Lean-Agile Partners

Safety-Critical Applications Built via Agile Discipline

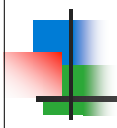
Nancy Van Schooenderwoert
http://www.leanagilepartners.com/
nancyv@leanagilepartners.com

September 16, 2008

Nancy V's Background

- 15 years safety-critical systems experience
- 10 years agile team coaching
- 3 years agile enterprise coaching
- Industries: Aerospace, Medical Devices, Sonar Weaponry, Scientific Instruments, Financial Services
- Electrical Engineering and Software Engineering, embedded systems

Lean-Agile Partners

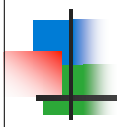


Introduction

- We'll cover these
  - Intersection of Safety-critical practices and Agile team practices
  - How "agile" and "discipline" go together
  - What real agile teams are doing now
- Not these
  - Complete safety-critical procedures
  - Various agile methodologies and frameworks

Questions welcome at any point!

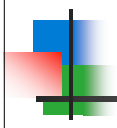
Lean-Agile Partners



Agenda

1. Basics of Safety Design and Agile
2. Case Studies
3. Wrap Up

Lean-Agile Partners

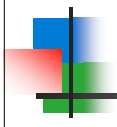


Terminology

- Scrum
- XP (Extreme Programming)
- Iterations
- Stories
- Product Owner

Lean-Agile Partners

5



Basics of Safety-critical Design (1)

- Terms [Ref. Levison]
  - Accident - An undesired and unplanned (but not necessarily unexpected) event that results in (at least) a specified level of loss
  - Incident - An event that involves no loss (or only minor loss) but with the potential for loss under different circumstances
  - Hazard - A state of a system (or an object) that, together with other conditions in its environment, will lead inevitably to an accident (loss event)

Lean-Agile Partners

6

Basics of Safety-critical Design (2)

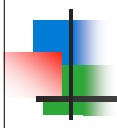
- List all possible hazards
- For each hazard, design a control
- Two traditional approaches
  - Freeze up-front (and trace all code to original requirements)
  - ~~Ad Hoc~~

Lean-Agile Partners

Problems of "Freeze Up-front"

- Risk: your requirements may be in conflict
- Risk: requirements may be incomplete
- Risk: hard to think of every possible hazard up front
- Risk: After risks & controls frozen, future changes defeat a control

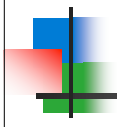
Lean-Agile Partners



Basics of Agile Discipline (1)

- Agile does not treat safety-critical s/w differently; all is max quality
- Agile's great strength is time-to-market, and ability to hit moving targets
- How? By s/w practices that keep us grounded to tech reality; management practices that keep us continually in touch with customer's needs

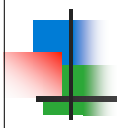
Lean-Agile Partners



Basics of Agile Discipline (2)

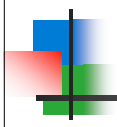
- Characteristics of a healthy Agile system:
  - Tested working code at end of each iteration
  - Team routinely delivers *all* stories promised
  - Customer is routinely satisfied that stories meet their needs
- Result: Can make a commitment *and keep it*
- Note - agile teams typically achieve < 0.5 defects per function point [Ref "Newbies" paper]

Lean-Agile Partners



Agile offers a 3rd pathway

- Neither Ad Hoc nor Freeze Up-front
- Not a compromise - *better* than 'Freeze'
- Cut Requirements risks via:
  - Iterative customer involvement
  - Revisit Hazards & Controls each iter.
- Idea: Software that cannot be tested inexpensively and thoroughly is itself a hazard!



Part 2

1. Basics of Safety Design and Agile
2. Case Studies
3. Wrap Up

Case Study: Medtronic (1)

- Product: Programmer for implanted pacemaker/defibrillator

Programmer Pacemaker

Lean-Agile Partners

Case Study: Medtronic (2)

- Began using Agile (Scrum, some XP) in 2002
- Team of approx. 50 developers and testers
- 2-week iterations
- 15-36 months typical project length
- 4 agile projects run within past 5 years
- C++ several hundred thousand lines

Lean-Agile Partners

Case Study: Medtronic (3)

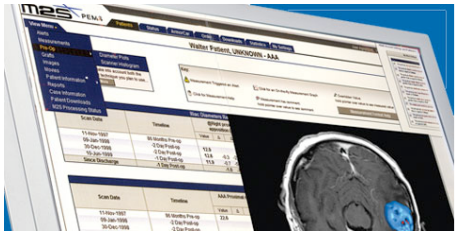
- Bug rate - A few hundred in past 5 years
- All were minor except one that required field action
- Before Agile, same level of exterior quality, but took more effort to achieve
- Now far fewer bugs are found in QA
- FDA Regulators:
  - "Do your practices generate acceptable results?"
  - "Are they implemented within the context of a robust quality system?"

Case Study: Medtronic (4)

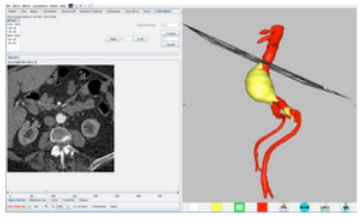
- Biggest changes from move to agile
  - Changing organization to short iterations (2 weeks)
- Most difficult changes
  - Getting comfortable with the agile culture --
  - "Agile teams are highly disciplined but it's a different kind of discipline. Instead of command & control agile relies on the discipline of teams to commit to their product and process."
- "Agile for us is less of a switch from bad to good, and instead it lets you turn up the knobs on the good. We need a system that allows engineers to think."

Case Study: M2S Inc. (1)

- Two Products using agile methods:
  - PEMS - (Patient Evaluation and Management System) is now the largest radiologically-based registry in the world, by a factor of 10.
  - Preview - treatment planning software



PEMS



Preview

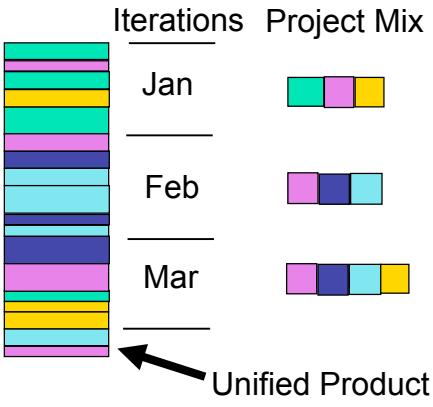
Lean-Agile Partners

Case Study: M2S Inc. (2)

- Began using Agile (Scrum) at the end of 2007
- 6 developers and a couple QA people, but 8 projects of 1 to 4 people each, all co-located
- We are now all working off of one unified, prioritized backlog feeding all our projects.
- 4 week iterations, but want to shorten
- Mix of Perl, Java, Tcl, C, SQL

Lean-Agile Partners

Case Study: M2S Inc. (3)



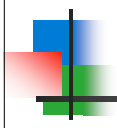
- Changing project mix
- Team composition shifts for each iteration
- Friday standup meeting includes all

Lean-Agile Partners

Case Study: M2S Inc. (4)

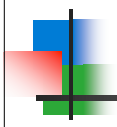
- Biggest impact of agile
  - Clarity on our priorities!
  - New prioritization process is fair and open, overseen by SVPs and CEO
  - Relationships are a company asset
- Most Difficult changes
  - Stakeholders all wanted to “own” a developer, but all now prefer new way
- Managers received Agile mgmt training

Lean-Agile Partners



Case Study: Major Euro… (1)

- Products:
  - Medical imaging archive software
  - Radiology office workflow management software
  - Platform to use imaging to create measurements and 3D renderings
- Using Scrum for 1.5 years, some XP practices
- 4 week iteration length
- Using retrospectives, daily stand-up meeting, ‘test first’ or in parallel (for unit testing)
- Team size: 500 - 600, 3 continents; 8M lines C++
- One code base worldwide, staged multi-level builds



Case Study: Major Euro… (2)

- Biggest impact of move to agile
  - Moving to 4-week iterations
  - Better understanding of our requirements
  - Quality impact data not available yet, but confident of improvements

Case Study: Major Euro… (3)

- Most Difficult changes
  - Changing the organization, leap of faith
  - Accepting our early failures and re-trying
  - Getting process tailored to us and documented for regulators (FDA, ISO)

Case Study: Major Euro… (4)

- Safety-critical software improved by:
  - Fast feedback - know if we broke anything
  - Can adapt without safety compromises
  - Easier for customer to commit to small feature sets
  - Modular traceability “trees” originating with each hazard are more manageable

Part 3

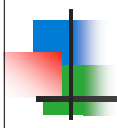
1. Basics of Safety Design and Agile
2. Case Studies
3. Wrap Up

Lean-Agile Partners

Implications

- More than one way to cover “Product Owner” role
  - Top product owner plus feature-set owners
- How Project Manager role is changing
  - “Disintermediation” of customer-team communications

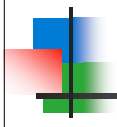
Lean-Agile Partners



Observations

- Lack of metrics just shows:
  - "For those who believe, no proof is necessary; For those who do not believe, no proof is possible." –anonymous
- If Agile is so good why isn't everyone using it?

Lean-Agile Partners



Recommendations

- Avoid having to compete against a truly agile company!
- ……..Hint: Get there first
- Smaller companies shift to agile more easily – less inertia
- Larger companies usually need help - org change in combo with lean-agile is a very difficult thing to do on "moonlighting" basis
- Prediction: Brain drain toward agile companies

Lean-Agile Partners

Resources

- Books
  - 'Safeware' by Nancy G. Leveson
  - 'Software Configuration Management Patterns' by Steve Berczuk
  - 'Implementing Lean Software Development' by Mary and Tom Poppendieck
  - 'User Stories Applied' by Mike Cohn
- Papers by Nancy V. available no-charge, at http://www.leanagilepartners.com/publications.html
  - The Four Pillars of Agile Adoption
  - Embedded Agile Project by the Numbers with Newbies
- Contact: nancyv@leanagilepartners.com

Lean-Agile Partners

29

Upcoming Presentations

Planning Your Agile Initiative

Software Development Best Practices Conference, Boston, Oct 29, 2008

http://www.sdbestpractices.com/

Embedded Agile Development Techniques

Half day tutorial, Great Lakes Software Excellence Conference, Grand Rapids MI, Nov 4-5, 2008

http://www.glsec.org/

Lean-Agile Partners

30