Formal Methods and the Defense Industrial Base

Ray Richards
Program Manager
DARPA/I2O

Formal methods technology investments

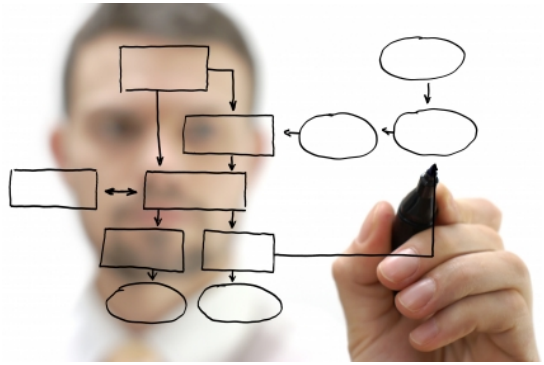
- The Government has long invested in formal methods research and technology development
  - DoD's goal is to provide value to the military
- Tools for development of military articles can provide value on several dimensions
  - Reduced development costs
  - Better verification evidence
  - Shorten time to deployment
  - Provide new capabilities
    - Verify properties that are untestable
    - HACMS demonstrated Formal Methods' ability to improve a systems cyber posture

HACMS
High Assurance Cyber Military Systems

- I built a better mousetrap, where is everyone?
  - Institutional resistance to untrusted technology insertion

Defense contracting

- Federal Acquisition Regulations and the U.S. Code govern how the DoD acquires defense articles
  - Fair and open competition among contractors



http://www.respect-it.com

- A simplified view
  - KPPs and other requirements are published in an RFP
  - Proposals describe how requirements are to be met
  - Lowest cost compliant bidder is awarded contract
  - Systems undergo stringent evaluation and certification to show requirements have been met

- Contractors compete on costs
  - How you control development costs provide a comparative advantage
    - Engineering processes guarded as intellectual property
    - Engineering processes are predictable and repeatable
      - Human resources are commoditized

Technology insertion

- New technologies are inserted into programs once it is demonstrated to be sufficiently mature
  - 'Risk burned down'
  - High TRL
  - Component-level C&A
- Resistance to adopt development approaches that require a restructuring of engineering processes
  - Introduces 'unacceptable risk' to programs
- Formal methods tools insert into development process, not integrated into systems.
  - How are risks of this insertion to be managed?

Defense contractor program management's view

- Manage program for schedule and cost performance
  - Earned Value Milestone is a preferred style of program management for the defense industry
    - CPI, SPI
  - Requires cost and schedule predictability and execution

http://www.managed-programs.com

- Risks and Opportunities
  - Events that have a probability of occurrence that if realized will increase (risk) or decrease (opportunity) program costs
  - PMs leverage MR to lower risk likelihood and increase opportunity likelihood
    - And to cover 'unknown risks'

- Front loaded analysis and verification activity stresses cost and schedule metrics
  - Looks over budget and behind schedule when compared to traditional process
  - MR will be needed at integration

Executive's view

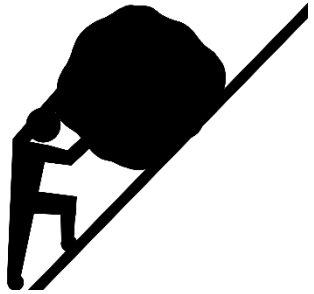
- Cost-benefit analysis
  - What are the benefits, measured in dollars
  - Capture new business
    - Substantiate with market analysis
  - Reduce costs (cost avoidance is a tough sell)
    - "If I never find a bug, then its free"
    - What is ROI?

$$FMnre + \sum i \uparrow FMrci << \sum i \uparrow TRADrci$$

orgchanger.files.wordpress.com

  - Understand all of the costs
    - How do Formal Methods tools integrate into complex engineering workflows?
    - What is the schedule impact? – with respect to earned value milestones
    - What is the cost impact? – with respect to earned value milestones
    - Training
    - Other costs

The uphill battle



- The bad reputation of formal methods
  - Expensive
  - Schedule buster
  - Lacks scalability
  - Does not live up to promises
- Drive down risk by increasing the TRL of the formal methods-enhanced engineering workflow.
  - The FM has to provide value
    - ROI
  - Understand how to reliably predict cost and schedule expenditures though the development process
  - Repeatable
- Direct evidence of costs and benefits of formal methods approach is needed but is difficult to get
  - Compelling apples-to-apples numbers
- Standardization

Creating a pull for formal methods

- Customer pull can motivate industry to embrace new development approaches
  - Convincing evidence of technical value can spur action
  - Defense contractors and tool providers will respond to market conditions
    - Invest to sustain, support, and commercialize FM technologies
    - Effective engineering workflow integration
  - DoD has a carrot and a stick
    - Requirements
      - Will not specify development methods
      - Evidence that objectives are met
    - C&A
      - Provide certification 'credit' for the use of Formal Methods
      - C&A evaluators will need to be able to judge FM evidence on its merits

http://birneysdivision.weebly.com

A recap

- Aerospace and Defense industry sector is conservative and risk adverse
- Many exquisitely engineered complex critical systems
- No compelling business case to drive formal methods adoption
- Demonstrated success can drive market conditions

www.darpa.mil