

Cleanroom / Formal Methods / Walkthroughs

Dror Feitelson
Basic Seminar of Software Engineering
Hebrew University 2009

Harlan D. Mills



- A bomber pilot in WWII
- A “super programmer”
- An IBM fellow
- Contributions to automata theory, adoption of structured programming, use of formal methods
- On faculty of several universities
- IEEE Harlan Mills award recognizes “contributions to the practice of software engineering through the application of sound theory”

Cleanroom

- Iterative approach, 5000-15000 lines each
- In each iteration specifications are fixed
- Design and code are developed and formally verified in tandem
- Verification replaces debugging
- Testing used to provide statistical quality control, based on distribution of usage scenarios
- Testing results used for feedback to improve process and achieve reliability goals

Cleanroom

- Claims

- Verification can effectively replace debugging, and does not require more time
- Vast majority of defects are found before first execution
- In total there are less bugs (half the amount with normal development), leading to a higher MTTF
- Better productivity and simpler programs
- Problems left behind by formal verification are easier to fix than problems left behind by debugging

Independent Verification

- Experiment based on groups of students doing the same project
- Cleanroom indeed led to better results
 - Not clear whether used formal verification
- At least part of this was change of attitude
 - Programmers were more careful with their code out of anticipation of review
- Large majority missed the fun of running the program
- Large majority would use cleanroom again

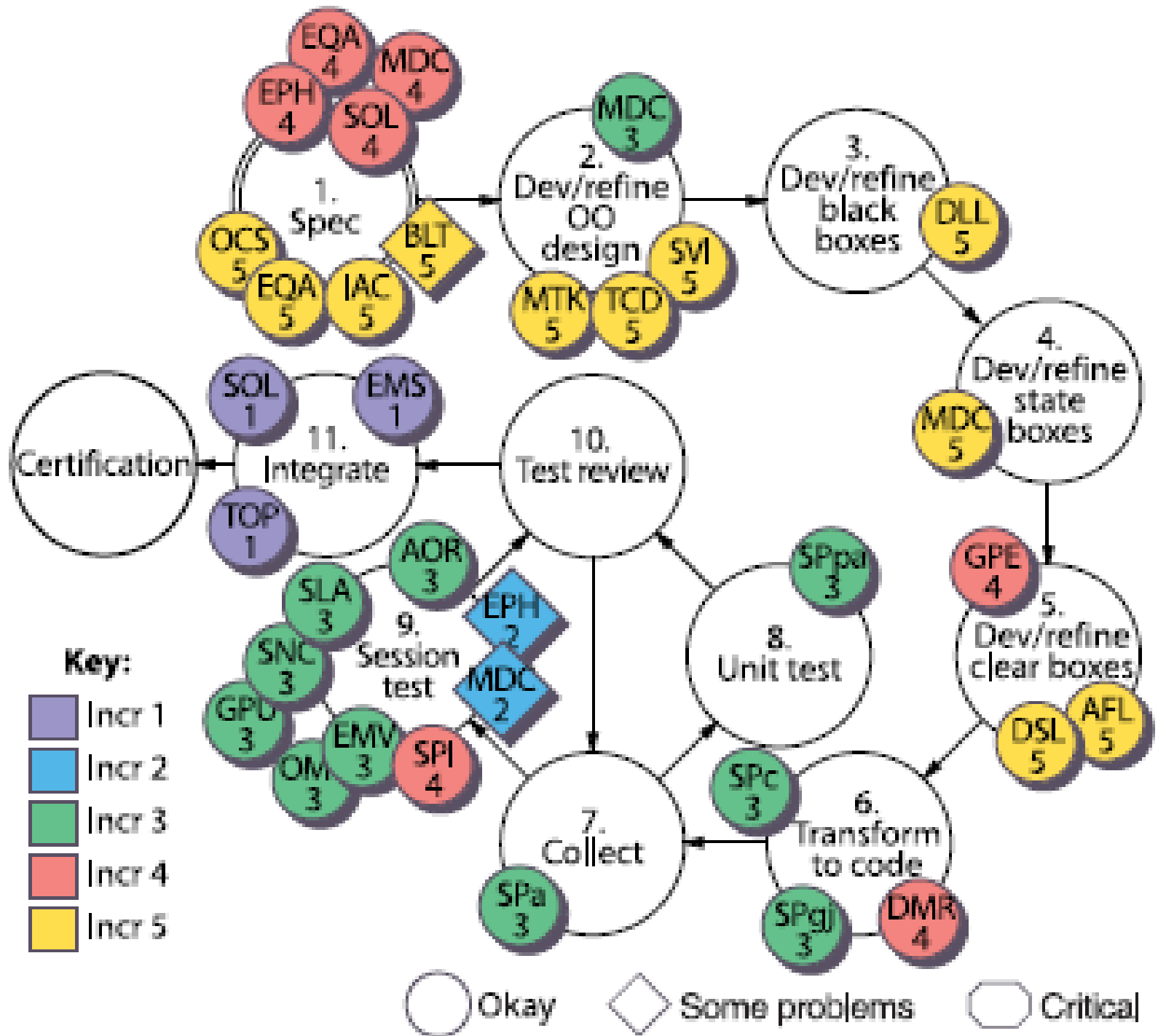
State-Based

- Based on cleanroom approach
- Iterative approach
- Each release includes several pipelined increments, each with several “development items”
- Development items go through a sequence of 12 states (spec, define, code, test, certify)
- Progress monitored by walkthroughs and inspections

State-Based

Success factors:

- User involvement in walkthroughs and design
 - Provide for correct requirements
 - Users already know the product when it is delivered
- Management involvement
 - Simple states and well-defined transitions
 - Management can monitor complete project with one comprehensive view
- Process improvement
 - Ideas for improvements become action items in walkthrough



Formal Methods

- Somewhat controversial approach
 - Some people think this is the only way to go
 - Others think it is essentially useless
- An important component in the cleanroom approach
- Replaced by walkthroughs in the state-based approach
- State-based approach has many similarities with current agile methods