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

Clayton Christensen

Richard Gabriel

Everett Rogers

First model we used – EVES and Z/EVES

Everett Rogers

Relative advantage

Compatibility

Simplicity

Trialability

Observability

Transferability

65 Countries

Incremental adoption

Everett Rogers – FM

Everett Rogers

Z/EVES Adoption Path

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

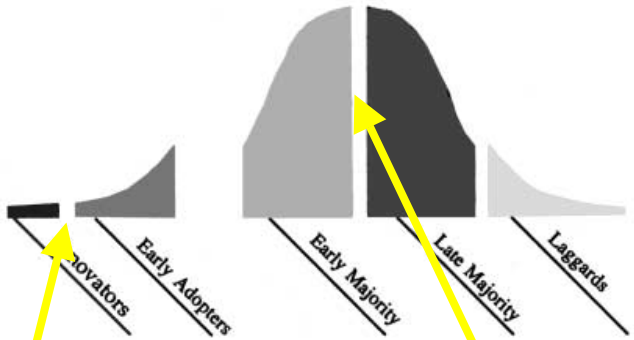
	H.A.	Z	ESC/Java2	PathStar	UML	Alloy
Compatibility	Low	High	High	High	High	Medium
Simplicity	Low	Medium	Medium	High	High	High
Trialability	Low	High	High	High	High	High
Observability	High	High	High	High	Medium	High
Transferability	Low	Medium	Medium	High	High	Medium

The Chasm

Technology Adoption Lifecycle

Geoffrey Moore

Symbolizes the dissociation between two psychological groups



Technology lovers

Change artists

Productivity improvers

Standards lovers

Technology haters

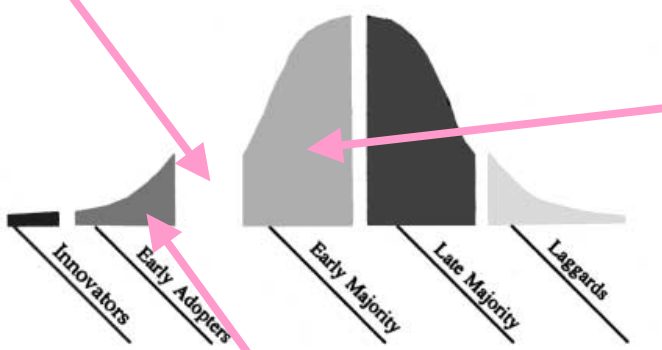
Innovator/Early adopter: difficulty of translating a technology into a compelling benefit

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

The Chasm

Chasm

Geoffrey Moore



Productivity improvements (preferably through evolution)

Change agent (competitive edge)

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

Clayton Christensen

Comparison is of a disruptive product with nothing at all

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

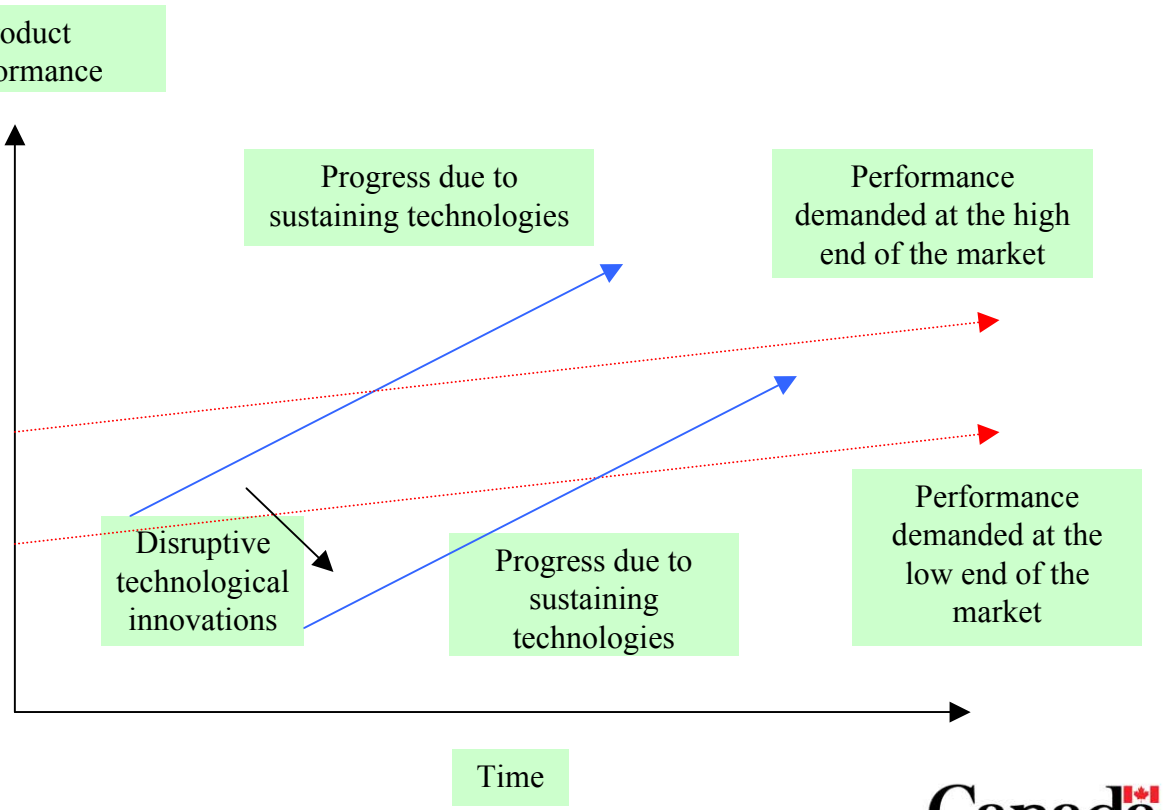
The Innovator's Solution

A disruptive technology is an innovation that results in "worse" product performance – at least at the beginning

Clayton Christensen

Sustaining technologies

Disruptive technologies



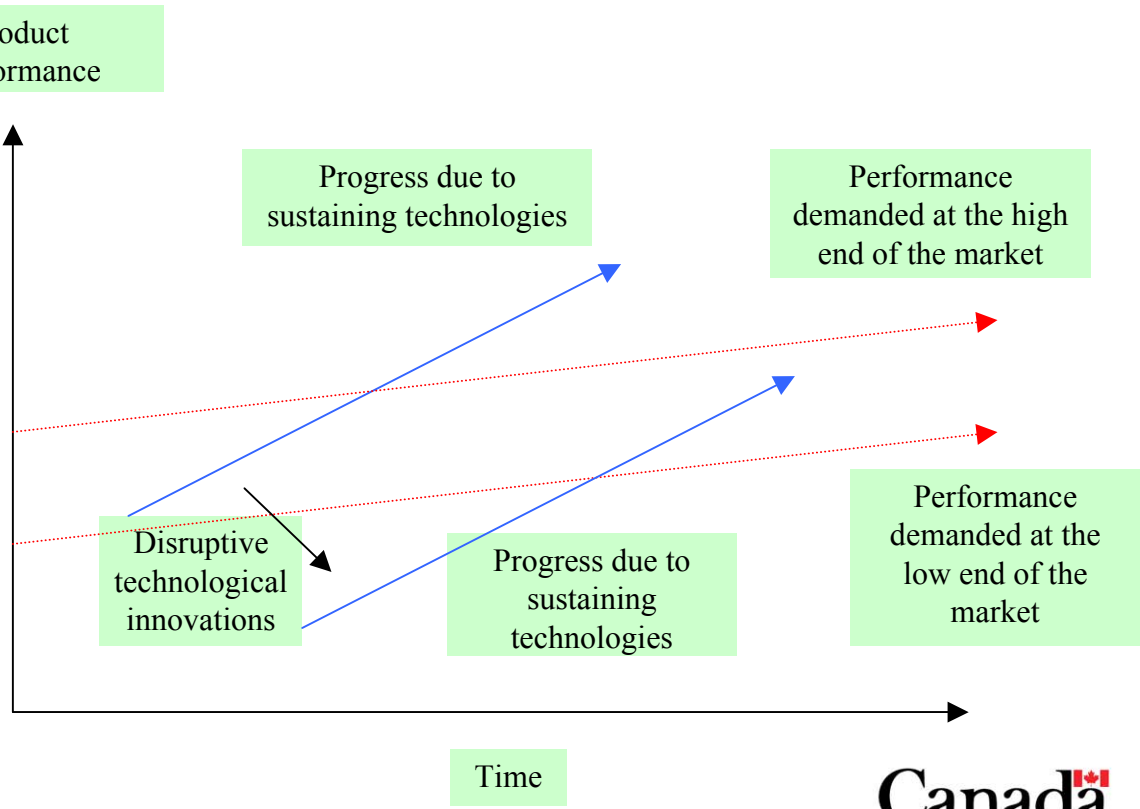
The Innovator's Solution

Disruptive technologies will under perform established products in mainstream market

… but they have other benefits recognized by new customers or a fringe portion of the existing market

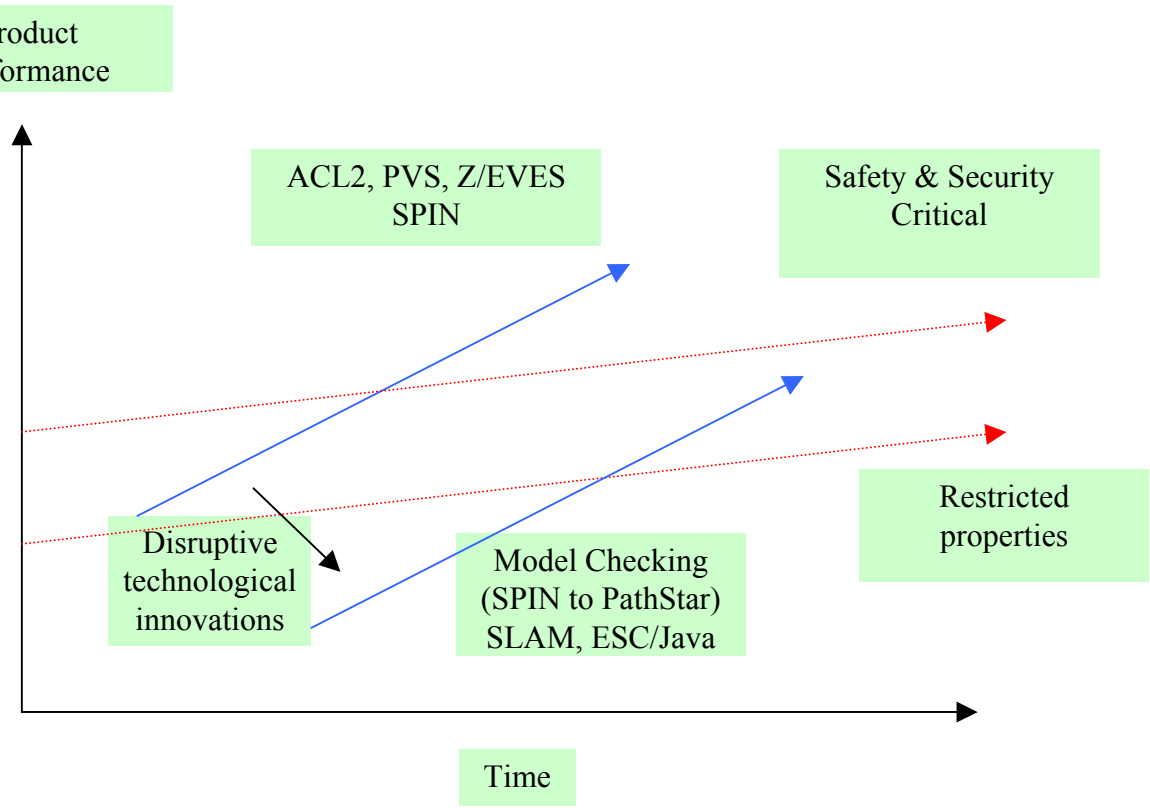
Clayton Christensen

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



The Innovator's Solution – FM

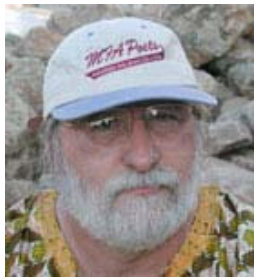
Clayton Christensen



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:

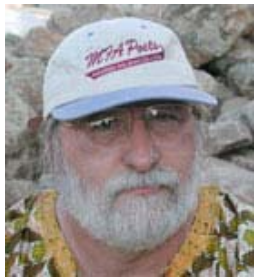
Everything is stable until the environment changes

On an environmental change, already existing technology is quickly adapted

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

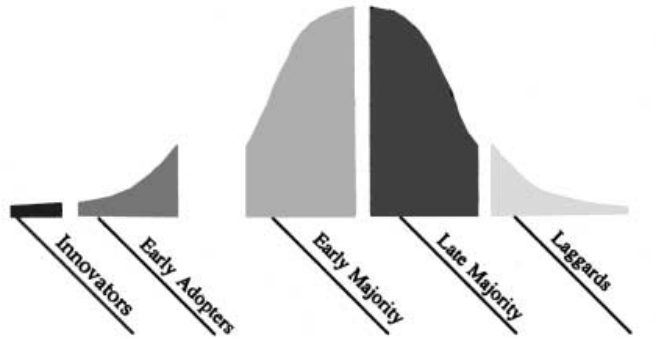
Disruptive adoption arises from environmental change

Worse is Better!



Richard Gabriel

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

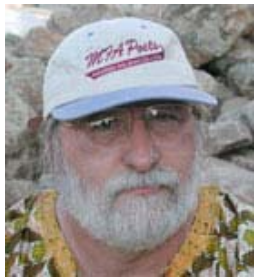


Gabriel: Chasm is crossed as a result of a change in environment that renders a technology necessary – changing a "nice to have" to a "must have"

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

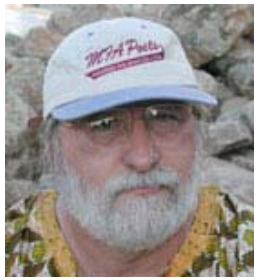
Worse is Better!



Richard Gabriel

	The Right Thing	Worse is Better
Simplicity	Simplicity!	"The Right Thing" – this is the most important consideration
Correctness	Not negotiable	Slightly better to be simple than correct
Consistency	Not negotiable, even if not as simple	Cannot be too inconsistent – simplicity wins
Completeness	Cover as many important situations as practical; simplicity loses	Can be sacrificed in favor of any other quality – simplicity wins

Worse is Better! - Adoption



Richard Gabriel

An undervalued technology resides in the innovator, early adopter groupings. The technology is mature from an engineering perspective, but not market relevant.

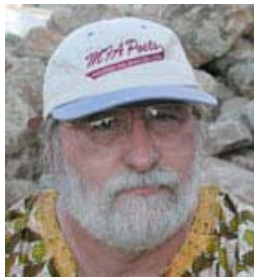
The environment changes so that compelling value propositions can be developed from the undervalued technology.

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



Richard Gabriel

Microsoft Trustworthy Computing Initiative

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

Intel Pentium FDIV Environmental Change

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

Others: Z and ESC/Java2

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

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

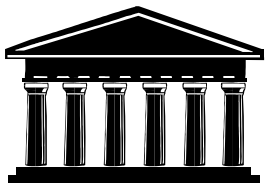
Aspiration and Inspiration

Theology – core believers through to laity

Society benefits even though predictability school is not ascendant

Reality

Environment



Reformation

The church, the saloon and the Reformation