Agile: Quality, Safety, and Compliance

Brian Shoemaker, Ph.D.

ShoeBar
Associates

Brian Shoemaker, Ph.D.

- Originally an analytical chemist
- 15 y in clinical diagnostics (immunoassay):
  analytical support → assay development → instrument software validation
- 6 y as SW quality manager (5 in clinical trial related SW)
- 13 y as independent validation consultant to FDA-regulated companies – mostly medical device
- Active in: software validation, Part 11 evaluation, software quality systems, auditing, training

ShoeBar
Associates

Acknowledgement

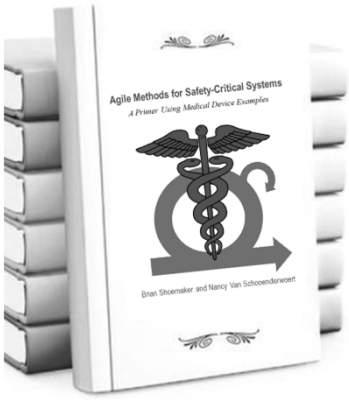
Part of this material was developed by Nancy Van Schooenderwoert, Lean-Agile Partners Inc., and is based on her work in coaching teams in lean methods for high-quality software development.

Nancy Van Schooenderwoert
Lean-Agile Partners, Inc.
162 Marrett Rd., Lexington, MA 02421
781-860-0212
NancyV@leanagilepartners.com
http://www.leanagilepartners.com

Lean-Agile Partners

ShoeBar Associates

For More Information



Agile Methods for Safety-Critical Systems:
A Primer Using Medical Device Examples
By
Nancy Van Schooenderwoert
And Brian Shoemaker

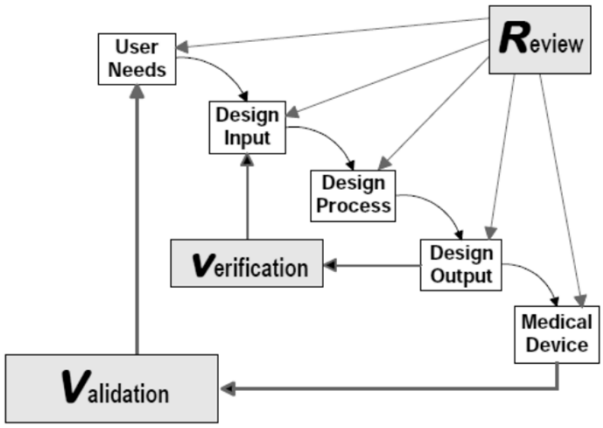
Topics go beyond what I'll discuss here.

ShoeBar Associates

Quality – Safety - Compliance

- **Face reality - Agile is here**
- *Docs – capture info when generated*
- *Iterative Risk Management: learning*
- *Agile events reinforce quality*
- *Agile: not an easy transition*

Where I Come From



Why Something Different?

- Traditional doc-heavy SW development is expensive, slow, and error prone
- Regulatory bodies rightly concerned with product software vs. safety
- Classic belief: tightly controlled process engineering
- Agile is highly productive, but seems the antithesis of tightly controlled process

Village Rumors are False!

*The standards say we **must** use a waterfall model*

Agile isn't suitable for safety-critical work!

TRUE Agile means you don't plan and don't write documents.

Agile is just an excuse for sloppiness!

SDMD Attendees Using Agile

- Dräger Medical
- Elekta
- Given Imaging
- Medidata Solutions
- Philips Healthcare
- Renishaw
- Siemens
- Systelab Software

INCOSE Agile in HC Conference

- Attendees included reps from:
  - Battelle Memorial Institute
  - Boston Scientific
  - Cook Medical
  - GE Healthcare
  - Medtronic
  - Roche
- All were there to share successes!

We've Worked With Others

- Clinical trial data mgmt software (2 companies)
- ICU aggregated-data risk prediction SW
- Histology / pathology networked slide imaging & assessment system
- Clinical diagnostics
- IVUS
- Optical measurement systems

ShoeBar Associates

Agile Manifesto – Read Closely!

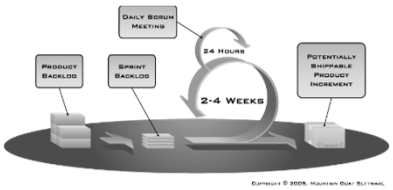
ShoeBar Associates

12 Principles Support the Manifesto

- Satisfy customer: deliver software which has value.
- Welcome changing requirements.
- Deliver working software frequently.
- Business and development must work together throughout.
- Allow motivated individuals to get the job done.
- Communicate face-to-face!
- Working software is the primary measure of progress.
- Develop at a sustainable pace.
- Being Agile also means technical excellence and good design.
- Keep it simple - maximize what you ***DON'T*** do.
- Self-organizing teams produce the best work.
- Teams must regularly reflect and adjust how they work.

Paraphrased from http://agilemanifesto.org/principles.html

Contradiction?



These aren't inherently incompatible – but documentation and risk management are crucial differences

Scroll Image: http://www.nifter.com/free_clipart_downloads.htm

Know the Objections and Benefits

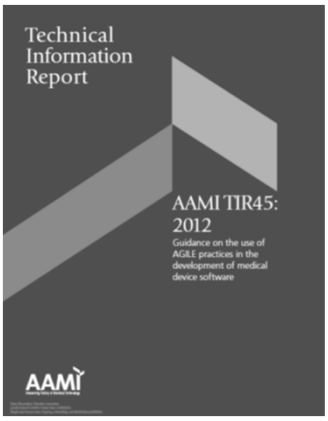
Points to counter:

- Lack of defined requirements
- Lack of structured review/release cycles
- Lack of documentation

Advantages to offer:

- Ability to resolve incomplete / conflicting requirements
- Ability to reprioritize requirements (mitigations) as system takes shape
- Many chances to identify hazards (controls not frozen too soon)

AAMI TIR 45 Provides Support



- Published in 2012
- Authors include industry experts, Agile experts, and FDA personnel
- Gives guidance on using Agile methods for medical device SW development
- Covers key concepts and practices

Quality – Safety - Compliance

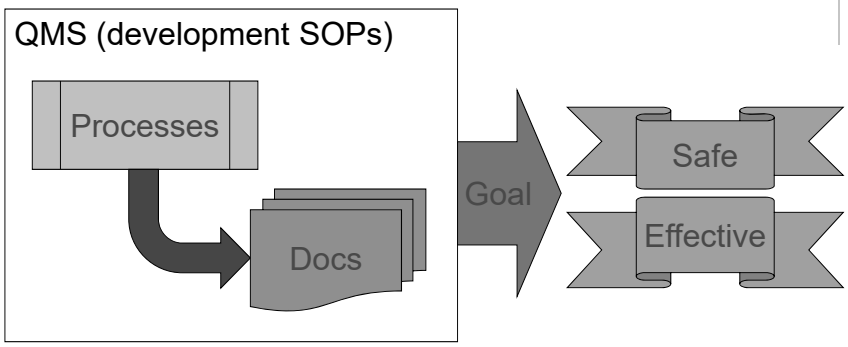
- *Face reality - Agile is here*
- **Docs – capture info when generated**
- *Iterative Risk Management: learning*
- *Agile events reinforce quality*
- *Agile: not an easy transition*

From a QA Manager

"I will not allow a project to be carried out if requirements aren't approved before the end."

This manager was concerned that an Agile approach would lead to projects without predetermined specifications (language used in GPSV) or other documentation.

Documents = Evidence



GOAL is crucial; docs provide evidence. *Process* is up to you.

Documentation – Not for the team

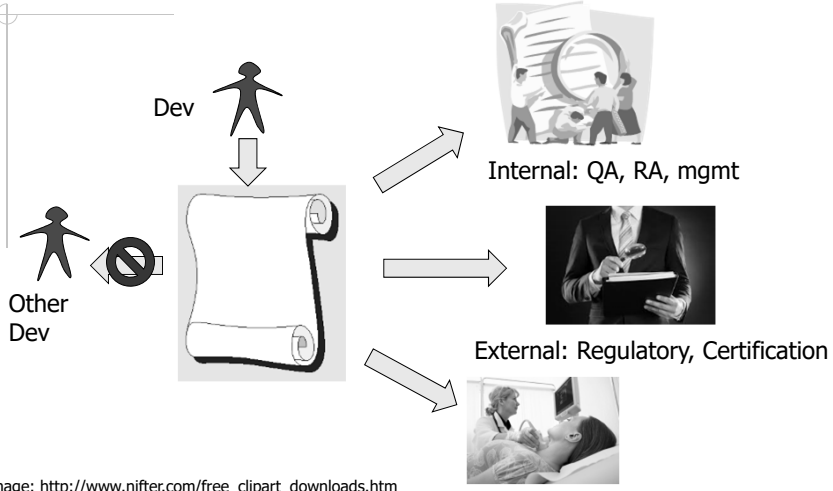


Image: http://www.nifter.com/free_clipart_downloads.htm

How to address the concern?

Be careful. SOPs need to specify WHAT you generate, not full details of HOW you get there.

Say what you do and do what you say!

Propose: Let *User Stories* serve as the software requirements

User Stories

- Emphasize the user's goals, not the system's attributes
- Can be verified by SQA
- Can be demoed to stake holders
- Bridge the communication gap PM - Dev - SQA
- Support and encourage iterative development
- Provide means for flexible and efficient planning

Ben Nahum & Livni, SDMD Europe Jan 2013

User Stories: Two Goals

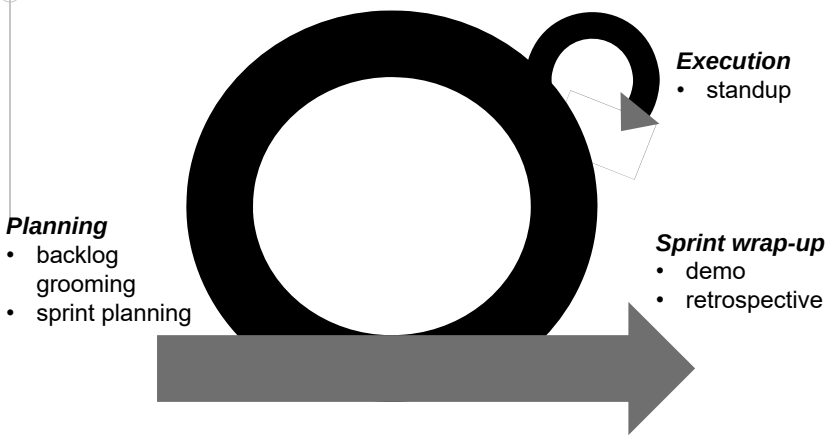
Each user story satisfies two goals at the same time:

- Describes the software requirement behavior cleanly
- Also describes a piece of development work for planning purposes

Ben Nahum & Livni, SDMD Europe Jan 2013

ShoeBar Associates

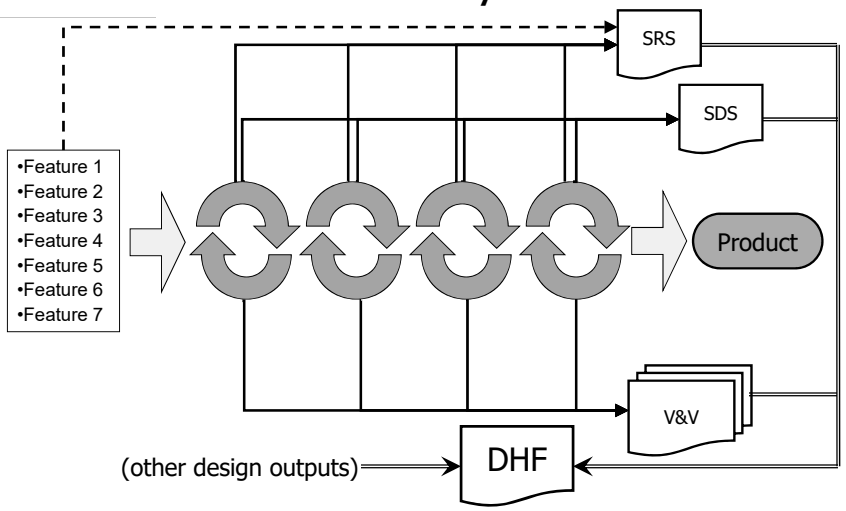
Iteration: Quality Process



Ben Nahum & Livni, SDMD Europe Jan 2013

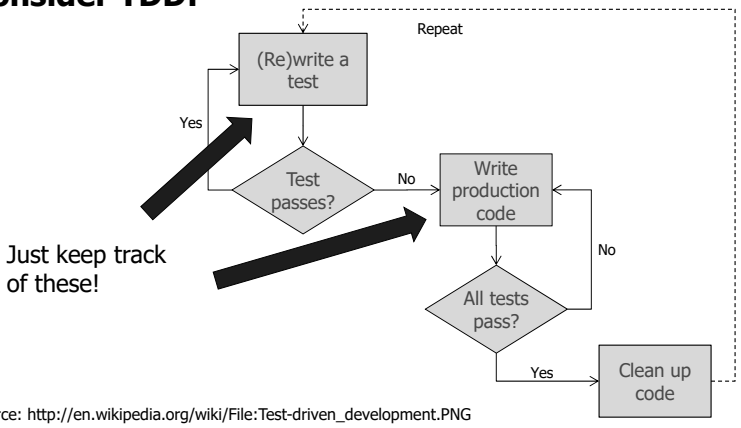
ShoeBar Associates

Document Cumulatively



How about Traceability?

Consider TDD:

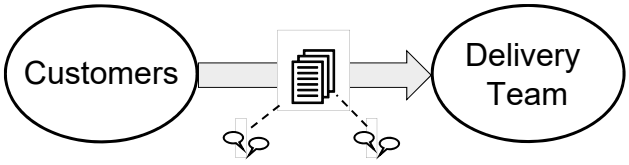


Just keep track of these!

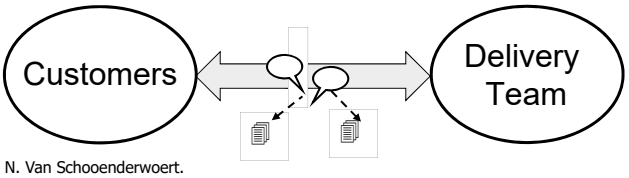
Source: http://en.wikipedia.org/wiki/File:Test-driven_development.PNG

Let Documents Be *Output*

- From **Document-centric**, supported by Conversation



- To **Conversation-centric**, supported by documents



Source: N. Van Schooenderwoert.

ShoeBar Associates

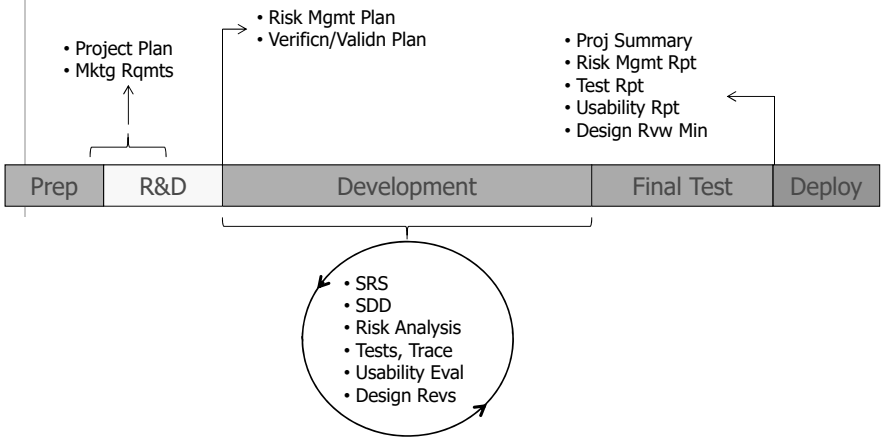
Documentation – what was done

From TIR 45:
'In an AGILE model, where a team is working together on a set of activities, documentation is less important to initiating an activity ("when we begin") and guiding an activity ("while we are working"), but documentation is still important to communicating the results of the activity ("when we are done").'

In his book *User Story Mapping*, Jeff Patton describes this as "taking vacation photos" so that the team can remember what they agreed on.

ShoeBar Associates

Document at time of generation

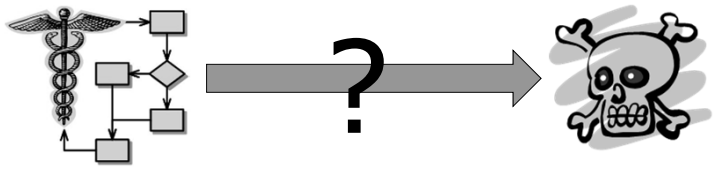


Source: N. Van Schooenderwoert.

Quality – Safety - Compliance

- *Face reality - Agile is here*
- *Docs – capture info when generated*
- **Iterative Risk Management: learning**
- *Agile events reinforce quality*
- *Agile: not an easy transition*

What is a software safety hazard?



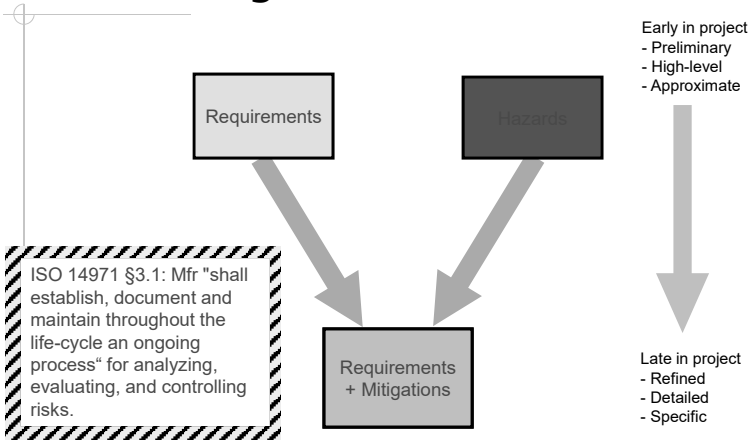
Some ideas - sources?

- Direct failure
- Permitted misuse
- User Complacency
- User Interface confusion
- Security vulnerability
- *Incorrect algorithm / logic*
- *No input checking*
- *Inadequate warnings*
- *Poor UI design, no validn*
- *No attention to security*

Who Should Help Evaluate?

- Electronic / Mechanical engineers?
- Physicians / Nurses?
- Patients who have used similar devices?
- Researchers who work on pain relief?
- Regulatory experts (review of other devices on market)?

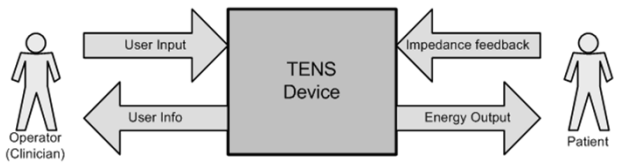
Risk Management *MUST* Iterate



TENS – a compact example

TENS, or transcutaneous electrical nerve stimulation, is a pain-relief therapy in which weak electrical signals are applied to a patient via standard skin electrodes.

The goal is for treatment to be fully automated: working parameters are to be set dynamically, with no manual adjustment required other than regulating stimulus intensity, which is manually set at the perception threshold.



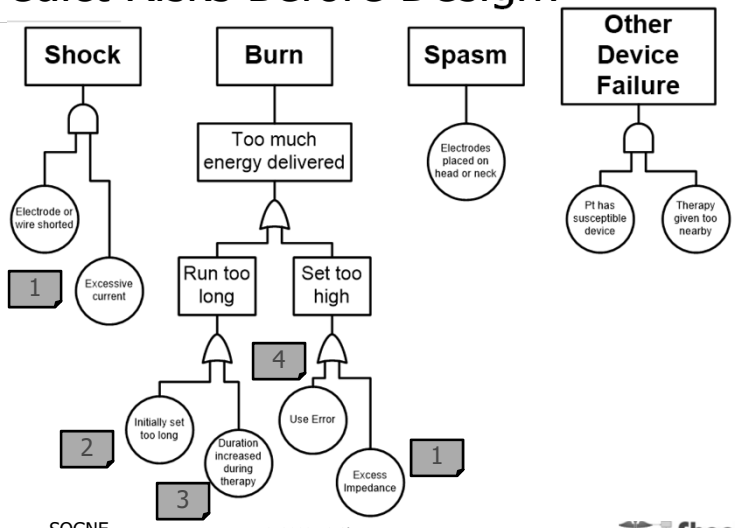
Mitigations – RM Stories

How could TENS harm a patient?

- Shock
- Burn
- Spasms
- Cause some other device to fail (e.g. cardiac device)

ShoeBar Associates

Predict Risks Before Design?



ShoeBar Associates

Risk Mitigation Stories

As a caregiver,
I want to ensure that therapy will stop if short, open circuit, or high impedance is detected,
to avoid harming the patient.

As a caregiver,
I want the unit to prevent setting duration longer once therapy has begun,
to avoid harming the patient.

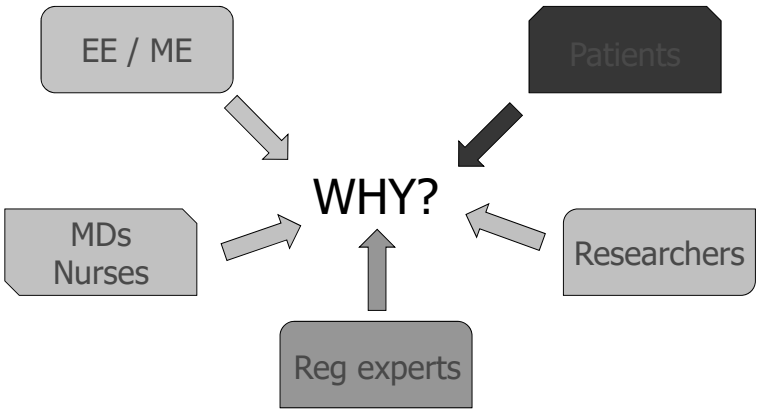
As a caregiver,
I want the unit to limit the therapy duration,
to avoid harming the patient.

As a caregiver,
I want the unit to prevent setting output too high,
to avoid harming the patient.

Is This Ever "Complete"?

- Do we know enough about hazards when a project begins?
- Will we learn as potential users try out our design?
- What other analyses can we do when we have a detailed design?
- Might we bring in other stakeholders later in development?

Team Diversity → Questions



ShoeBar Associates

Don't Forget Human Factors

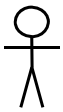
- Who will actually operate your system?
- Do you know what jobs they have to do every day? Where and under what conditions?

- What will make the device you're designing better than the one they're already using?
- How will you ever really know whether you've met their needs?
- **Could they misuse the system in a way that would hurt or kill the patient, the user, or a bystander?**

ShoeBar Associates

… Or Cybersecurity!

Use Cases



- Concern: harm to people or property – from normal use or permitted misuse
- Mitigation: prevent the hazardous action or warn user
- Information helps reduce the risk
- Typically, mitigate once

Abuse Cases

- Concern: unauthorized control of device, malicious altering of data, access to protected health information
- Mitigation: block vulnerability in software
- Information may *increase* risk of exploit
- Mitigation – must check repeatedly

Illustrations: Mass & McNair, SDMD 18, Oct 2014

Agile Practices Support RM

- Initial ("sprint zero") evaluation and planning
- Iteration and refinement, with frequent review
- Team diversity / cross-functionality
- Reducing complexity and coupling; providing transparency

Quality – Safety - Compliance

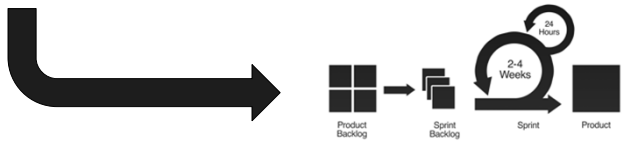
- *Face reality - Agile is here*
- *Docs – capture info when generated*
- *Iterative Risk Management: learning*
- **Agile events reinforce quality**
- *Agile: not an easy transition*

Plan – at multiple levels

Formal – high level

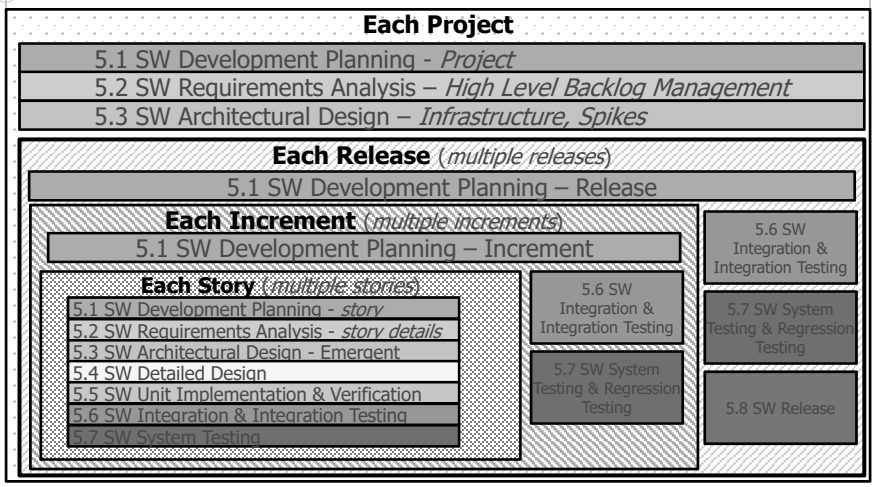
Goals
Resources
Milestones
Deliverables

An Agile team will find that they need more than a backlog and release strategy to cover some of these planning topics. They now will have to write formal plans around such subjects as testing (at all levels), risk management, and software configuration management. A good way to remain Agile is to document the high-level strategy / resources / schedules / milestones and use the story creation / backlog / increment / release management to plan and execute detailed tasks. Together, they form the software development plan for a project.

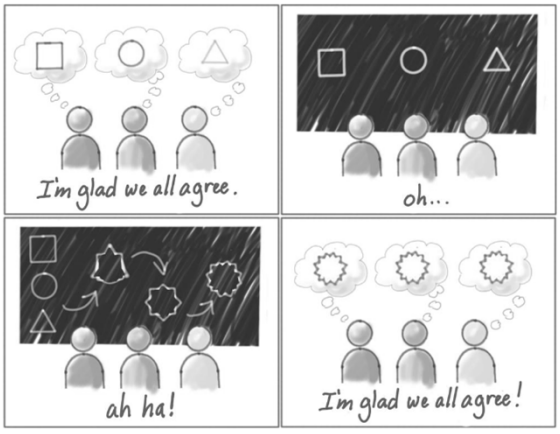


Less formal *(emergent details)*

Plan in "Layers"



Story Grooming: Common Understanding



Source: Patton, Jeff, and Peter Economy, *User Story Mapping: Discover the Whole Story, Build the Right Product*, Sebastopol CA, O'Reilly Media Inc, 2014.

Team Agreements for Quality

Image: http://www.nifter.com/free_clipart_downloads.htm

Typical Definitions

Ready:

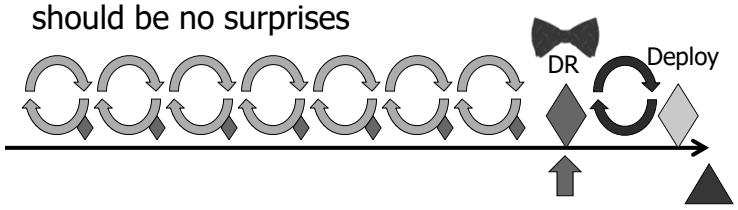
- Story has been estimated by the team
- All team members have seen the story and had their questions answered
- A test environment is available
- Story has clear conditions of satisfaction

Done:

- Code is checked in and unit tested
- Each feature functions in the demonstration environment
- Each story's conditions of satisfaction have been turned into system tests

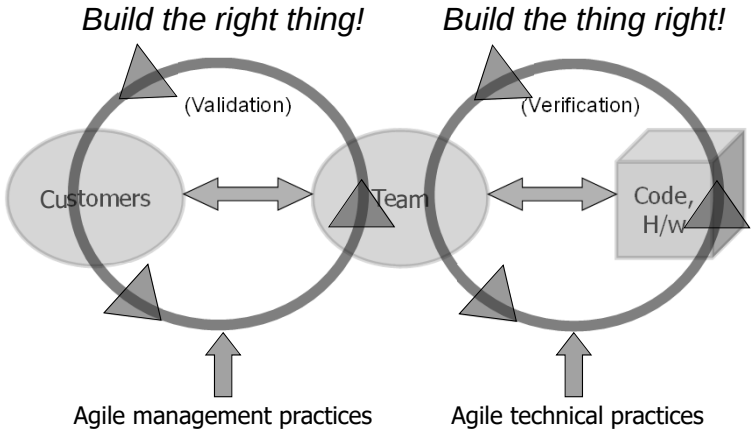
Demos can be design reviews

- Each iteration has design, dev, test, demo (♦)
- Each demo an incremental design review
- Document via memo to file – attendance, topics covered, issues/action items
- We'll hold the complete Design Review at the end – should be no surprises



ShoeBar Associates

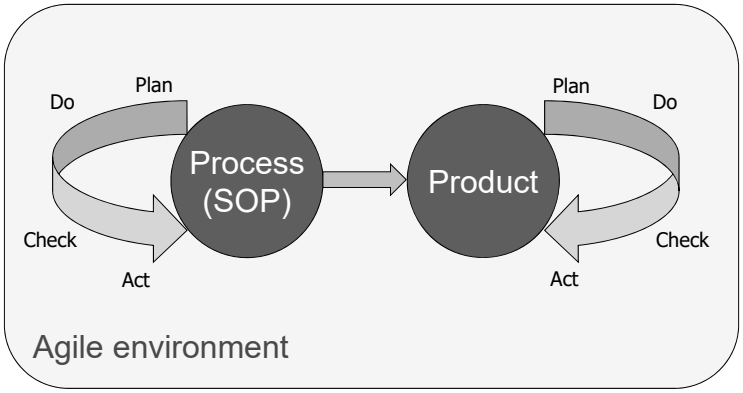
Dual Feedback Loops



Source: N. Van Schooenderwoert.

ShoeBar Associates

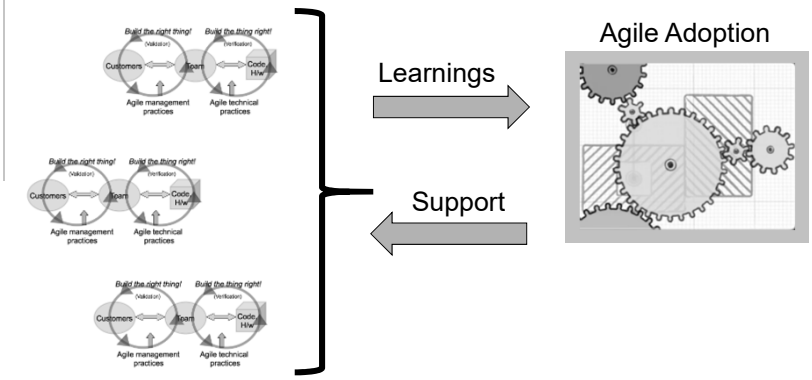
Retrospectives: Reflect and Improve



Quality – Safety - Compliance

- *Face reality - Agile is here*
- *Docs – capture info when generated*
- *Iterative Risk Management: learning*
- *Agile events reinforce quality*
- **Agile: not an easy transition**

Multiple Pilots are Essential

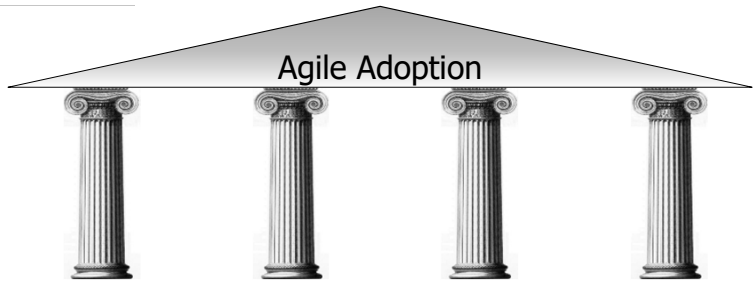


Source: N. Van Schooenderwoert.

Multiple Elements Are Essential

- High level product vision
- Access to REAL CUSTOMERS
  - Hospital med techs – Radiologists – Nurses - Patients, e.g. diabetics
- Collaboration across functions
  - SW, HW, UI design, marketing
- Managers need to participate!
  - Remove roadblocks, keep team focus

4 Pillars Must Support Agile Adoption

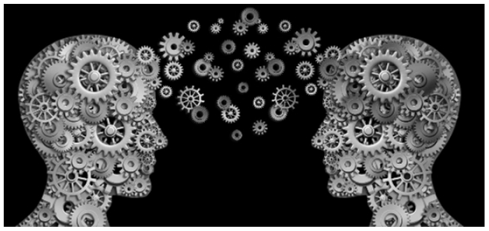


- Teams must be able to produce defect-free software sustainably
- Teams must consist of empowered, engaged people
- Workflow to the Agile teams must be controlled via a "pull" system
- Lean portfolio management must be used to control workflow for the organization

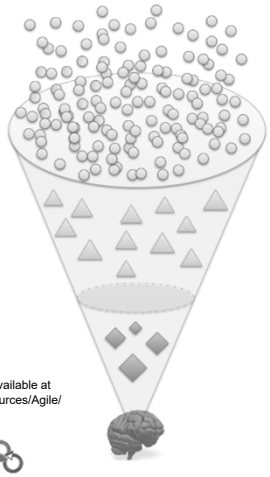
Challenge: the SOP Mindset

NOT this:

But this:



Agile Mindset – 3 Levels



Agile is a mindset

[that in software world is]

- Established through 4 values
- Grounded by 12 principles, &
- Manifested through many many different practices

Product visioning
Project chartering
Affinity (relative) estimation
Size-based (point) estimation
Planning poker
Group estimation
Value-based documentation
Prioritized product backlog
User stories
Progressive elaboration
Personas
Story maps / MMF
Story slicing
Acceptance tests as requirements
Short iterations
WIP Limits
Early and frequent releases
Roadmapping
Velocity-based planning and commitment
Iteration planning / Iteration backlog
Release planning / Release backlog
Time boxed iterations
Adaptive (multi-level) planning
Risk backlog
Team structure of VT / DT
Pull-based systems
Slack
Sustainable pace

Frequent face-to-face
Team chartering
Cross-silo collaborative teams
Self-organizing teams
Cross-functional teams
Servant leadership
Task volunteering
Generalizing specialist
Tracking progress via velocity
Burn-up/burn-down charts
Refactoring
Automated unit tests
Coding standards
Incremental/evolutionary design
Automated builds
Ten-minute build
Monitoring technical debt
Version control
Configuration management
Test driven development
Pair programming
Spike solutions
Continuous integration
Incremental deployment
Simple design
End-of-iteration hands-on UAT
Automated functional tests
Automated developer tests (unit tests)
Exploratory testing
Software metrics

Credit: Ahmed Sidky, "The Agile Mindset", available at http://www.softed.com/assets/Uploads/Resources/Agile/The-Agile-Mindset-Ahmed-Sidky.pdf

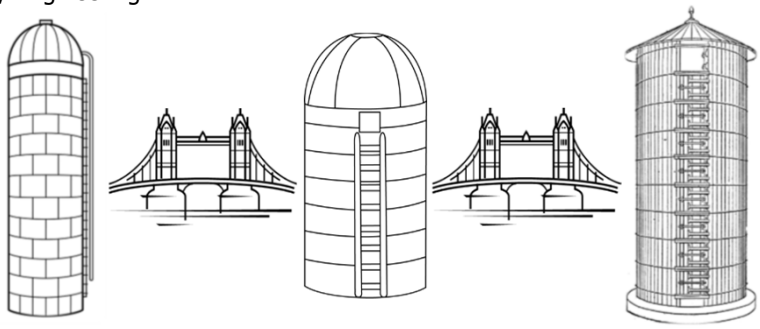
ShoeBar Associates

Bridge Those Silos!

R&D / Engineering

Clinical / Support

Marketing



ShoeBar Associates

What HAVEN'T I Discussed?

- Standards and their interrelations
- "Mapping" methods for planning (impact mapping, story mapping)
- Agile for mixed HW / SW development
- Scaling Agile to larger projects

These elements are also crucial in medical product development – we cover them in more detail in other presentations.

References

- AAMI TIR45:2012 "Technical Information Report: Guidance on the use of AGILE practices in the development of medical device software", Association for the Advancement of Medical Instrumentation, August 2012. (available at http://my.aami.org/store/)
- Agile Manifesto: http://agilemanifesto.org/
- Ben Nahum, Boaz, and Hagai Livni, From Generation Based Product to a Brand New One: Accelerating Scrum through advanced methodologies, testing & collaboration, presented at Third Software Design for Medical Devices Europe, 29.-30. January 2013, Munich Germany.
- ISO 14971: Medical devices — Application of risk management to medical devices, International Organization for Standardization, Second edition 1. March 2007.
- Maass, Eric, and Patricia McNair, Managing Risk Exposure and Reducing Field Corrective Actions, presented at Eighteenth Software Design for Medical Devices, 27. - 28. October 2014, Boston MA.
- Patton, Jeff, and Peter Economy, *User Story Mapping: Discover the Whole Story, Build the Right Product*, Sebastopol CA, O'Reilly Media Inc, 2014.
- Scrum diagram: https://www.mountaingoatsoftware.com/agile/scrum/resources/overview
- Sidky, Ahmed, "The Agile Mindset", available at http://www.softed.com/assets/Uploads/Resources/Agile/The-Agile-Mindset-Ahmed-Sidky.pdf
- Test-driven development: http://en.wikipedia.org/wiki/File:Test-driven_development.PNG
- U.S. Food and Drug Administration, *Design Control Guidance For Medical Device Manufacturers*, 11-March-1997.

Contact Information

Brian Shoemaker, Ph.D.
Principal Consultant, ShoeBar Associates
199 Needham St, Dedham MA 02026 USA
+1 781-929-5927
bshoemaker@shoebarassoc.com
http://www.shoebarassoc.com

ShoeBar
Associates