation: GAO, Germany
- Domain: Bank note processing
- Tools: The VDM-SL Toolbox
- Experience:
  - Better understanding of sensor data
  - Errors identified in other code
  - Savings on maintenance
- Statement:
  - VDMTools provides unparalleled support for design abstraction ensuring quality and control throughout the development life cycle.

Flower Auction (1998)

iha.dk

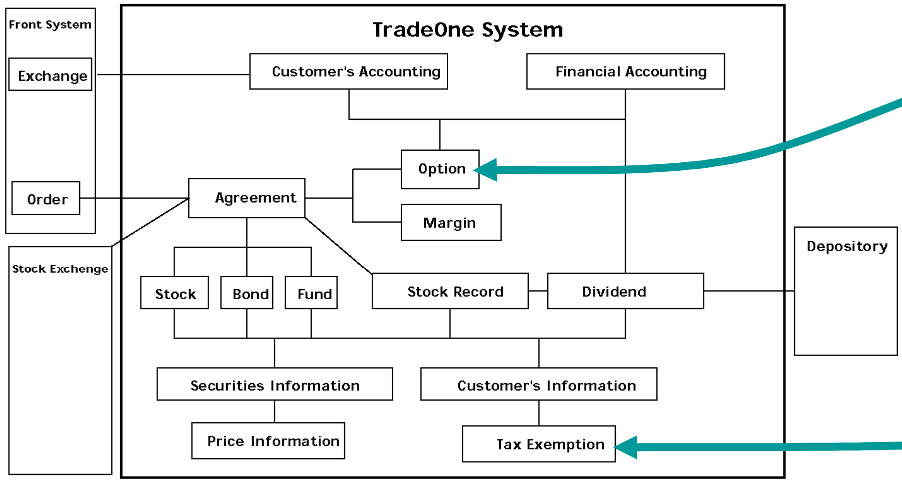


- Organisation: Chess, The Netherlands
- Domain: Financial transactions
- Tools: The VDM++ Toolbox
- Experience:
  - Successful combination of UML and VDM++
  - Use iterative process to gain client commitment
  - Implementers did not even have a VDM course
- Statement:
  - “The link between VDMTools and Rational Rose is essential for understanding the UML diagrams”

TradeOne, CSK, 2000 - 2001

iha.dk

- Full TradeOne system is 1.3 MLOC system
- Mission-critical backbone system keeping track of financial transactions conducted
- Used by securities companies and brokerage houses



Options Subsystem handles the business process for trading options. Modelled in VDM++

Tax exemption subsystem has particularly complex regulations to implement. Modelled in VDM++.

TradeOne Cost Effectiveness

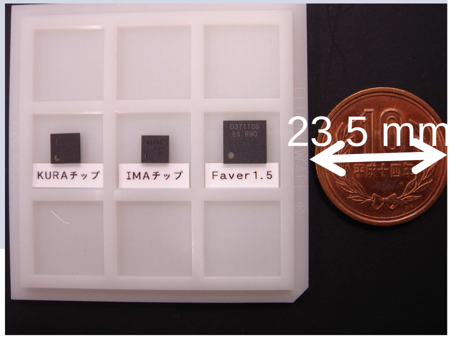
iha.dk

Subsystem	COCOMO estimate	Real time	Time saving
Tax exemption	Effort:38.5 PM Schedule:9M	Effort:14 PM Schedule: 3.5 M	Effort:74% Schedule:61%
Options	Effort:147.2 PM Schedule:14.3M	Effort: 60.1 PM Schedule:7M	Effort: 60% Schedule: 51%

The FeliCa Mobile Chip Project

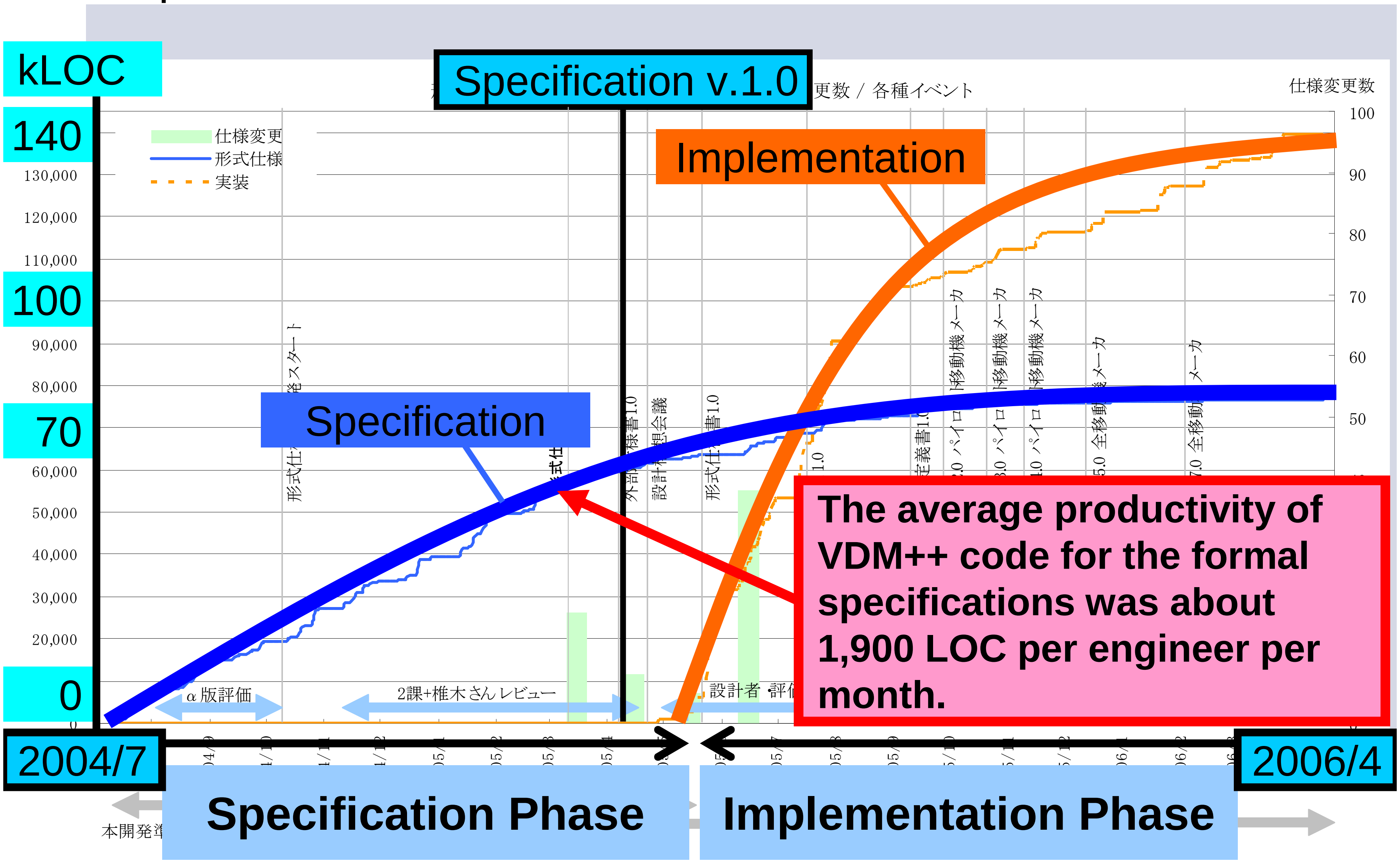
iha.dk

- Mobile FeliCa IC chips can be embedded inside mobile phones
- Used for different on-line services including payment
- Uses Near-Field-Communication technology
- Used for example for metro ticking in Tokyo
- The IC Chips contains an operating system as firmware for 50 million mobile phones
- This is fully developed using the VDM++ technology
- Between 50 and 60 people in total on the project

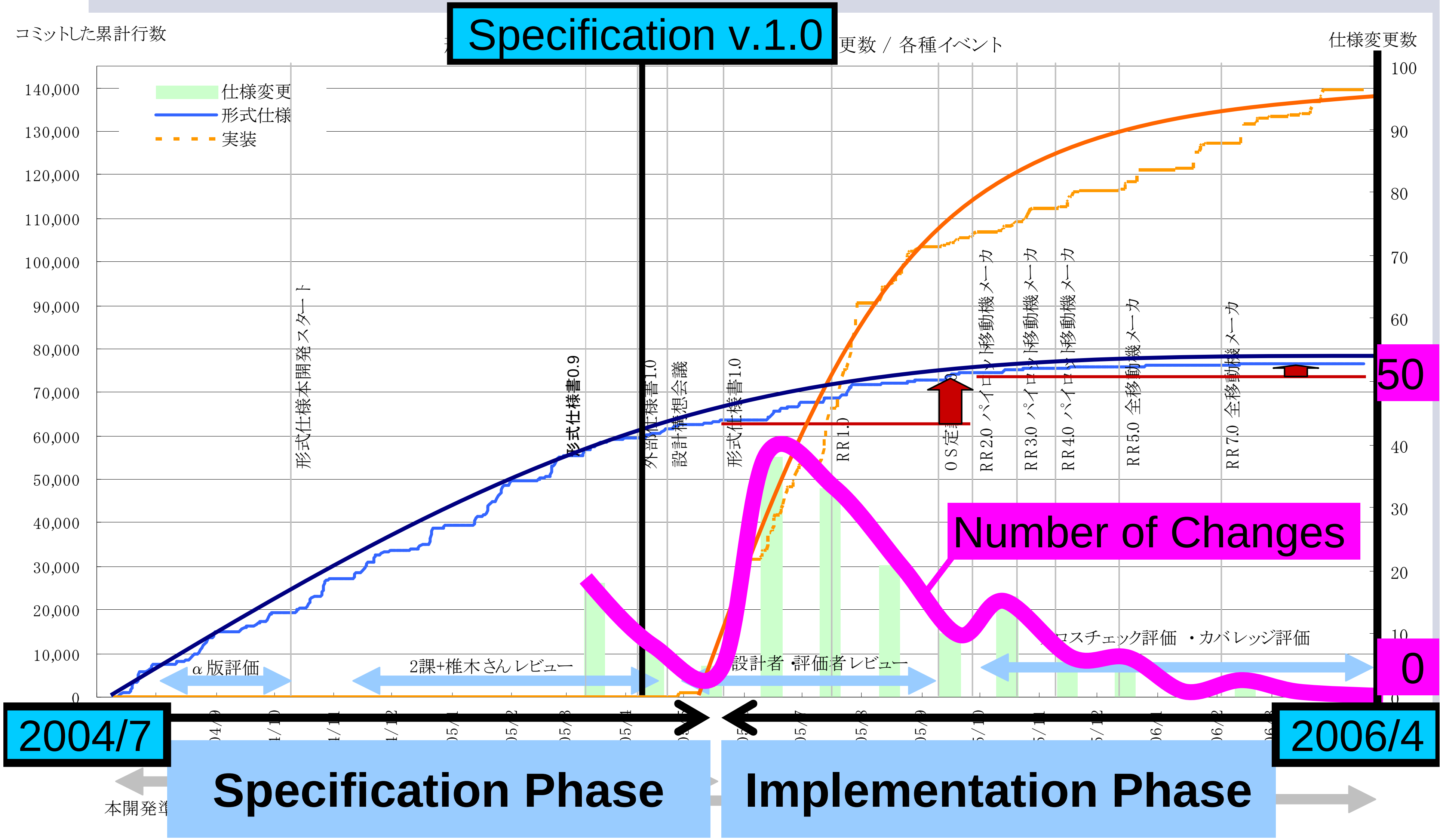


Specification and Implementation Growth

iha.dk



Number of Changes



Overview of Formal Methods

iha.dk

- ✓ **Selected Industrial VDM Projects**
- ➢ **A Survey of Industrial FM Applications**
- **Expected Future use of Formal Methods**

Background: FM industrial survey

iha.dk

- Different FM stakeholders know about different subsets of industrial applications
- FM is still not widely used in the software industry
- Many different surveys/reports about FM 10-15 years ago

- What has happened since then?
- Are there anything we can do to change the uptake of FM?

7 Myths, Anthony Hall, 1990

1. Formal methods can guarantee that software is perfect
2. Formal methods are all about program proving
3. Formal methods are only useful for safety-critical systems
4. Formal methods require highly trained mathematicians
5. Formal methods increase the cost of development
6. Formal methods are unacceptable to users
7. Formal methods are not used on real large-scale software

Questions troubling us in the 1990s...

iha.dk

- **Methods**

  Are methods powerful enough for real problems?
- **Tools**

  Are tools “industry-strength” and do they integrate?
- **Education and Training**

  Do graduate engineers appreciate the technology?
- **Deployment**

  How do you seek take-up? Convincing evidence? Persuading managers or engineers?

Findings from Craigen et al. (93)

iha.dk

1. Formal methods are maturing
2. Formal methods are applied for systems of significance
3. The primary use of formal methods vary between applications
4. Regulators advocate the use of formal methods
5. Tool support is neither necessary nor sufficient
6. Technology transfer is in progress
7. Skills are building slowly
8. Formal methods are applied in a few cases at code level
9. No generally accepted cost model exists

Recommendations from Craigen et al

iha.dk

1. Improved integration of formal methods
2. Ruggedized formal methods tools are needed
3. Making formal methods easier to understand for newcomers
4. Formal methods needs to evolve with computer science trends
5. Regulatory use of formal methods require improved proof support
6. Formal methods needs to incorporate real-time, concurrency and asynchronous processes
7. Technology transfer needs to be broader

Findings by Austin and Parkin (93)

Reasons why formal methods are not used more widely in industry

1. Lack of commercially supported tools
2. No convincing demonstration of cost effectiveness
3. Many of the barriers are symptoms of the process of change

Suggested solutions

1. An education programme to enable process changes
2. Case studies that can demonstrate cost-effectiveness
3. Research in metrics and data collection to support this
4. Efforts to get VDM and Z standardized ASAP

Management guidelines from NASA (95)

iha.dk

Volume 1: Planning and technology insertion

- Integrating formal methods into development process
- Establishing formal methods on a project
- Selected list of formal methods and tools

Volume 2: A practitioner's companion

- Practical application of formal methods
- Use of formal methods in relation to requirements
- Technical introduction to models
- Formal specification
- Analysis of formal specifications
- SAFER example in PVS

Applications of FMs (Bowen&95) iha.dk

Application	Domain	Formalisms	Authors
Darlington	Nuclear	Discrete Math	Parnas
Sizewell B	Nuclear	MALPAS	Bruns, Anderson
Tektroinix	Oscilloscope	Z	Garlan, Delisle
STV	Voting security	VDM-SL	Mukherjee, Wichmann
CICS	Transaction Proc.	B	Hoare
AAMP5	Microprocessor	PVS	Srivas, Miller
Railroad Gate	Railway	Nqthm	Young
CombiCom	Railway Logistics	VDM++	Dürr, Plat, deBoer
Railway Signalling	Railway	B	Dehbonei, Mejia
A330/340	Avionics	Z	Hamer, Peleska
OS Kernel	Security	Larch	Guaspari et al.
Attitude Monitor	Avionics	Z+RTL	Coombes et al.
Trusted Gateway	Security	VDM-SL	Fitzgerald et al.
Hazardous Materials	Critical Systems	Z+MALPAS	Hamilton
Switching	Telecoms	Z+Statecharts	Mataga, Zave

What has changed in 10 years?

iha.dk

- **Tools capabilities** (but instability in tools area and mainly pre-competitive quality)
- **ISO Standards have been approved** (with very limited effect, because fewer industrial tools supporting these now)
- **Verification advances** (Moore's law have helped but appears to be separate communities)
- **Regulators play a less active role** (FM still required at high levels)
- **Some FMs now incorporate real-time, concurrency and asynchronous processes** (however typically this implies less formal analysis)

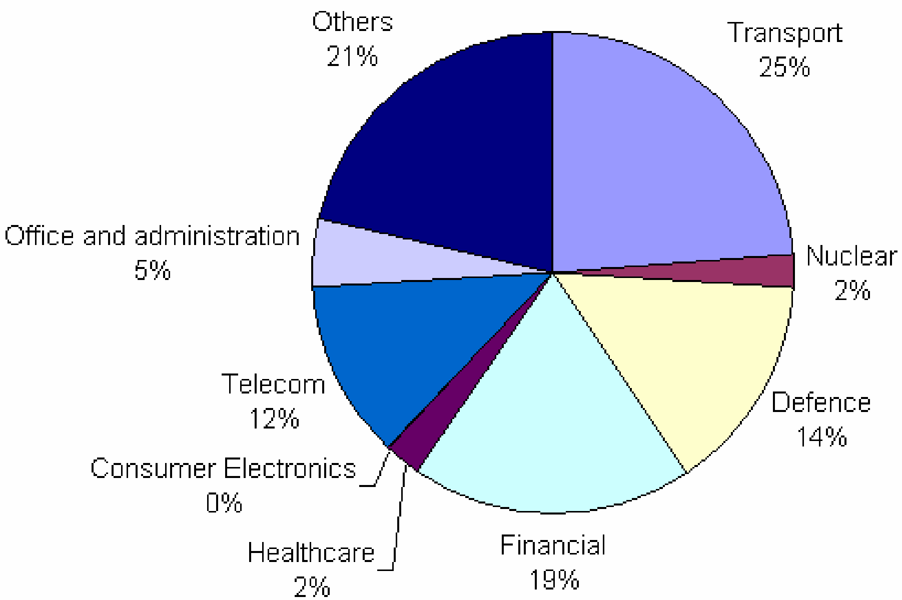
What has not changed?

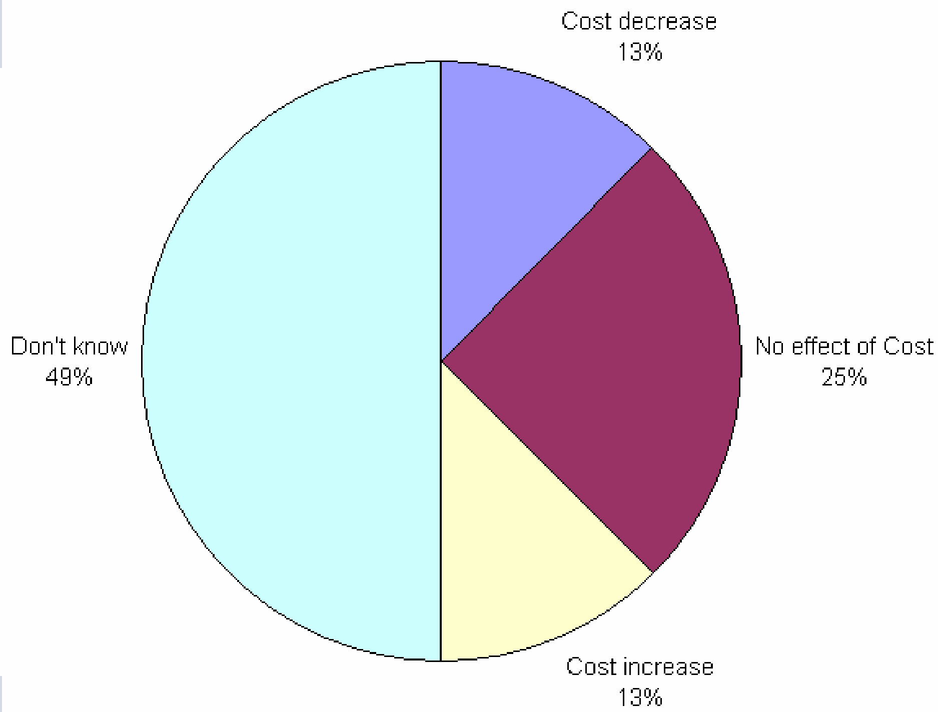
iha.dk

- **Still no appropriate cost models** (also true for OO)
- **Still a lack of commercially supported tools** (with notable exceptions)
- **FMs still used for significant systems** (mainly demanded by standards)
- **Champions are needed at different levels inside industrial organisations**
- **Formal methods are still difficult for newcomers**
- **Formal methods still lag behind computer science trends** (SOA, design patterns,…)
- **The process of change is still an issue for FMs**

Initial response to FM survey

- Very limited feedback so far: 31 applications
- The hope is to get more than 100 applications
- So please help us with adding more to the survey!





Revisiting questions troubling us in the 1990s...

iha.dk

- **Methods**

  Are methods powerful enough for real problems?

  Yes but it is important to use them when it is advantageous

- **Tools**

  Are tools "industry-strength" and do they integrate?

  Generally no, and integration must be made pragmatic

- **Education and Training**

  Do graduate engineers appreciate the technology?

  Partly, but most students are trained with too simple examples and lack the skill of abstraction and precision

- **Deployment**

  How do you seek take-up? Convincing evidence? Persuading managers or engineers?

  As a community we are still pour in industrial deployment of FM

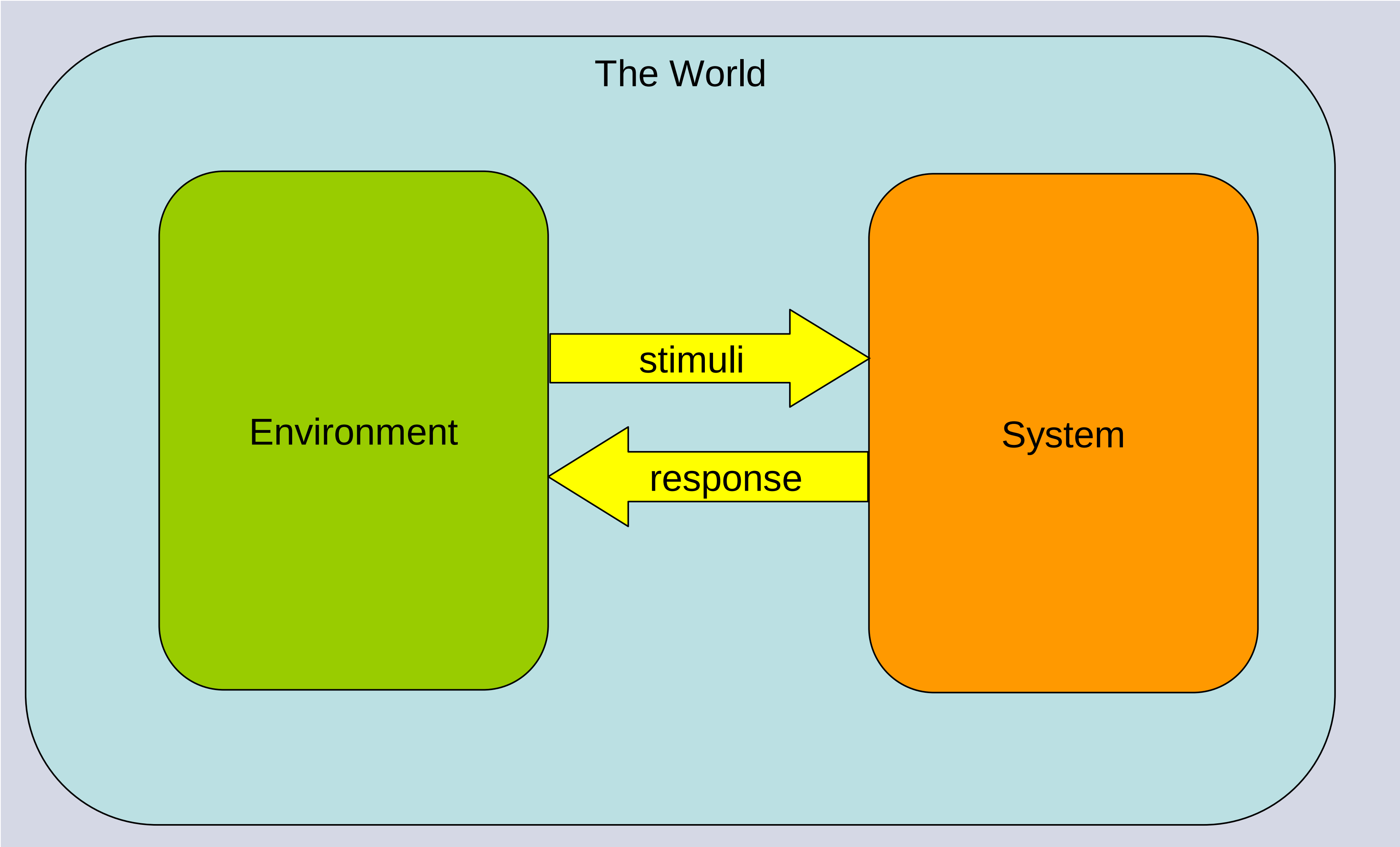
Overview of Formal Methods

iha.dk

- ✓ **Selected Industrial VDM Projects**
- ✓ **A Survey of Industrial FM Applications**
- ➢ **Expected Future use of Formal Methods**

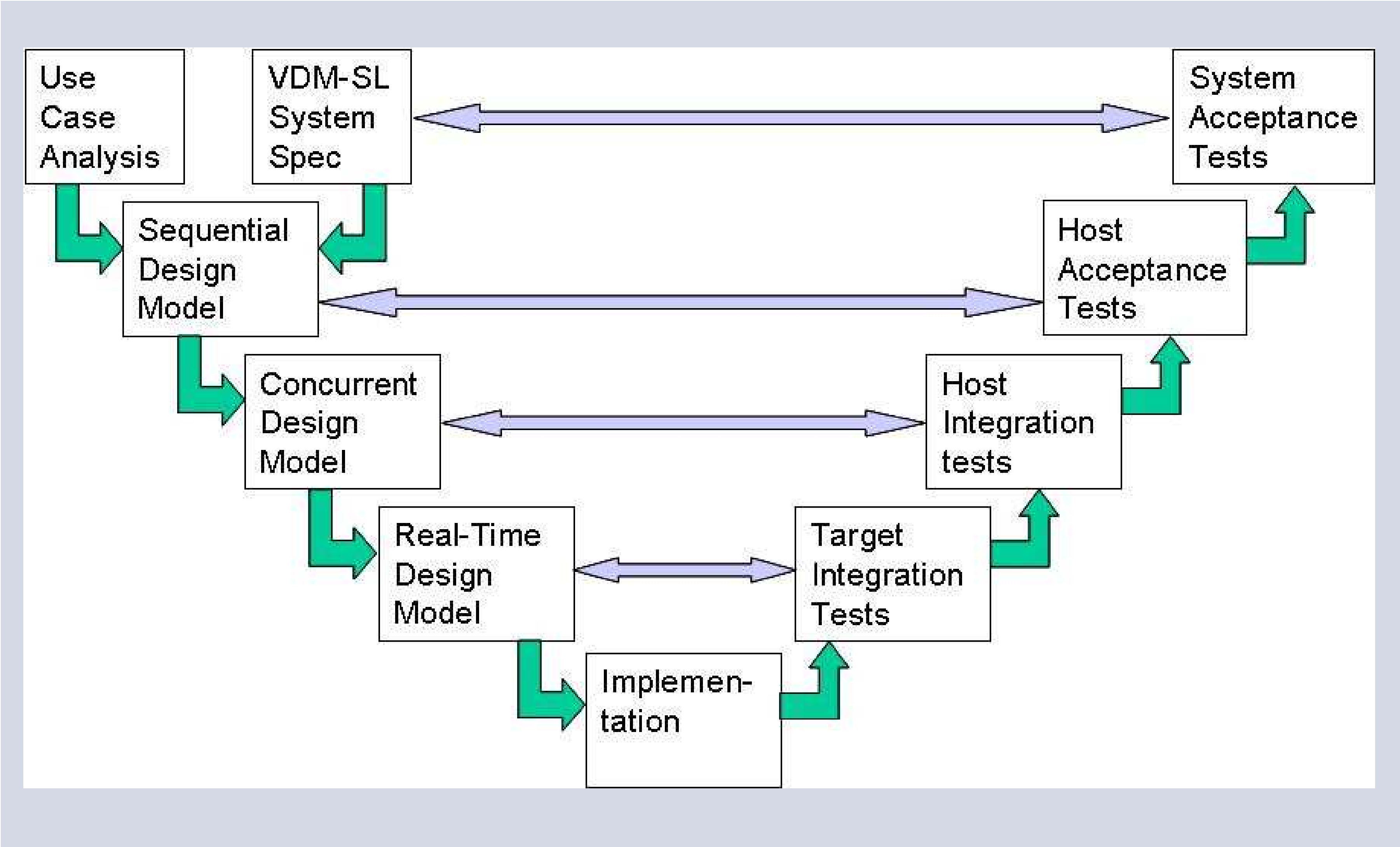
Reactive Systems Nature

iha.dk



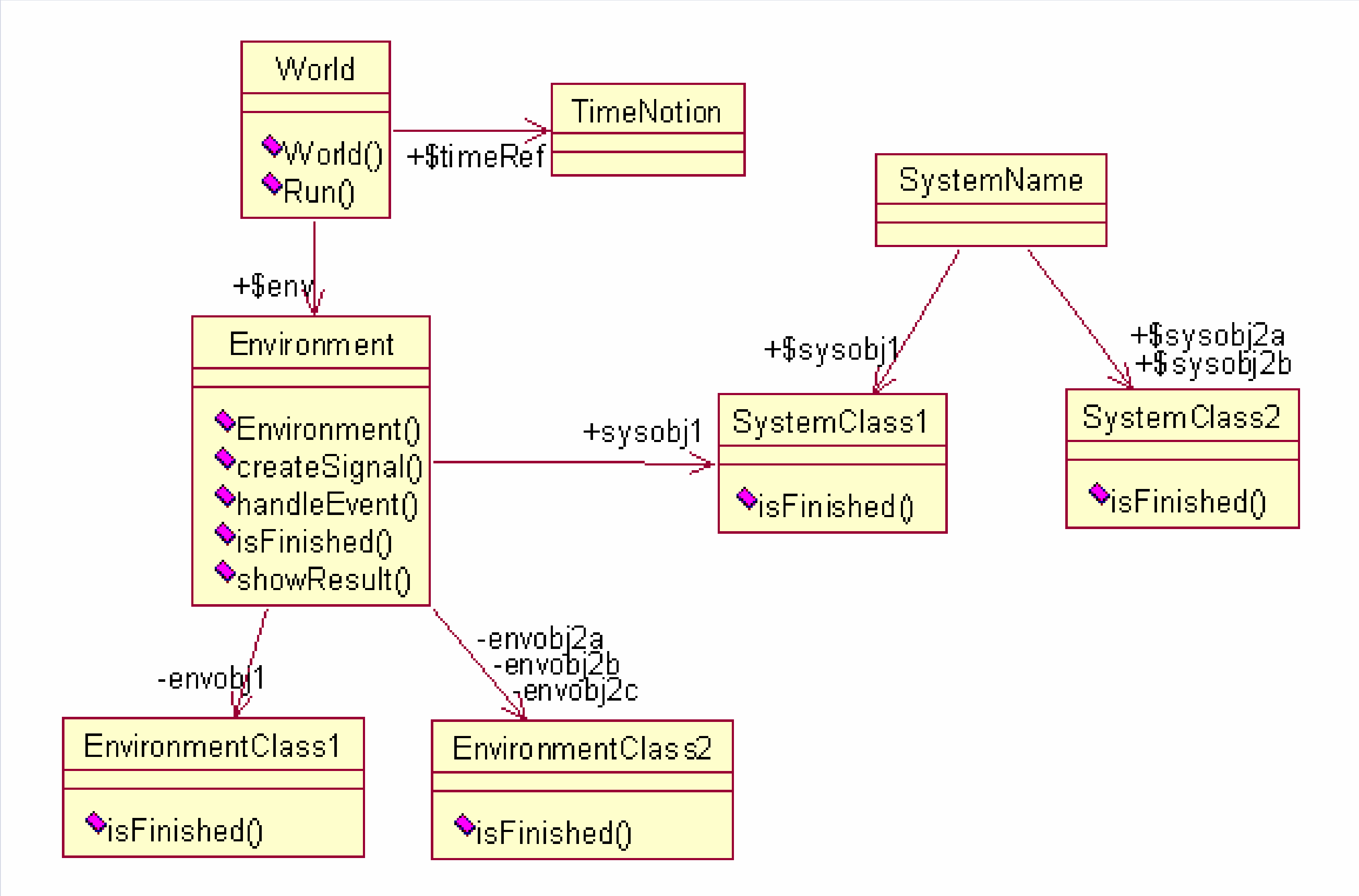
Overview of Development Process

iha.dk



Sequential Design Model

iha.dk



Concurrent Design Model

iha.dk

- Similar to sequential design model but
  - Identification of threads
  - Determine necessary communication
  - Establish synchronization points
  - Validation of model
- Typical design structure
  - Flow of control is distributed
  - Synchronization using permission predicates and mutex
  - `isFinished` operations become skip with permission predicates
  - A simple `Timer` class is replaced with the `TimeStamp` class

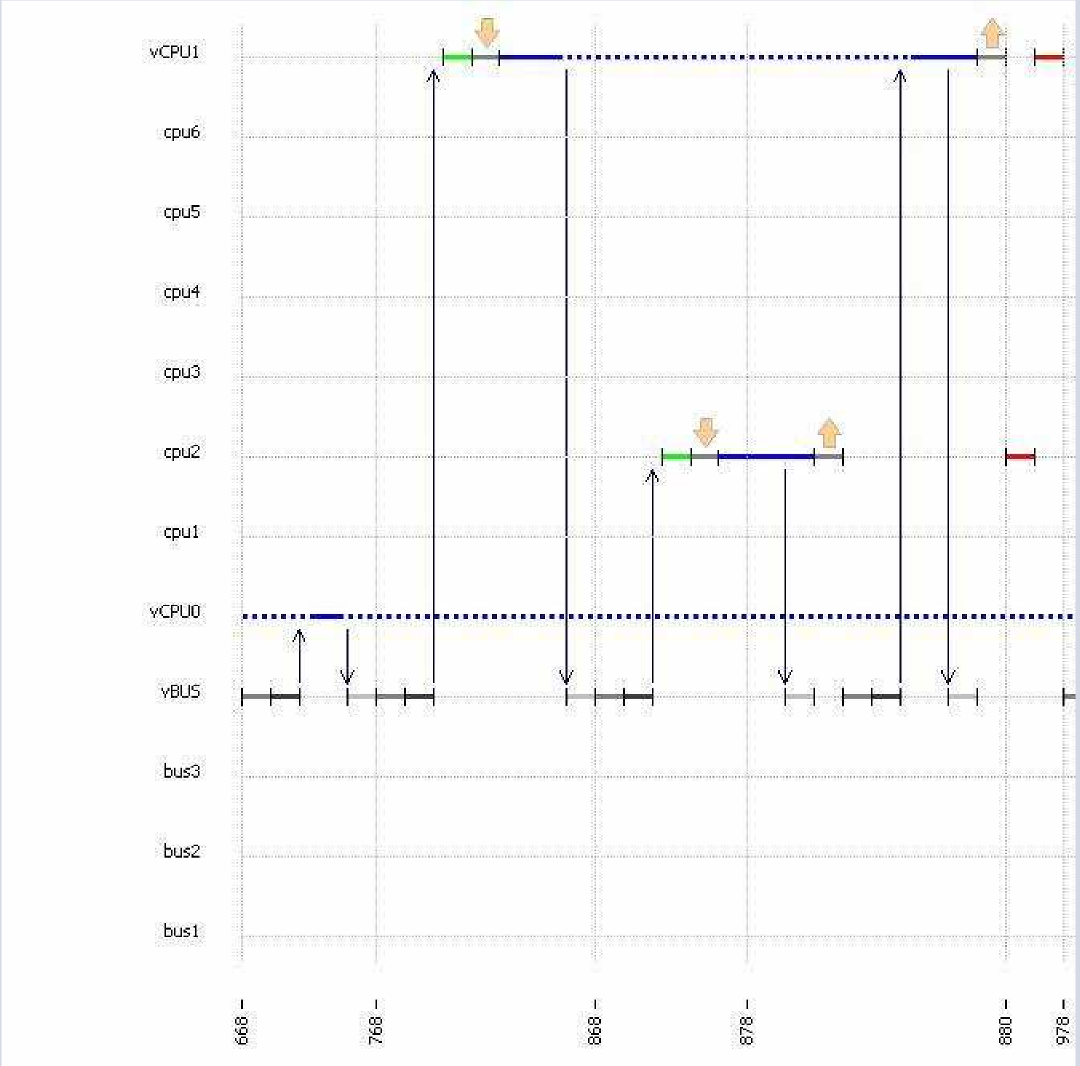
Concurrent Real-Time and Distributed Design Model

iha.dk

- Timing built in:
  - Use of default durations
  - Use of duration and cycles statements
- Typical Design Structure
  - `SystemName` is now turned into a system
  - `CPU`'s and `BUS`'es are introduced inside `SystemName`
  - `Environment` may be turned into a system
  - Some operations are made asynchronous
  - Some `Step` like threads are made `periodic`
  - Explicit use of `TimeStamp` is removed

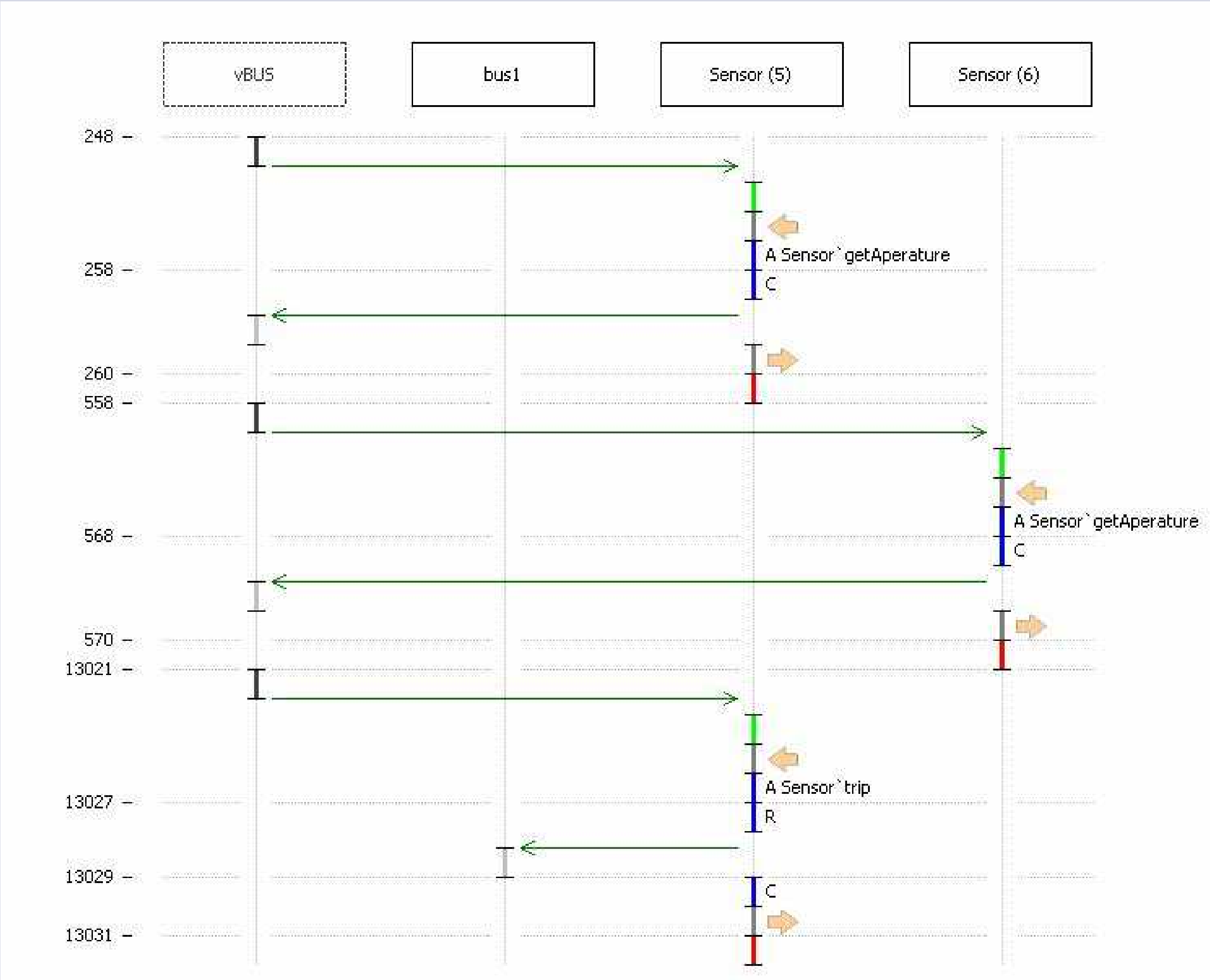
Execution Overview in showtrace

iha.dk



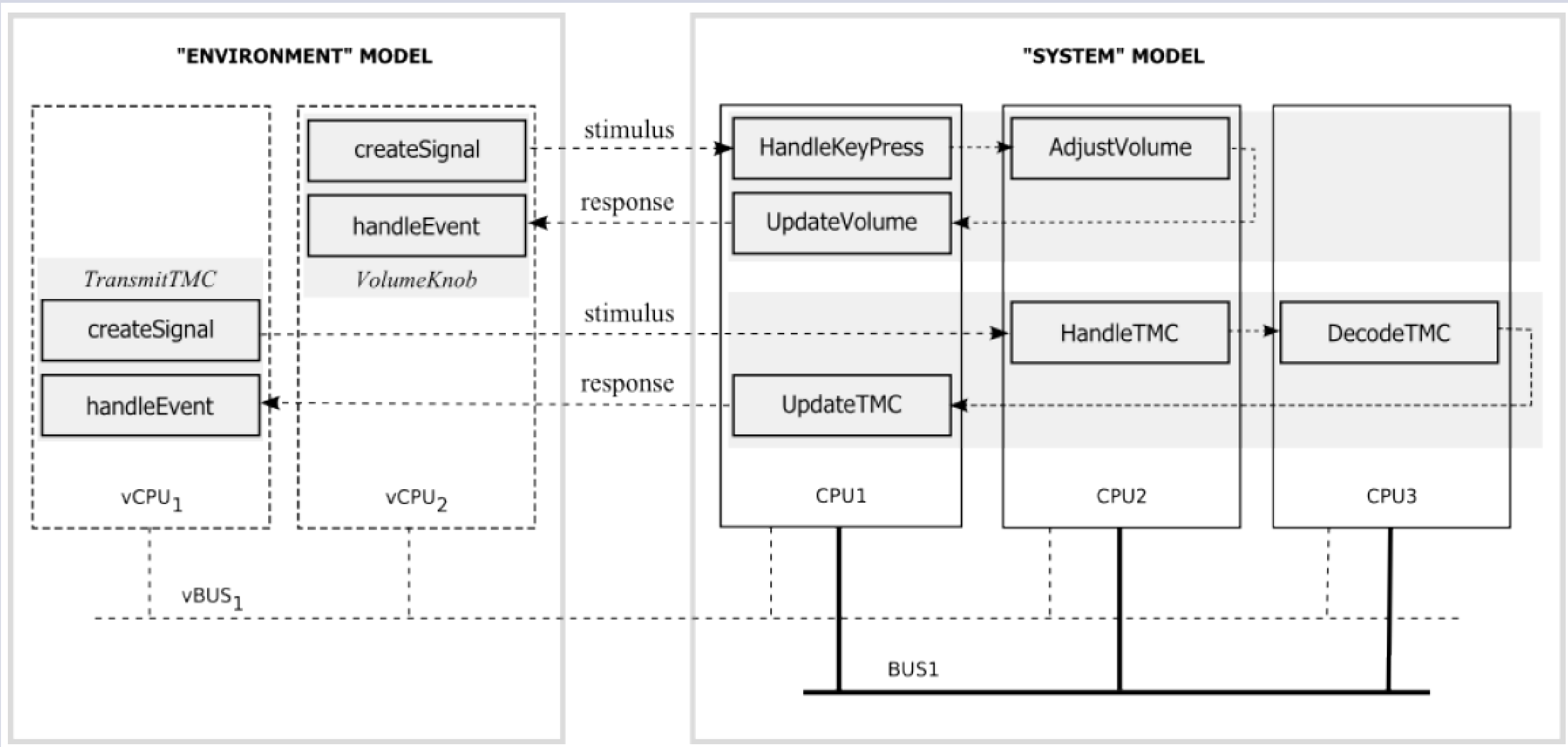
Detailed Overview at one CPU

iha.dk



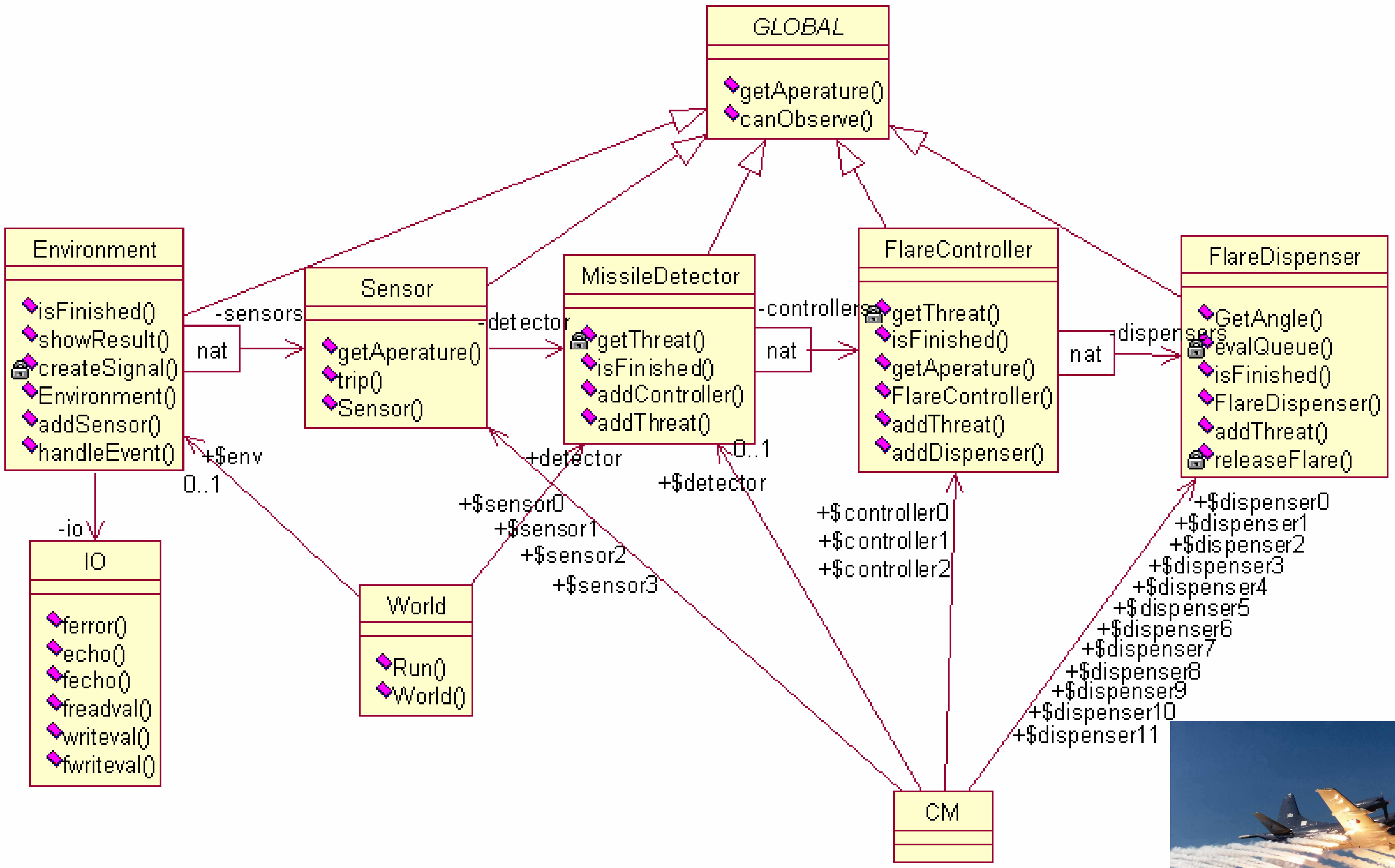
In-Car Radio Navigation System

iha.dk



The Counter Meassures System

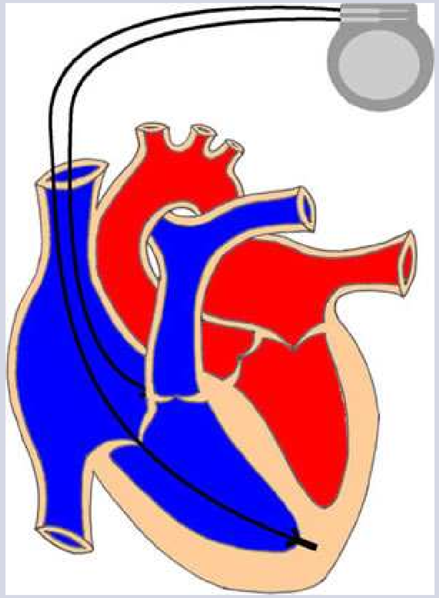
iha.dk



The Pacemaker Challenge

iha.dk

- A Safety-Critical Application
- Report over project made by Hugo Macedo
- 4 different models made in VDM
  - High-level VDM-SL model
  - Sequential VDM++ model
  - Concurrent VDM++ model
  - Real-time distributed VDM++ model
- Follow VICE Guidelines + new validation conjectures over timed traces
- http://www.cas.mcmaster.ca/sqrl/pacemaker.htm

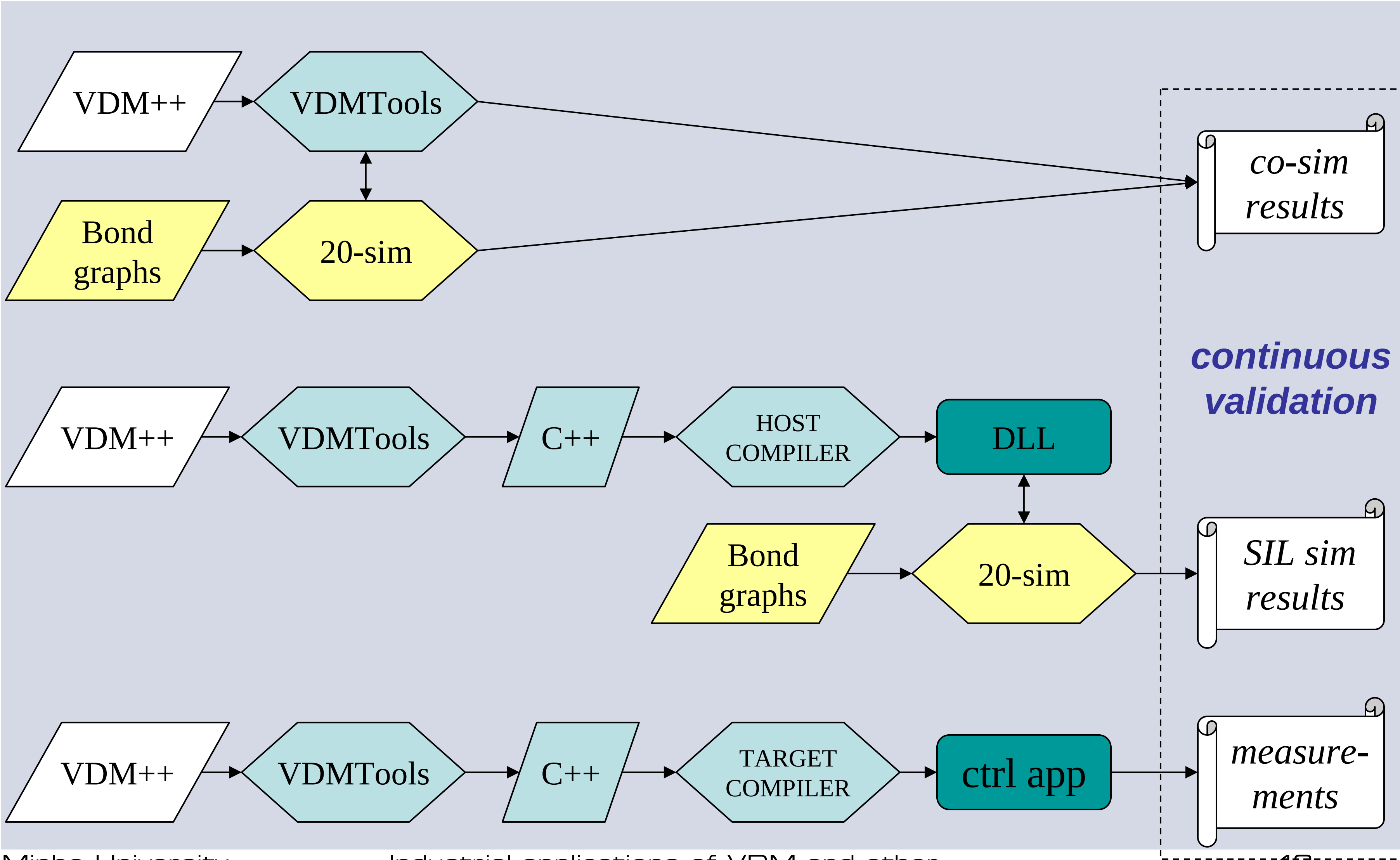


Beyond the Ordinary:
Design of Embedded Real-time Control

iha.dk

- BODERC project @ ESI
- Sept 2002 - Apr 2007
- Multi-disciplinary design
  - mechanics
  - electronics
  - software
- High-tech systems focus
- Early life cycle trade-off analysis
- Industry as a laboratory
- http://www.esi.nl/boderc

Printer paper path - case study



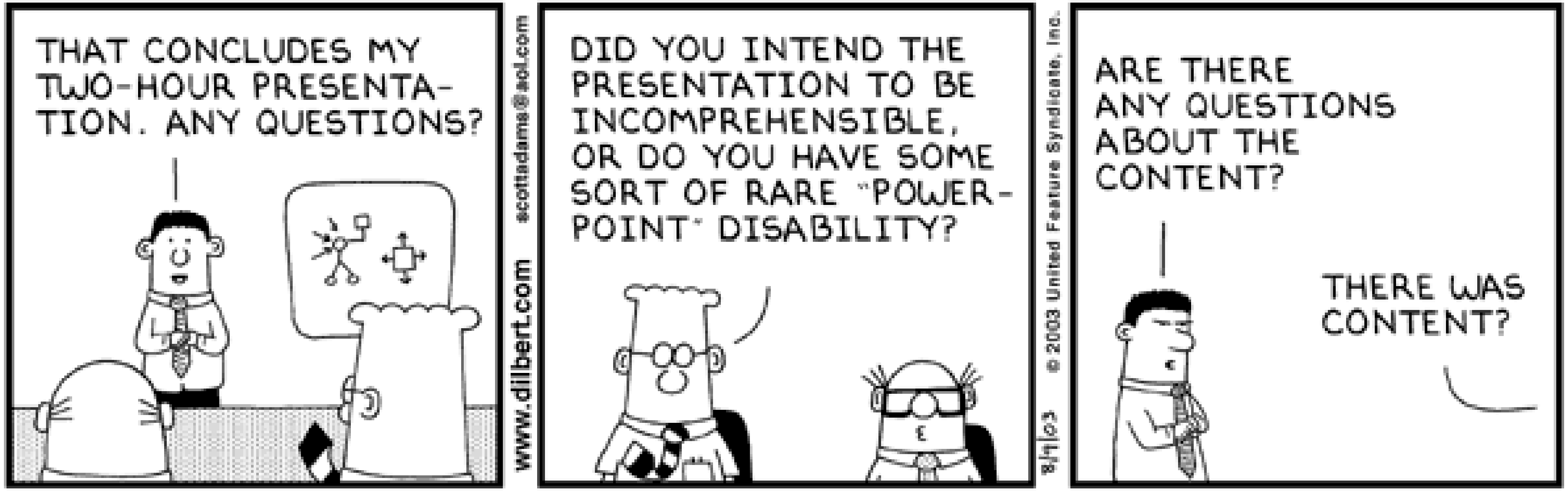
Looking ahead for industrial use

iha.dk

- FM tool features must be worthwhile for industrial applications (balance between time versus insight)
- Prototype tools are often used because of funding schemes
  - EUs FP7 ESPRIT focus on new research rather than ESSI-like process improvement projects
  - Hindrance of cost-efficient case studies
- More systematic exchange of people between academia and industry could create more champions
- Pragmatic integrations of different FMs and other kinds of models is important
- Essentially FMs with zero additional cost are needed
- Companies will get more interested if they see competitors using formal methods technology

Any Questions?

iha.dk



Thank You for Your Attention

http://home0.inet.tele.dk/pgl/peter.htm
http://www.vdmtools.jp/en