Formal Methods: Worse is Better!

Dan Craigen
Mark Saaltink

Daniel.Craigen@cse-cst.gc.ca
Mark.Saaltink@cse-cst.gc.ca
Abstract

**HCSS is usually focused on the best of mathematically sound methods and models.**

*In this talk, we **celebrate** unsound, incomplete, or incorrect models, methods, and tools.*

We will argue that these can be highly beneficial, are more widely usable, and may facilitate the adoption of formal methods.
Formal Methods Anecdotes

Anecdotes background

Motivated by ESC/Java2

- Why not use something better?
- Why are we getting good results?
- Why are the weak results good enough?
ESC/Java2

The bad:
- Weak
- Unsound
- Incorrect
- Incomplete
- Concurrency
- Difficult to extend

The good:
- Easy to learn and use
- Skilled users find lots of bugs
- Integrates with common practice
- Moderate assurance
- Adds useful documentation
Z Specifications

The good:
- Z can be used rigorously (Mondex)
- Semantics well defined
- Refinement proofs well-studied
- ISO Standard
- Formal enough for many useful proofs

The bad:
Many sloppy efforts (e.g., misused constructs, incorrect combination, too loose, no proofs)

Meant to explore and communicate, not for analysis; errors were irrelevant to that goal!
Others

- PathStar
  - Automated extraction of models from C
- UML
  - Modeling language – market success
- Alloy
  - Small scope hypothesis

*Successful because of, not despite, the limitations*
Technology Transfer Models

Discuss four technology transfer models

Understand why unsound, incomplete or incorrect models are effective in providing customer value

Everett Rogers

Geoffrey Moore

Richard Gabriel

Clayton Christensen
First model we used – EVES and Z/EVES

Relative advantage
Compatibility
Simplicity
Trialability
Observability
Transferability

65 Countries
Incremental adoption
Everett Rogers – FM

- Syntax and type checking
- Schema expansion
- Precondition calculation
- Domain checking
- Refinement proofs
- General theorem proving

<table>
<thead>
<tr>
<th></th>
<th>H.A.</th>
<th>Z</th>
<th>ESC/Java2</th>
<th>PathStar</th>
<th>UML</th>
<th>Alloy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compatibility</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>Simplicity</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Trialability</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Observability</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Transferability</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
</tr>
</tbody>
</table>
The Chasm

Technology Adoption Lifecycle

- Symbolizes the dissociation between two psychological groups

Geoffrey Moore

Innovator/Early adopter: difficulty of translating a technology into a compelling benefit

Early & Late majority: willing to become competent in new technology versus easily adopted product

Technology lovers
- Change artists
- Productivity improvers
- Standards lovers
- Technology haters
The Chasm

Productivity improvements (preferably through evolution)

Need to target a market niche defined around a “must have” value proposition – a niche that can be dominated

Value proposition: “Our new product radically improves productivity on an already well understood critical success factor specific to your business, and there is no existing means by which you can achieve a comparable result.”
The Innovator’s Solution

Customers “hire” products

Critical unit of categorization is the “circumstance,” not the customer

Comparison is of a disruptive product with nothing at all

Clayton Christensen

A disruptive product must be simple, convenient and fool proof – somewhat “Rogerian”

To guarantee focus and resources frame the innovation as a threat and use an autonomous organization to frame the opportunity
A disruptive technology is an innovation that results in “worse” product performance – at least at the beginning.
The Innovator’s Solution

Disruptive technologies will underperform established products in mainstream market … but they have other benefits recognized by new customers or a fringe portion of the existing market

Clayton Christensen

Such products are “typically cheaper, simpler, smaller and often easier to use.”

Product Performance

Progress due to sustaining technologies

Performance demanded at the high end of the market

Disruptive technological innovations

Progress due to sustaining technologies

Performance demanded at the low end of the market

Time
The Innovator’s Solution – FM

Product Performance

ACL2, PVS, Z/EVES
SPIN

Safety & Security
Critical

Restricted properties

Disruptive
technological
innovations

Model Checking
(SPIN to PathStar)
SLAM, ESC/Java

Time

Clayton Christensen
Worse is Better!

Better to start with a minimal creation and grow it as needed

Natural selection – Prevents change by choosing what survives, which is almost always what survived before since environmental change is slow

What is free to change is not crucial to survival

Richard Gabriel

In a free market:

Everything is stable until the environment changes

On an environmental change, already existing technology is quickly adapted

After the change, companies improve and innovate slowly so as to maximize ROI

Disruptive adoption arises from environmental change
Worse is Better!

Moore: Focuses on the chasm representing a niche that can be overwhelmed and owned by a technology

Gabriel: Chasm is crossed as a result of a change in environment that renders a technology necessary – changing a “nice to have” to a “must have”

There is a collection of technologies waiting to cross the chasm; some will, many will not

These technologies have been planted by innovative and inventive folk – many technologies will not transition – but the diversity and failure is crucial to an adaptive market
## Worse is Better!

<table>
<thead>
<tr>
<th></th>
<th>The Right Thing</th>
<th>Worse is Better</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Simplicity</strong></td>
<td>Simplicity!</td>
<td>“The Right Thing” — this is the most important consideration</td>
</tr>
<tr>
<td><strong>Correctness</strong></td>
<td>Not negotiable</td>
<td>Slightly better to be simple than correct</td>
</tr>
<tr>
<td><strong>Consistency</strong></td>
<td>Not negotiable, even if not as simple</td>
<td>Cannot be too inconsistent — simplicity wins</td>
</tr>
<tr>
<td><strong>Completeness</strong></td>
<td>Cover as many important situations as practical; simplicity loses</td>
<td>Can be sacrificed in favor of any other quality — simplicity wins</td>
</tr>
</tbody>
</table>

*Richard Gabriel*
Worse is Better! - Adoption

An undervalued technology resides in the innovator, early adopter groupings. The technology is mature from an engineering perspective, but not market relevant. The environment changes so that compelling value propositions can be developed from the undervalued technology.

Act quickly – create a minimal product using worse-is-better approach with the expectation of setting the de facto standard in a new market area. If it has value it will spread. If it becomes popular, there will be pressure to improve in a manner consistent with customer requirements.

We find that Gabriel’s perspective is largely consistent with the Rogers, Christensen and Moore models.
Worse is Better! – FM Examples

Microsoft Trustworthy Computing Initiative

Richard Gabriel

Intel Pentium FDIV

Environmental Change

- Change of threat space – networking, code complexity, legacy code
- Well-regarded research labs
- SLAM – reduce # of errors and potential vulnerabilities

Others:
Z and ESC/Java2

- Often simplicity & readability; at the cost correctness and consistency (Z)
- Unsound proof methods, but works mostly (ESC/Java2)

- Substantial financial penalty
- Simulation/testing limits
- MC adoption
- Mature, but no market penetration
- Analysis of larger state spaces
Observations

- High assurance formal methods stuck in Innovator and Early Adopter groups
- Safety- & security-critical MC/EC with compelling value from changed circumstances
- Being stuck isn’t all bad
- Technology evolves Diversity awaiting adoption High aspirations – grand challenges
- Then the environment changes
- Massive cyber attack Environmental change? Security versus functionality
Observations

Predictability school sets a tone; an aspiration

Aspiration and Inspiration
Theology – core believers through to laity
Society benefits even though predictability school is not ascendant

Reformation

The church, the saloon and the Reformation

Environment

Reality