AARHUS
UNIVERSITY
DEPARTMENT OF ENGINEERING

OCTOBER 2012

FORMAL METHODS IN INDUSTRY

PETER GORM LARSEN (PGL@IHA.DK)
PROFESSOR
(IN COLLABORATION WITH BICARREGUI, FITZGERALD, AND WOODCOCK)

FORMAL METHODS IN INDUSTRY

- **Example Industrial Projects using FM**
- Review of Industrial Deployment
- Comparison with Japanese IPA findings
- My personal recommendations

EXAMPLE INDUSTRIAL PROJECTS

Selected VDM projects

- ConForm
- CAVA
- Dutch DoD
- BPS 1000
- Flower Auction
- TradeOne
- FelicaNetworks

- Use of B for railways
- Use of formal methods at Rockwell Collins

CONFORM (1994)

- 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"

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)

- 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"

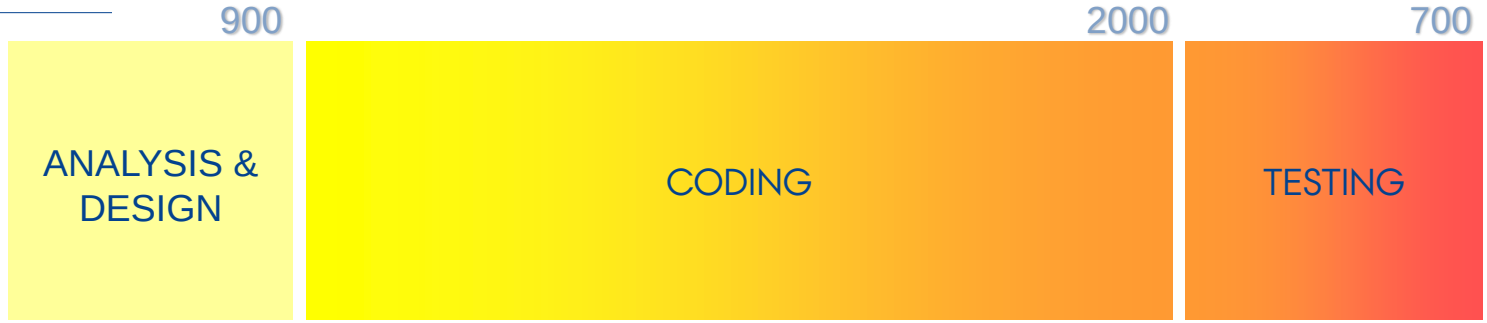
DOD, NL METRICS (1)

	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

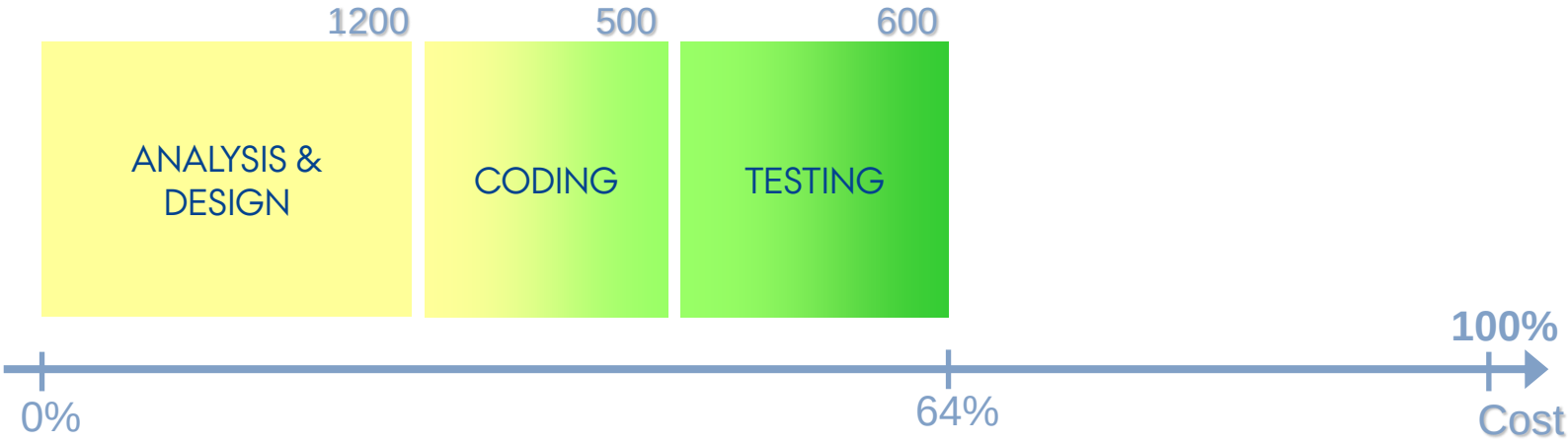
› Estimated 12 C++ loc/h with manual coding!

DOD - COMPARATIVE METRICS

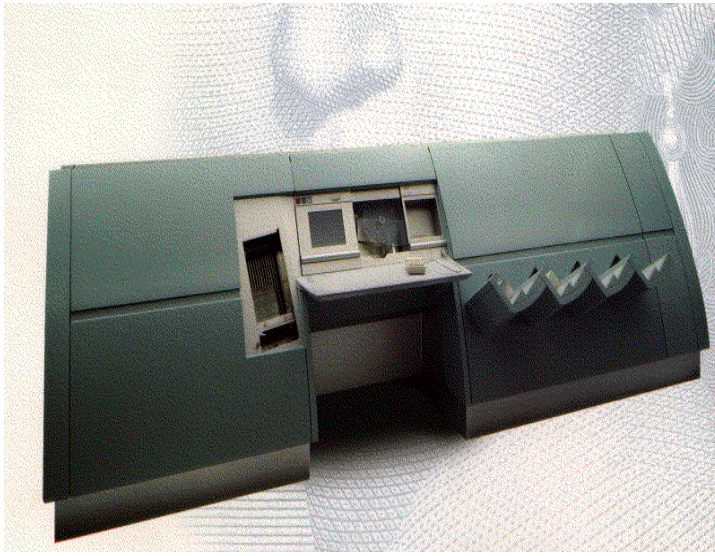
Traditional:



VDMTools®:

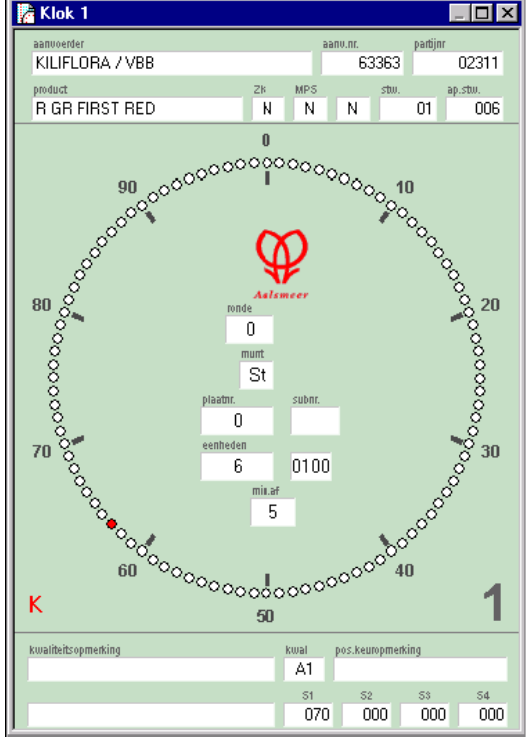


BPS 1000 (1997-)



- 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.

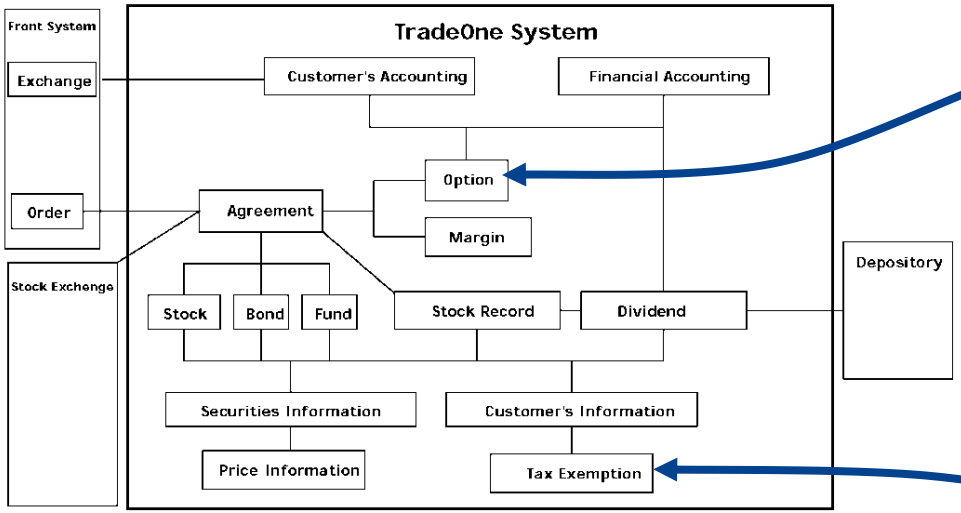
FLOWER AUCTION (1998)



- 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

- 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

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

- 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
- This is fully developed using the VDM++ technology
- More than 50 people in total on the project
- Used in 125 million mobile phones in 2009!

COMPARING THE PROJECTS

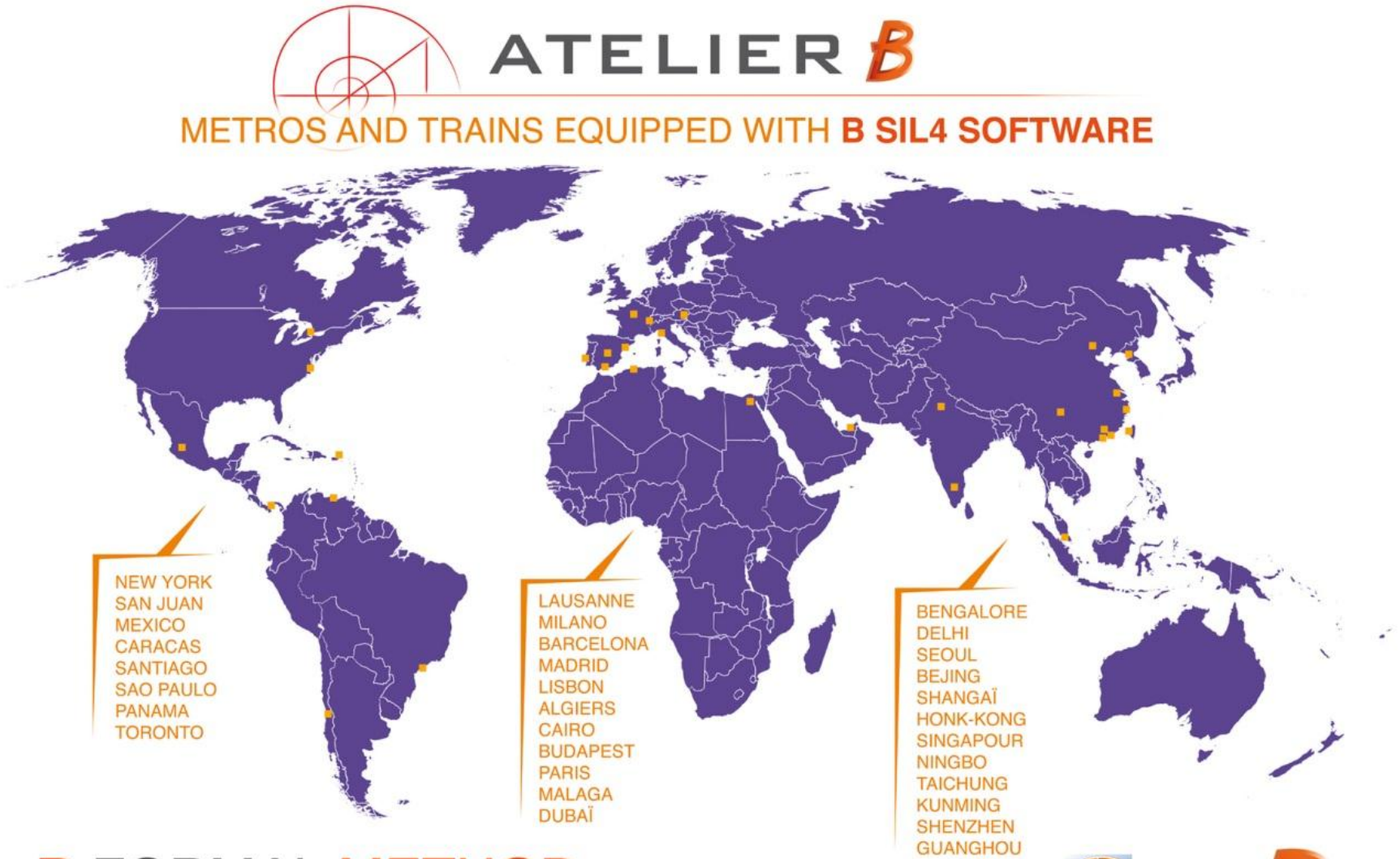
CSK Systems

- Requirements specification written with use cases was modeled using VDM++ (VDM++ modelling team: 2 – 5 people).
- Defect density: 6.25% of the product norm (zero defect since release).
- Productivity: 2.5 times COCOMO prediction.
- Development period: 45% of COCOMO. Finished on schedule.

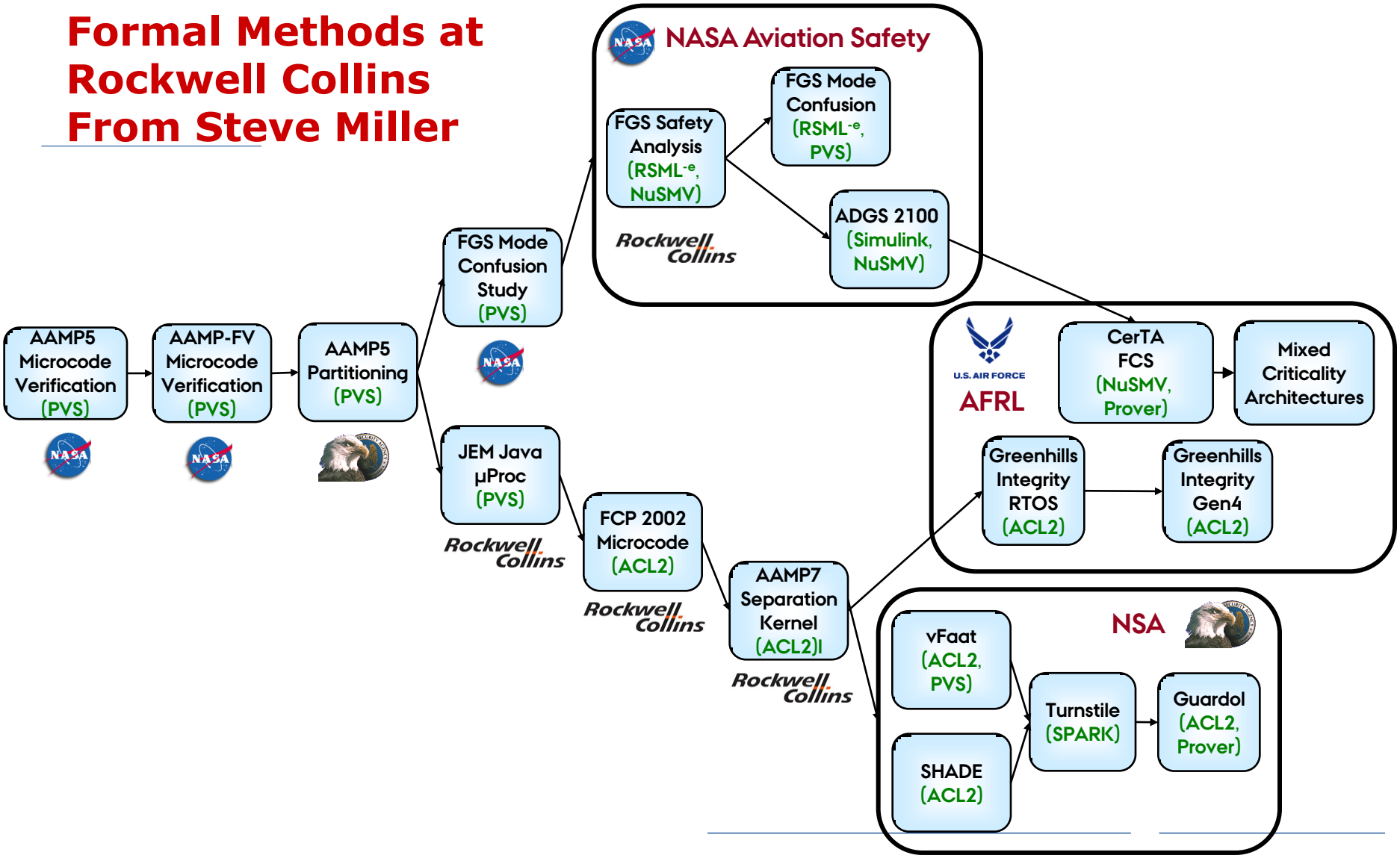
FeliCa Networks

- Operating system of Felica chip firmware modeled using VDM++ (Specification description team: ~20 people).
- Zero defect since release (discovered ~5 times more defects using VDM++ than with conventional review).
- Development period ~3 yrs. Finished on schedule.

USE OF B FOR RAILWAYS



Formal Methods at Rockwell Collins From Steve Miller



FORMAL METHODS IN INDUSTRY

- ✓ **Example Industrial Projects using FM**
- ➢ **Review of Industrial Deployment**
- › Comparison with Japanese IPA findings
- › My personal recommendations

REVIEW OF INDUSTRIAL DEPLOYMENT

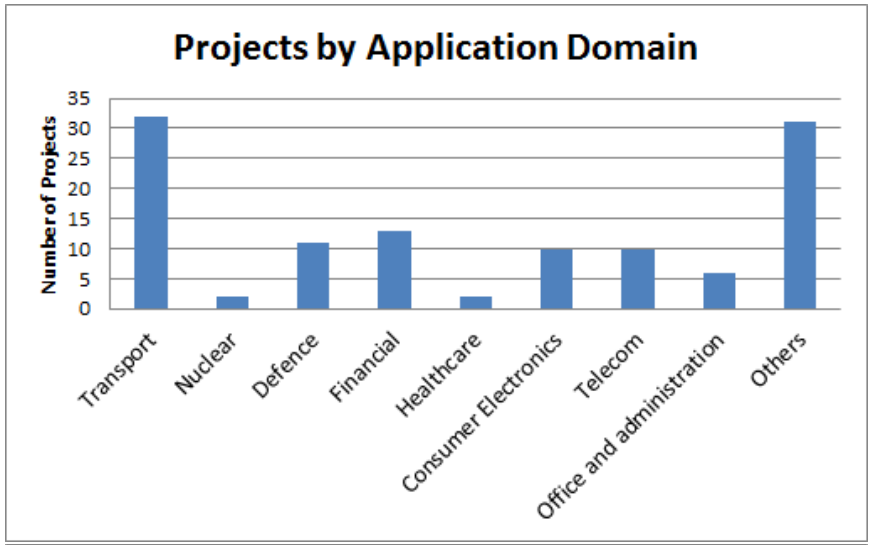
- 2009: first comprehensive review in a decade
- ACM Computing Surveys 41(4)
- Standard reporting format, >60 projects

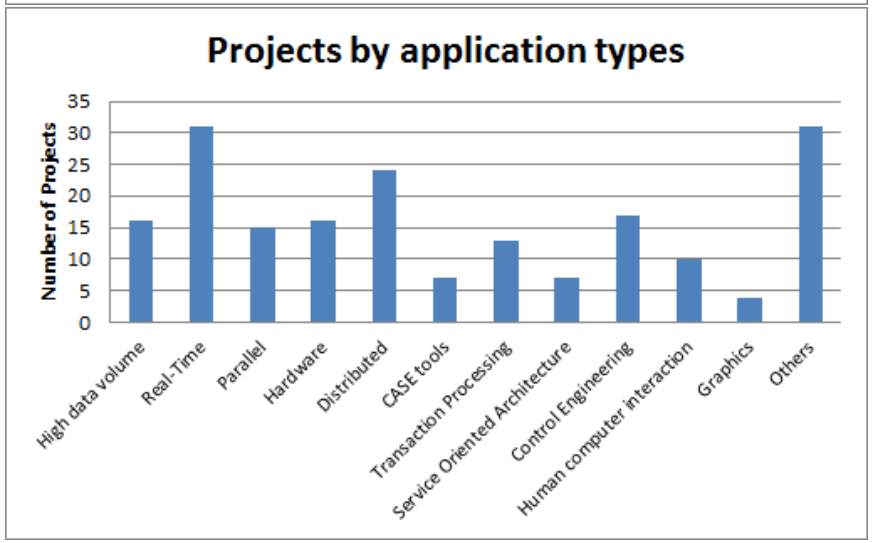
- 2012: extended review
- Common web site: www.fmsurvey.org
- In the Deploy Book (http://rodintools.org/dbook.html)
- Cleaned up data set
- Same format, 98 projects

2009 FINDINGS

- A bright picture: improving use, excellent success stories
- Lightweight approaches dominate
- Tools now critical, increasing automation, but lack usability
- Lack of evidence to support adoption decisions
- case for FMs is risk-based (who believes quantitative evidence?)
- Lack data on second/subsequent use
- Skills & psychological barriers remain high
- Training and education remain vital

2012 STATUS

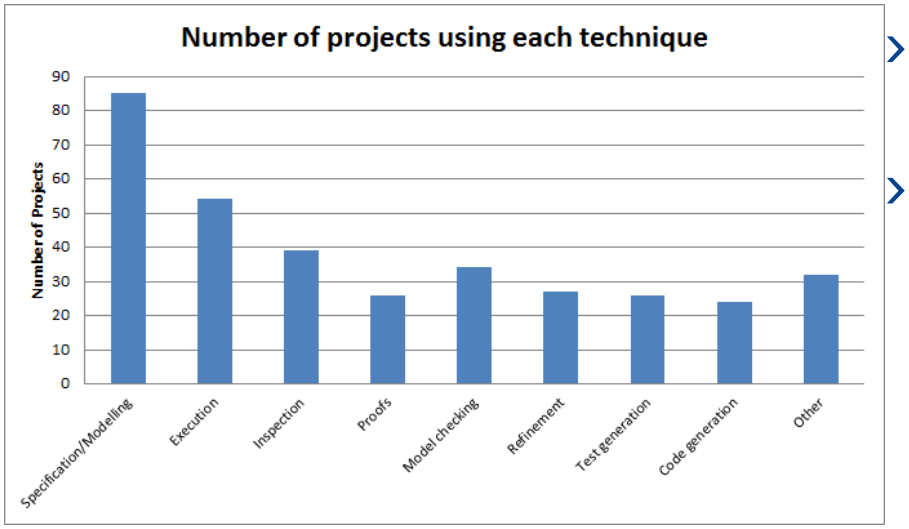




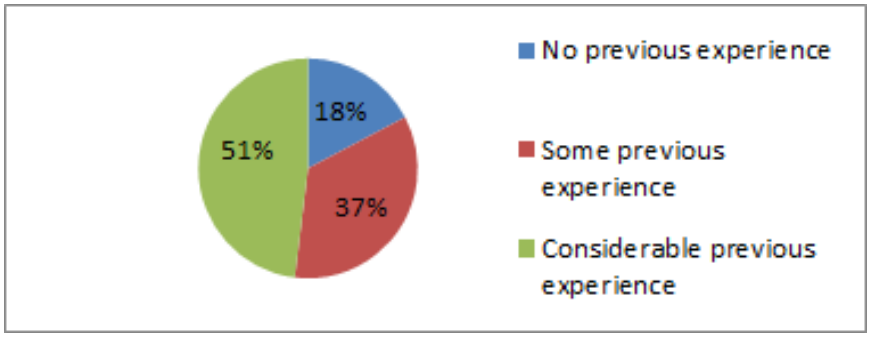
- 98 projects
- Transport and consumer electronics increased

Greater representation for real-time and distributed

2012 STATUS



- Techniques used – distributed broadly as 2009
- Marked increases over time in model-checking and test automation

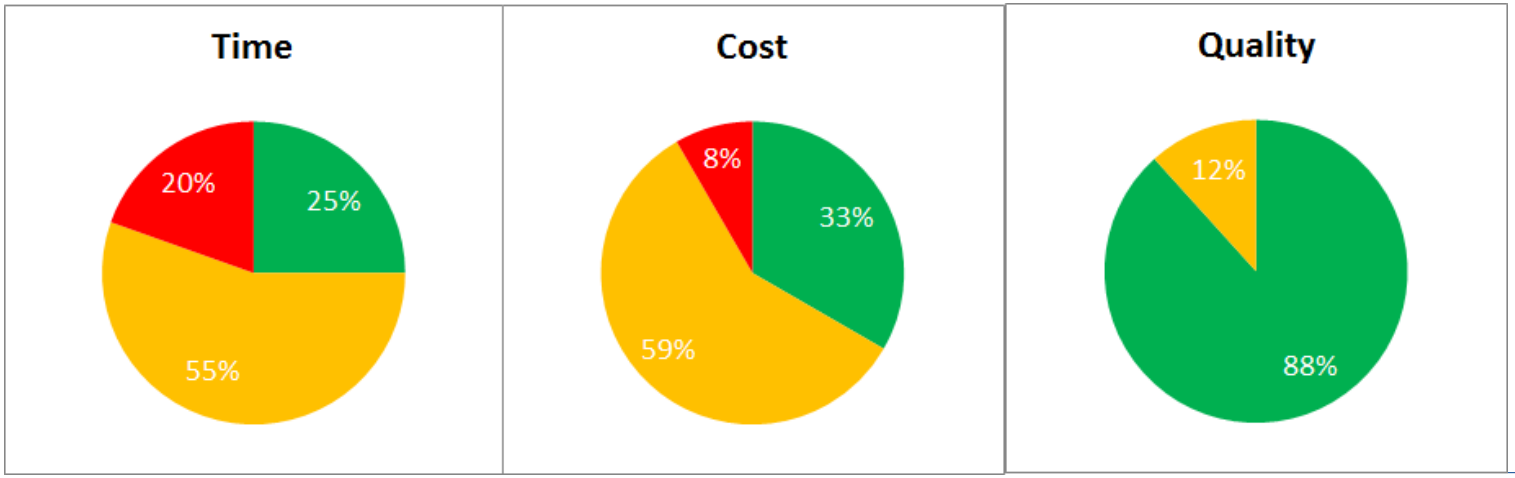


Considerable previous experience (multiple reports from same teams)

Level of training correspondingly (?) low

2012 STATUS

- Duration: 25% report saving, 20% report increase
- Cost: 4:1 improvement to loss
- Large proportion report no effect or don't comment
- Quality much less uncertain
- No negative reports
- Better and cheaper, probably not faster?



2012 STATUS

- Benefits seen in abstraction
- "the formal thinking (or methodology) helps a lot during the development process even if the formal method itself is not fully used."
- In test automation
- "thousands of different parameters to configure the software. [...] An attempt to write test cases [. . .] was a complete failure: the tests cannot be used in practice, since they are not parameterisable [...] A model can easily be made parameterisable and we are therefore able to use the same model to generate test cases for millions of different configurations."
- 80% regarded tools as adequate; 7% disagree (but median start date 2000, overall median 2006)

2012 STATUS

- Intention to use again: 73% positive; 2% negative
  - "…formal methods were used to differentiate our bid and team from competitors; their use is why we won the contract."
  - "This project was a very specialized "bug finding campaign". It required very high skills (which were fortunately available), and therefore we expect that similar methods will never be used on broader scale as "standard techniques" during system development and verification."
  - "…the main barrier is a lack of motivated people with FMs background … Teams should be slightly (+10%) supplemented by FMs specialists … Light-weight techniques and user-friendly tools simplify introduction of FMs."

FORMAL METHODS IN INDUSTRY

- ✓ **Example Industrial Projects using FM**
- ✓ **Review of Industrial Deployment**
- ➢ **Comparison with Japanese IPA findings**
- › My personal recommendations

RECOMMENDATIONS FROM IPA REPORT

1. Using rigorous as the information hub of the project
2. Combining multiple descriptive methods
3. Selecting/tailoring/creating appropriate tools
4. Disclosing the successful cases of adoption proactively

One slide for commenting on each of these

USE FORMAL MODEL AS PROJECT HUB

- Essential to consider how to use models throughout
- Keeping documentation up to date when requirements change
- Tool automation required to make it worthwhile
- Ensure win-win for different stakeholders
- Animation capability of models for less technical stakeholders can be beneficial
- Keep consistent the purpose of model
- Prerequisite: More stakeholders can read the models

COMBINE MULTIPLE METHODS

- Can be a good idea
- Combination between informal and formal best to start with
- Combining different formalisms require skills
- Prerequisite: Knowledge about multiple methods and strengths

SELECTING/TAILORING/CREATING APPROPRIATE TOOLS

- Essential when used as information hub
- Selection depends upon the target use
- Tailoring tools in the small is possible without deep insight
- Creating your own tools requires high skills
- Determine the kinds of tailoring needed
- Prerequisite: optimal to have alliance with tool expert
- Organizations like Fujitsu already have a tool expert, probably without knowing about it!

DISCLOSE SUCCESSFUL CASES

- This would be great!
- In fact this is done at different level (e.g. VDM examples repositories and survey of industrial FM)
- Many companies are very reluctant to share
- So this one will unfortunately be difficult to accomplish
- Unless other incentives are made from government

FORMAL METHODS IN INDUSTRY

- ✓ **Example Industrial Projects using FM**
- ✓ **Review of Industrial Deployment**
- ✓ **Comparison with Japanese IPA findings**
- ➢ **My personal recommendations**

CHALLENGE: BRIDGING THE GAP

Academia

- Makes Δ of XYZ technology
- Demonstrate toy problem
- Publish new papers on Δ
- Why does industry not use Δ?
- Industry problems are trivial

Bridging

Industry

- Create new solutions
- Time to market essential
- Focus on cost-effective
- Use trusted technology
- Follow competition
- Academic Δ not useful

SOLUTION: BRIDGING THE GAP

Academia

Bridging

Industry

- Let academics and people in industry work together
- Support such exchanges from the government
- Gain mutual respect for each other
- Academics need to understand the industry challenges
- Industry need to understand what is possible
- I have played the bridging role for many years
- I will possible create start-up company for this kind of bridging

EVOLUTION INSTEAD OF REVOLUTION

- Unless you already have very strong theory/FM skills and the organization is extremely committed I recommend making small successes
- Possibly start in parallel with the traditional method
- Rather than trying to make a large revolutionary change
- Moving to the approach taken for B in railways and Rockwell Collins requires long-term commitment

CAN YOU USE FORMAL METHODS?

- Yes but start investing in education if you don't already know about it
- Use it at places where you currently have problems
- In particular if you are:
- Involved with critical systems
- Involved with complex data or functionality
- Don't think that it is a "wonder medicine" that should be used everywhere by everyone
- Get advice from an expert (when I have had students for a course I am still a factor between 10 and 100 better than them at modelling)

TAKE AWAY POINTS

- Formal methods have been used in many different industrial contexts
- Also outside critical applications
- IPA recommendations look very sensible
- Formal methods should be used when needed but not always
- A fool with a tool is still a fool!
- Thus training and tool support is essential!
- Come and talk if you wish to discuss your situation

THANKS FOR YOUR ATTENTION

Any questions?