



iha.dk

A Survey of Industrial Applications of Formal Methods

Professor Peter Gorm Larsen
Engineering College of Aarhus

(pgl@iha.dk)

joint work with Juan Bicarregui and John Fitzgerald



Background: FM industrial survey iha.dk

- Different FM stakeholders know about different subsets of industrial applications
- FM is probably 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?



iha.dk

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...



- **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



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) iha.dk

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?

- **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?

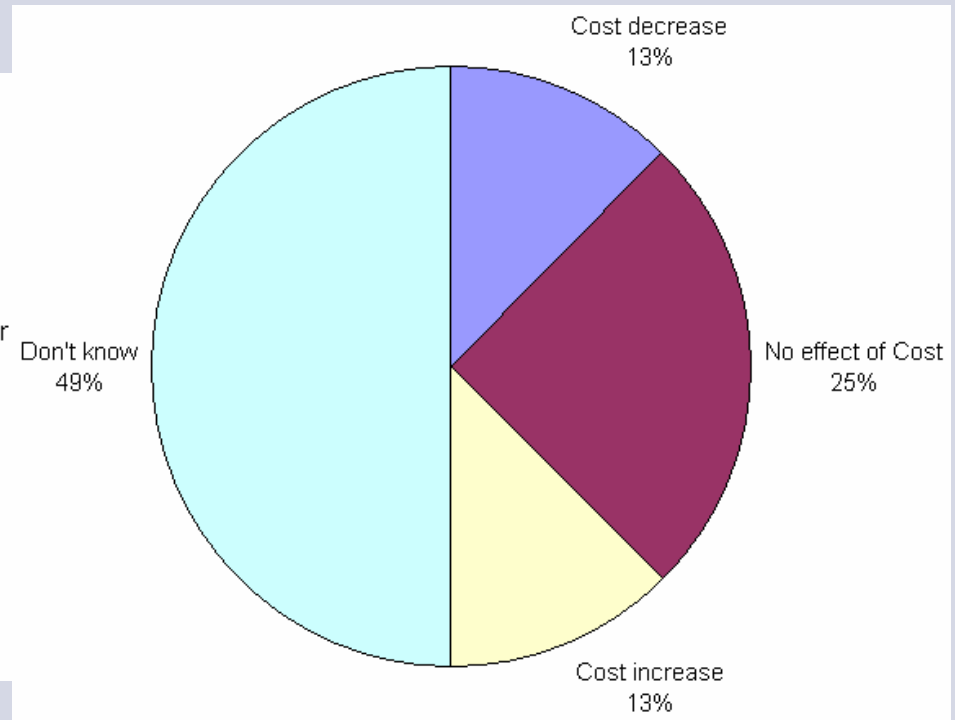
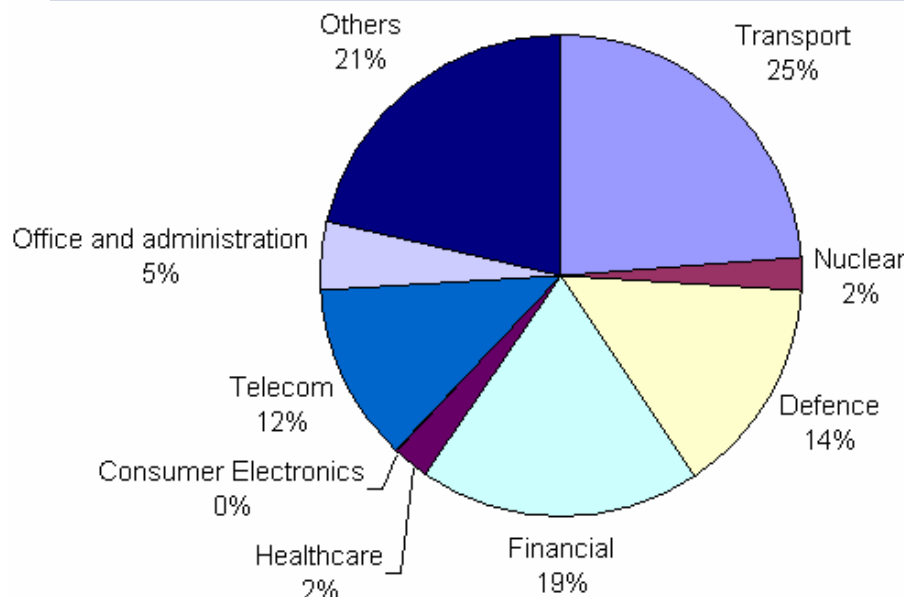
- **Still no appropriate cost models** (also true for OO)
- **Still a lack of commercially supported tools** (with notable exceptions)
- **FMs still used for significant systems** (mainly demanded by standards)
- **Champions are needed at different levels inside industrial organisations**
- **Formal 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**



iha.dk

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 poor in industrial deployment of FM

Looking ahead for industrial use

- 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



iha.dk

Today at IDay we will see

- **Application of a Formal Specification Language in the Development of the "Mobile FeliCa" IC Chip Firmware for Embedding in Mobile Phone**, Taro Kurita, FeliCa Networks Inc., Japan
- **Formal Methods for Trustworthy Skies: Building Confidence in the Security of Aircraft Assets Distribution**, Scott Lintelman, Boeing Phantom Works, USA
- **Safe and Reliable Metro Platform Screen Doors Control/Command Systems**, Thierry Lecomte, ClearSy, France
- **An industrial case: pitfalls and benefits of applying formal methods to the development of a network-centric RTOS**, Eric Verhulst, Open License Society, Belgium
- **Software Engineering with Formal Methods: Experiences with the development of a Storm Surge Barrier Control System**, Klaas Wijbrans, Acision, The Netherlands



iha.dk

Thanks for your attention!

Please help us with contributions!

<http://www.jiscmail.ac.uk/cgi-bin/surveys.cgi?A=hp&LMGT1=FMSURVEY>

Any questions?