IT infusion

Martin S. Feather

300 char max summary

Infusing IT technology is a perennial challenge. The Technology Infusion and Maturity Assessment approach of Cornford & Hicks is shown applied to an example of IT infusion: model-based V&V of spacecraft software. It highlights what the real problems are, and what can be done to best address them.

Full abstract:

Model-based validation holds great promise as a means for effective validation and verification (V&V) of critical spacecraft software systems. Groups within several NASA centers, JPL included, have performed pilot studies to investigate feasibility and utility of model-based validation. Their studies have demonstrated the promise of model-based validation to assure that critical requirements (flight rules, or software requirements derived from flight rules) are met by a software design/implementation. Generally, the results have been positive, and research into this approach is expected to continue, both within NASA and within the broader software engineering community. However, there has been little transfer of this approach into standard practice for flight code development and assurance.

Why is this?

More generally, successfully infusing IT technology into mainstream use is a perennial challenge. In fact, the IT world is not unique in facing this challenge. JPLers Hicks and Cornford recognized that "infusion rates for [spacecraft] technology have significant room for improvement", and pioneered the use of the Defect Detection and Prevention (DDP) methodology as a means to address this challenge. The have applied their DDP-based "Technology Infusion and Maturity Assessment" approach to a number of technologies, software included, but primarily hardware.

We report on this same approach, applied to examining the challenges of infusion of IT research, specifically infusion of model-based validation (MBV). A group was assembled to first identify possible uses for, and users of, MBV. This information became the DDP "requirements". Then, the group brainstormed the impediments to those uses and those users. This information became the DDP "Failure Modes" (things that adversely impact requirements). Finally, the group brainstormed the possible solutions to those impediments (things that reduce the likelihood and/or severity of the impediments).

The net result is the ability to focus on the major impediments, and guide selection of the solutions that as a whole most effectively address those impediments. The presentation will show this infusion data, captured in the DDP tool. You will see how to explore its implications. You will also see how to add to this data on-the-fly.

Is infusion a challenge for YOUR Information Technology? If so, you will likely find this approach to determining infusion challenges, and identifying solutions, to be of some ~~of~~ interest.

IT infusion

Martin S. Feather

300 char max summary

Infusing IT technology is a perennial challenge. The Technology Infusion and Maturity Assessment approach of Cornford & Hicks is shown applied to an example of IT infusion: model-based V&V of spacecraft software. It highlights what the real problems are, and what can be done to best address them.

Full abstract:

Model-based validation holds great promise as a means for effective validation and verification (V&V) of critical spacecraft software systems. Groups within several NASA centers, JPL included, have performed pilot studies to investigate feasibility and utility of model-based validation. Their studies have demonstrated the promise of model-based validation to assure that critical requirements (flight rules, or software requirements derived from flight rules) are met by a software design/implementation. Generally, the results have been positive, and research into this approach is expected to continue, both within NASA and within the broader software engineering community. However, there has been little transfer of this approach into standard practice for flight code development and assurance.

Why is this?

More generally, successfully infusing IT technology into mainstream use is a perennial challenge. In fact, the IT world is not unique in facing this challenge. JPLers Hicks and Cornford recognized that "infusion rates for [spacecraft] technology have significant room for improvement", and pioneered the use of the Defect Detection and Prevention (DDP) methodology as a means to address this challenge. The have applied their DDP-based "Technology Infusion and Maturity Assessment" approach to a number of technologies, software included, but primarily hardware.

We report on this same approach, applied to examining the challenges of infusion of IT research, specifically infusion of model-based validation (MBV). A group was assembled to first identify possible uses for, and users of, MBV. This information became the DDP "requirements". Then, the group brainstormed the impediments to those uses and those users. This information became the DDP "Failure Modes" (things that adversely impact requirements). Finally, the group brainstormed the possible solutions to those impediments (things that reduce the likelihood and/or severity of the impediments).

The net result is the ability to focus on the major impediments, and guide selection of the solutions that as a whole most effectively address those impediments. The presentation will show this infusion data, captured in the DDP tool. You will see how to explore its implications. You will also see how to add to this data on-the-fly.

Is infusion a challenge for YOUR Information Technology? If so, you will likely find this approach to determining infusion challenges, and identifying solutions, to be of some of interest.

CSMISS Center for Space Mission Information and Software Systems

JPL California Institute of Technology

IT Infusion

Martin S. Feather,
Jet Propulsion Laboratory
California Institute of Technology

This research was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.

Work funded by JPL's CSMISS SET, based on work funded by NASA's

- Code Q FDPP program
- Code Q/IV&V ARRT task, and
- Code R ECS program

If the need exists and the solution exists, why is IT infusion so hard?*

- New V&V practices exemplify **IT infusion needs and challenges**.
  - Needs: improved V&V (faster, better, cheaper)
  - V&V extended to new software products (e.g., autonomy software) and practices (e.g., code generation)

- Source of new V&V practices – the computer science research community
  - Breakthroughs in both theory (e.g., representations such as BDDs) and practice (e.g., tools such as SPIN)

* or, "I built a better e-mousetrap, but why is there no-one at my portal?"

Technology Infusion

Infusion rates* for **all** technologies (not just IT) are **dismal**.

Ken Hicks (JPL) & Steve Cornford (JPL) identify as reasons:

- miss-communicated requirements
- unforeseen engineering issues
- overtaken by commercial near-equivalents

"**Technology Infusion Maturity Assessment**" process :

- identify impediments to infusion
- identify means to overcome impediments
- emerge with assessment of whether, and if so how, to proceed.

* Infusion rate = number of technologies on mission after CDR / number of technologies at proof-of-concept

TIMA Process for study of infusion issues

"Technology Infusion Maturity Assessment" process:

- Applied to primarily hardware-centric problems
- Will it work for ***IT*** infusion?

Model Based Validation an example of an IT infusion problem:

- Try the TIMA process on it, to reveal:
  - insight into infusion of Model Based Validation (advanced technique for analysis of system requirements, designs and code)
  - insight into applicability of TIMA process to IT challenges

TIMA: Core Ideas

Objectives (a.k.a. "Requirements", "Goals")

Links indicate which Impediments impact which Objectives, and by how much

Impediments (a.k.a. "Risks", "Failure Modes")

Links indicate which Activities effectively overcome which Impediments, and by how much

Activities (a.k.a. "Investments", "PACTs"*)

* "PACTs" = Preventative measures, Analyses, process Controls and Tests

Model Based Validation TIMA

Information gathered from Model Based Validation people at both JPL and AMES

- Who would use MBV and for what purpose?
- What are the impediments to MBV?
- What are the potential solutions to overcoming those impediments?
- How do these connect?

What does this reveal

- about MBV?
- about TIMA on IT infusion?

Objectives

What's the purpose?

1:artifacts
- 1.1:rqmts
  - 1.1.1:consistency
  - 1.1.2:completeness
  - 1.1.3:validation
  - 1.1.4:test case generation
- 1.2:design
  - 1.2.1:requirements verification
  - 1.2.2:bug finding
- 1.3:code
  - 1.3.1:requirements verification
  - 1.3.2:unit testing
  - 1.3.3:integration testing
  - 1.3.4:structural, defect detection
  - 1.3.5:functional errors, bug finding
  - 1.3.6:timing errors
- 1.4:models
  - 1.4.1:sanity checking
  - 1.4.2:validation

Who's to do it?

2:who uses the tool
- 2.1:developers
- 2.2:test engineers
- 2.3:QA
- 2.4:IV&V
- 2.5:model checking gurus

Impediments

1:Technical issues
- 1.1:state space explosion
- 1.2:slow turnaround time
- 1.3:notation that mc can't handle
  - 1.3.1:design notation
  - 1.3.2:property notation
- 1.4:challenging generation of environment models
- 1.5:unknown what application domains are suitable
- 1.6:unknown how much work it takes
- 1.7:complexity of deciphering error traces

2: Social issues
- 2.1:resistance to learning new languages and tools
- 2.2:need to have specification expertise
  - 2.2.1:modeling expertise (how to build the model)
  - 2.2.2:LTL etc expertise (how to specify the properties)
- 2.3:well documented requirements are lacking
- 2.4:beneficiaries not the ones who do it
- 2.5:large effort of applying model checking
- 2.6:knowledge of the application domain is required

Activities

1:tools for abstraction
2:tools for translation into mc Ls
3:hiring PhDs
4:training application engineers
5:increase computing resources
    5.1:chips get faster
    5.2:more memory
    5.3: parallel h/w
6:short training course for LTL el al
7:emphasize the unique role that m/c can play
8:cost of failure a driver
9:specification patterns for properties
10:model checking provided as a "service"
11:Develop cost models
12:Case studies
13:Baselining & benchmarking
14:(Funded) partnerships with projects
15:Search heuristics
16:custom model checkers for programming Ls
17:compositional m/c
18:marketing
19:design for verification
20:tools for visualizing results
21:include mc into existing toolset
22:pick customers

Impediments

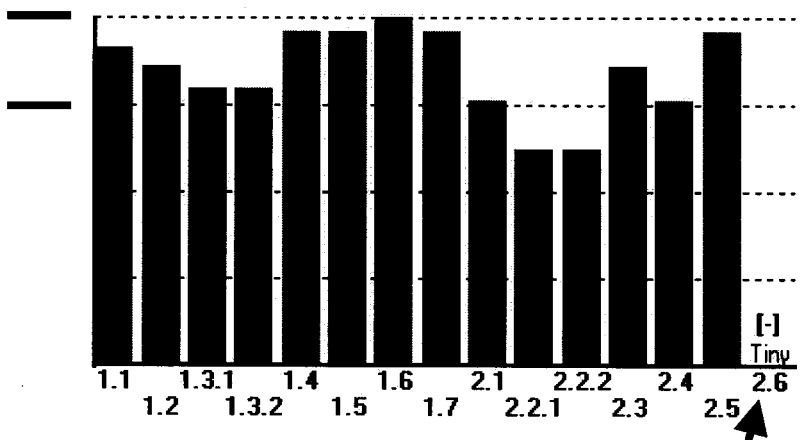
		REs	[-]Technical issues								[-]Social Issues				
		REs	state space explos	slow turnaro time	[-]notation that mc can't handle		challer genera of enviror models	unknov what applic domair are	unknov how much work it takes	comple of deciph error	resitan to learnin new langua	[-]need to have specification expertise		well docum require are	b n c
Activities		REs			design notatio incomp with model	proper notatio incomp with model						modeli experti (how to build	LTL etc experti (how to		
SOs	SOs	FoM\R	1	1	1	1	1	1	1	1	1	1	1	0.97	1
hiring PhDs		9.9	0.8	0.1	0.9	0.9	0.8	0.6	0.3	0.99	0.9	0.8	0.99	0.1	
training application engineers		11.2	0.3	0.7	0.9	0.99	0.9	0.9	0.3	0.8	0.1	0.99	0.99	0.5	0
[-]increase computing resources	chips get faster	1.14	0.1	0.7						0.1					
	more memory	1.2	0.6	0.3											
	parallel h/w	1.82	0.7	0.7											
short training course for LTL el al		2.03				0.99							0.99	0.2	0
emphasize the unique role that m/c		1.39						0.7			0.3				
cost of failure a driver		1.39						0.7			0.3				
specification patterns for properties		2.05		0.1		0.7					0.3		0.7	0.3	0

ESTIMATES OF EFFECTIVENESS

Impediments' magnitudes

Scenario using data gathered in MBV TIMA

Log scale, factor of 2

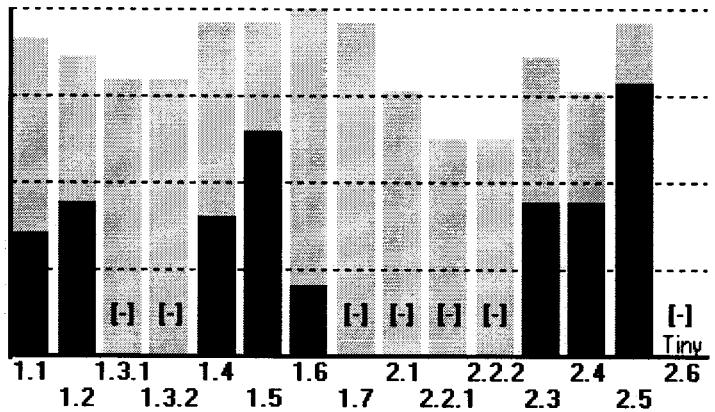


Objectives are: Requirements Validation, done by Developers

NO Activities

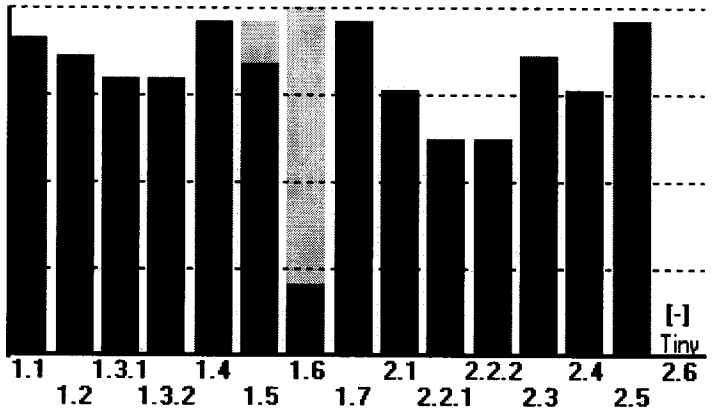
Impediment 2.6: Knowledge of the application domain is required" - tiny because scenario has MBV done by developers

Impediments' magnitudes



Funded partnerships with projects - very effective, but very expensive

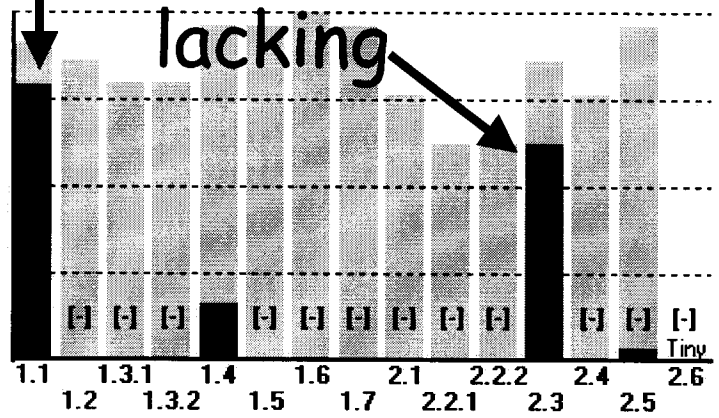
Impediments' magnitudes



Develop cost models

State space explosion

Well documented requirements are lacking



Develop cost models,
Training application engineers, *and*
Tools for translation into mc languages

Infusion of Model Based Validation

Model Based Validation:

Modest information gathered to date does encompass real issues

- JPL experiments in MBV field already encountered some of them:
- Paula Pingree at al target tractable translation problem
- Similar treatment of FP Engine itself less tractable (CSMISS SET studies by Feather & Fickas 2001, Nikora & Heitmeyer 2002)
- paucity of clear requirements to check of DI FP design
- state explosion problem may yet appear:
  - involvement of Holzmann an excellent mitigant to problem!
  - research work being done by JPLer John Powell might apply

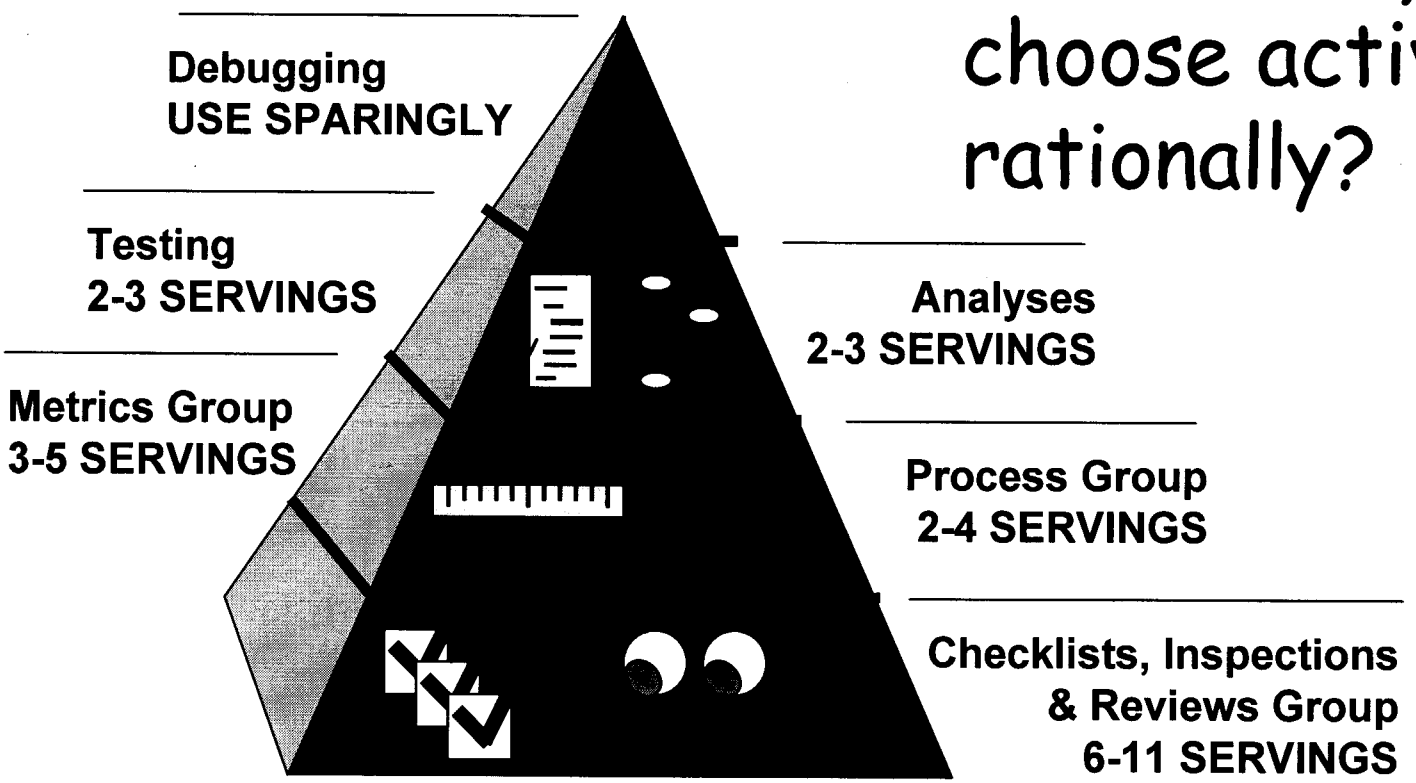
- Greater depth of information would lead to more insightful results
  - More specific intended application of MBV would give this depth

CONCLUSIONS

IT Infusion:

- TIMA approach appears viable, well-received in external contexts:
  - Basis for presentation at the Integrated Design and Process Technology conference (Pasadena, CA, June 2002; Society for Design and Process Science)
  - Used in position paper for workshop on Requirements for High Assurance Systems (Essen, Germany, Sept 2002; IEEE)
  - Major section of invited paper "Infusing and Selecting V&V Activities" for Foundations 2002 workshop on model and simulation (M&S) verification and validation (V&V) (Laurel, MD, Oct 2002; The Defense Modeling and Simulation Office (DMSO), Joint Army Navy NASA Air Force (JANNAF) Inter-Agency Propulsion Committee and National Training Systems Association (NTSA))
- Software V&V technology infusion important to ongoing Engineering of Complex Systems (ECS) program (Code R) - key JPL & AMES involvement
- NASA Software Working group also working the infusion issue

Do we *really* choose activities rationally?



Hypothetical V&V Pyramid

Not complete – just to convey the idea!

Tool used for study:

Defect Detection and Prevention (DDP):

http://ddptool.jpl.nasa.gov

The lead for this is

Steven.L.Cornford@Jpl.Nasa.Gov

Advice, guidance, feedback, ideas, applications: all welcome!

Martin.S.Feather@Jpl.Nasa.Gov