Software Division

When It Just ***Has*** to Work:

Agile Development in Safety-Critical Environments

Brian Shoemaker

ShoeBar Associates

Nancy Van Schooenderwoert

Lean-Agile Partners Inc.

Nancy'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

ShoeBar Associates Lean-Agile Partners

Brian's Background

- 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)
- 4 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 Lean-Agile Partners

When it just ***has*** to work: Agile Development in Safety-Critical Environments

- **Software too often contributes to poor safety**
- Lean principles → new style of organization & new tools
- Risk management benefits from iteration
- Essential elements: flexibility and learning, but rigor and documentation
- Teams report positive experiences

ShoeBar Associates Lean-Agile Partners

Software Can Compromise Safety

- Chemical plants
- Power stations (esp. nuclear)
- Aviation systems (civilian & military)
- Other transportation systems
- Medical devices

ShoeBar Associates Lean-Agile Partners

Right problem, wrong solution

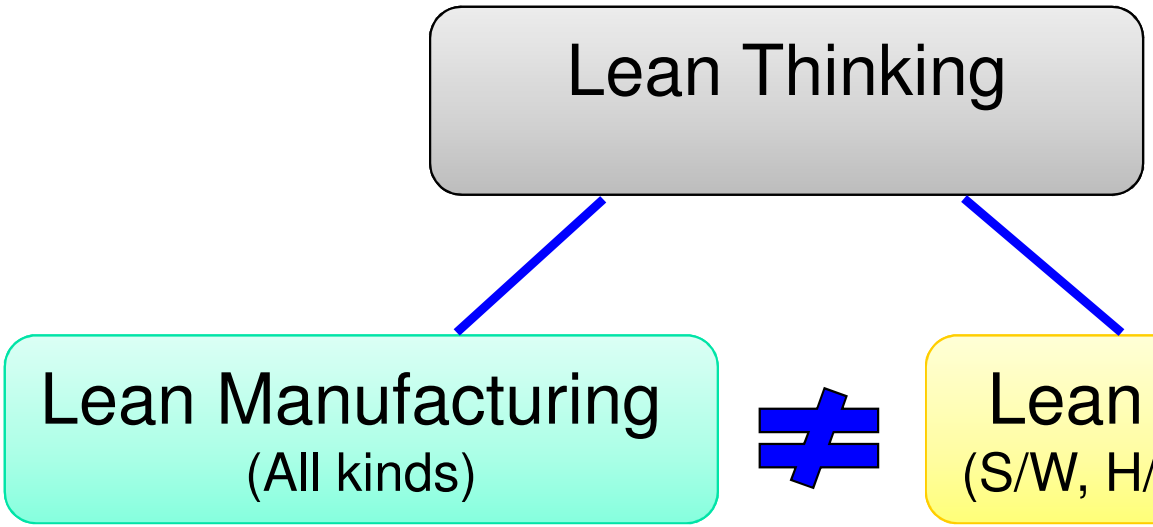
- Software issues prompt significant number of recalls
- Many still claim solution lies in rigorous, stepwise development
- Our view is that a different lifecycle is needed
- But we arrive at the same goal

When it just ***has*** to work: Agile Development in Safety-Critical Environments

- *Software too often contributes to poor safety*
- **Lean principles → new style of organization & new tools**
- Risk management benefits from iteration
- Essential elements: flexibility and learning, but rigor and documentation
- Teams report positive experiences

ShoeBar Associates Lean-Agile Partners

Lean Thinking



Lean Principles:

Zero Defects
Minimize Work In Progress
Continuous Improvement

Lean Manufacturing
(All kinds)

≠

Lean Development
(S/W, H/W, Services, other)

Common "pain points":

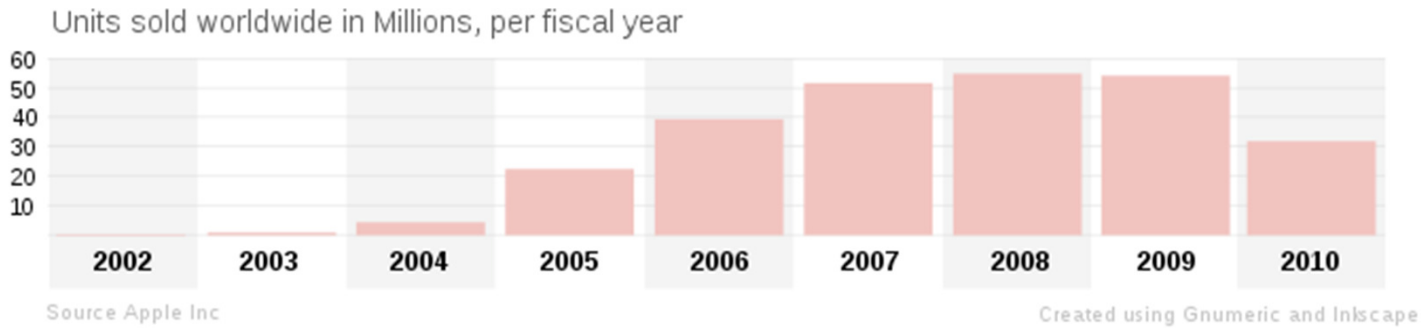
Bad news late in projects
Implementation different from spec
Documentation issues

Classic "best practices"
Agile practices:
- Continuous Integration
- Automated unit tests
- Small co-located teams

ShoeBar Associates Lean-Agile Partners

Nothing new in Agile?

- Iterative development example – Ipod



- Agile revives a proven engineering tradition

Source: Apple Ipod info courtesy of Wikipedia, http://en.wikipedia.org/wiki/Ipod. Not all 2010 data is complete.

ShoeBar Associates

Lean-Agile Partners

Yes Agile teams *DO* Plan

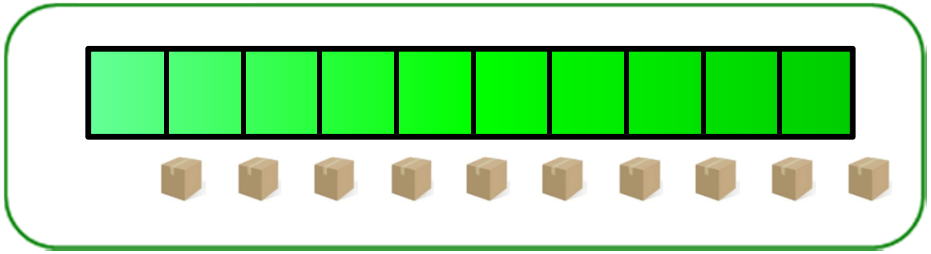
- We use mini specs called ‘Stories’
- But they *WILL* change.
- Change does not break Agile
- Like palm trees in a storm, Agile process bends with changes

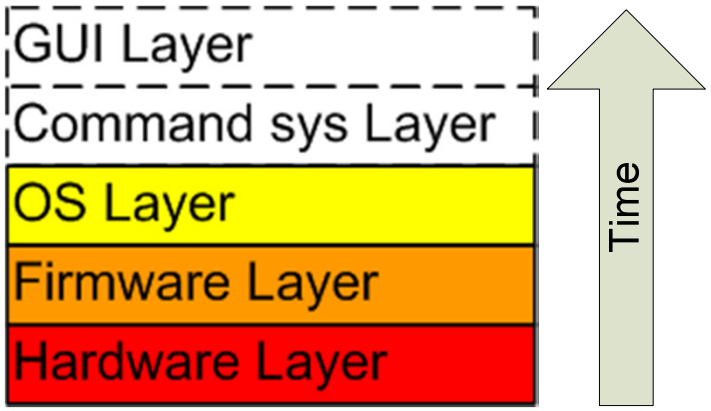
ShoeBar Associates Lean-Agile Partners

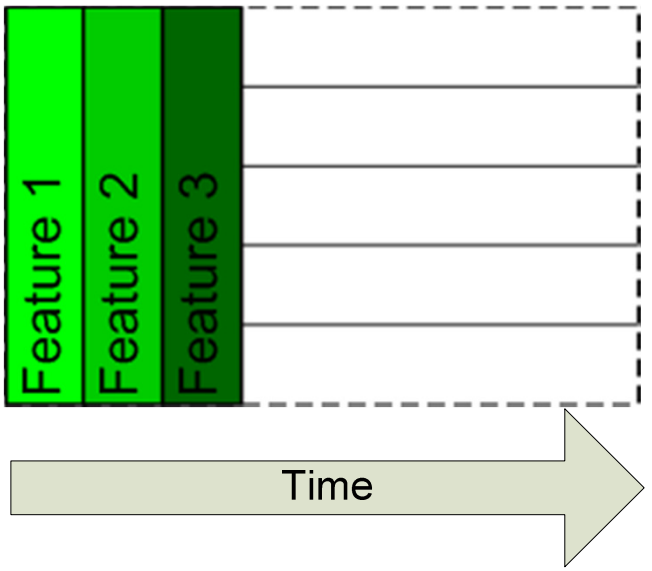
Deliver in *Working* Increments

Not This:

But This:







ShoeBar Associates

Lean-Agile Partners

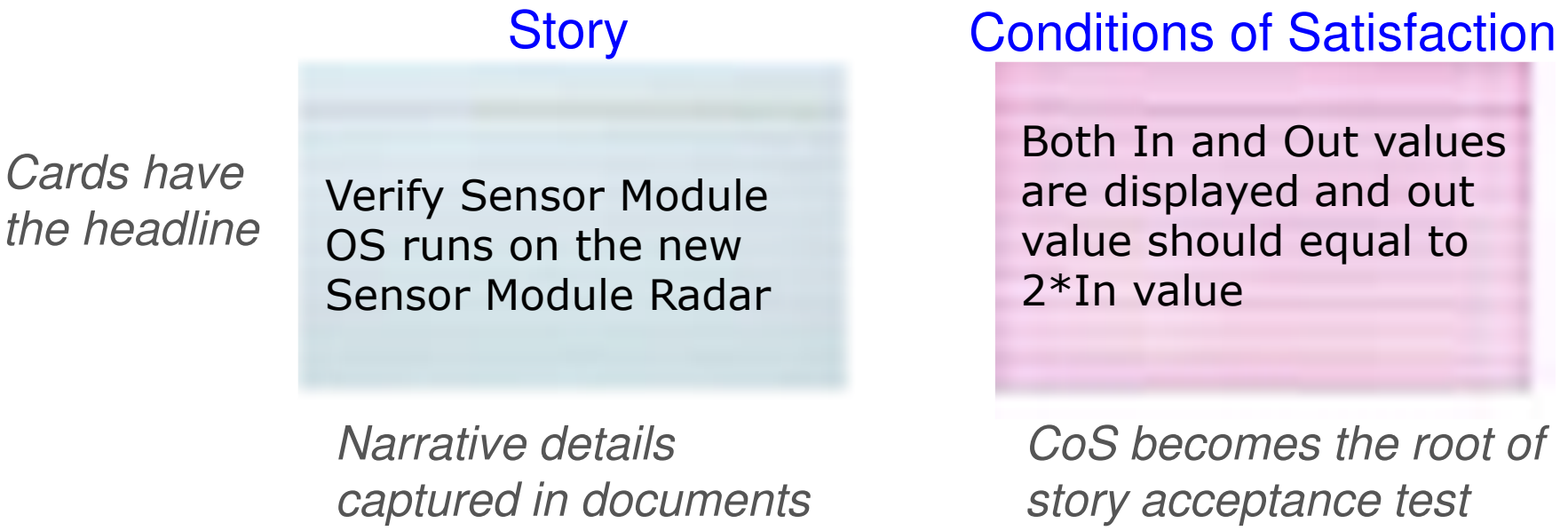
Work pieces: user stories

- User stories are similar to use cases
  - Written from customer view point
  - Written using words all understand
- Smaller than use cases
- Estimates are owned by the team
  - *Equally* likely to be too high or too low

ShoeBar Associates Lean-Agile Partners

Example user story

- Story – Card, Conversation, Confirmation – *headline, narrative, test*



An old idea: If you have a clear goal, you are much more likely to achieve it.

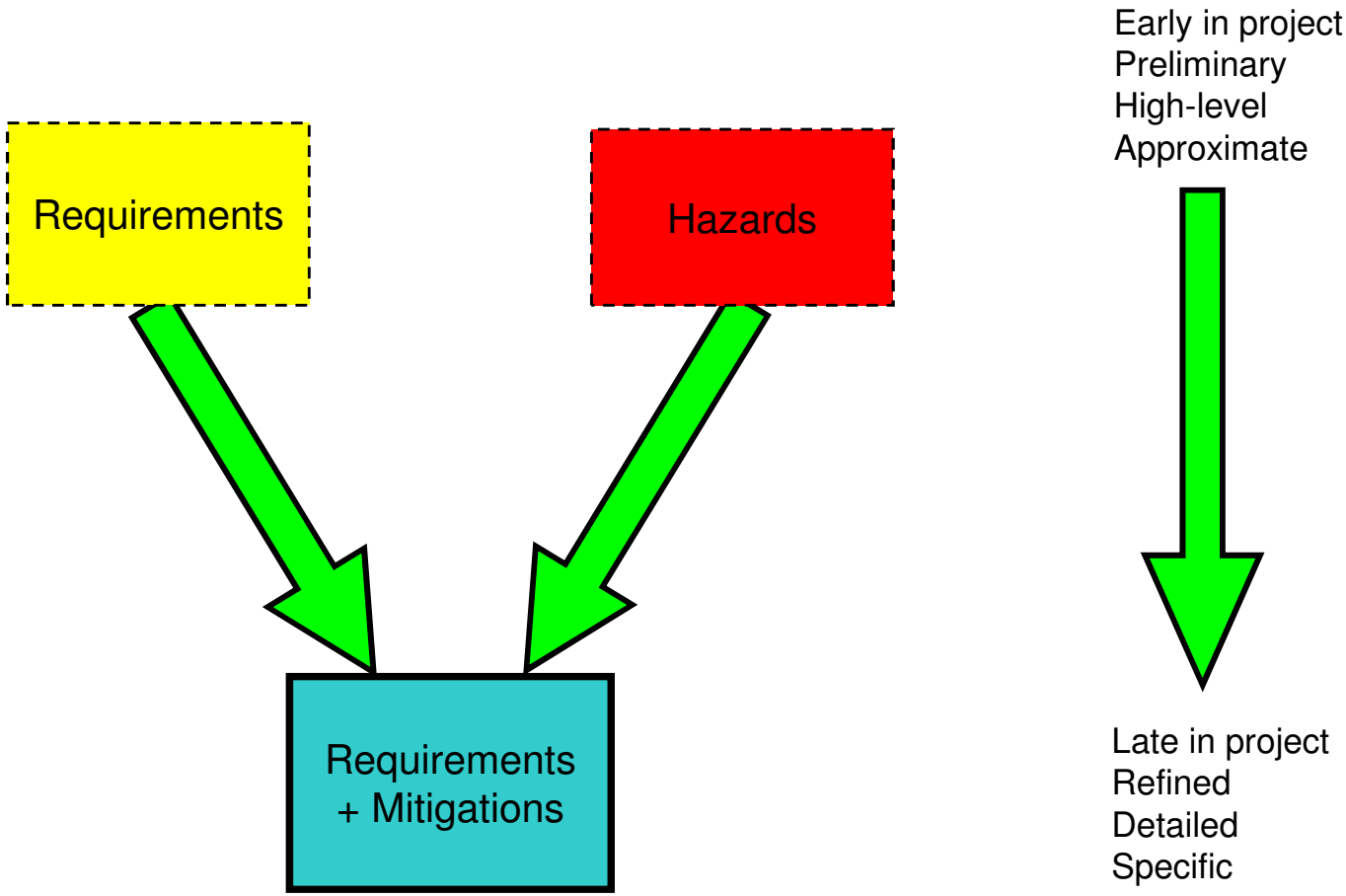
ShoeBar Associates Lean-Agile Partners

When it just ***has*** to work: Agile Development in Safety-Critical Environments

- *Software too often contributes to poor safety*
- *Lean principles → new style of organization & new tools*
- **Risk management benefits from iteration**
- Essential elements: flexibility and learning, but rigor and documentation
- Teams report positive experiences

ShoeBar Associates Lean-Agile Partners

Requirements / Hazards: Converging Analyses



ShoeBar Associates Lean-Agile Partners

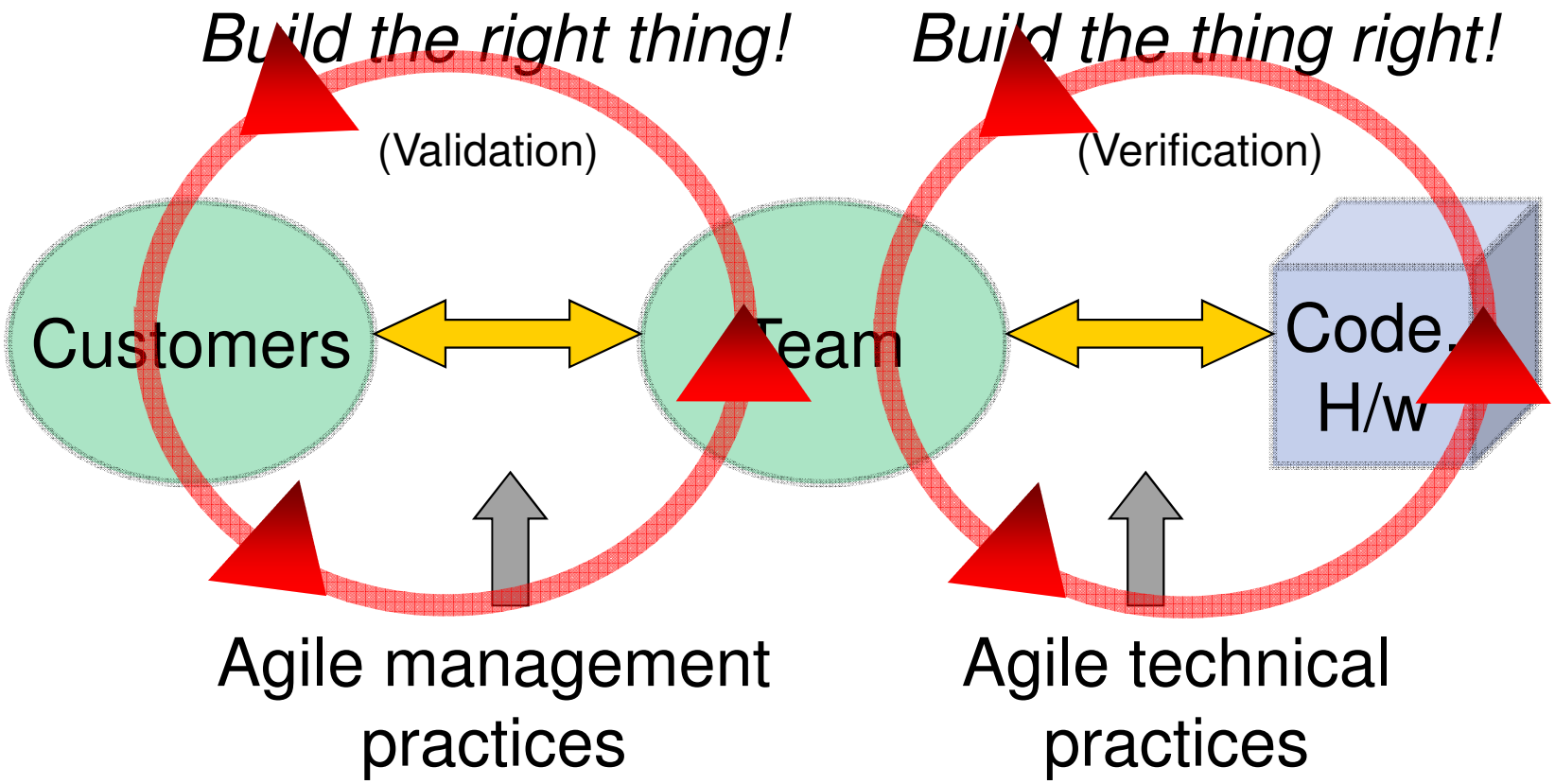
Risks: Analyze Early and Often

- Systematic methods (FMEA / FMECA, FTA) help analyze potential hazards
- Evaluate hazards repeatedly throughout project
- Just as requirements (aka User Stories) become more refined as design evolves -
- So identifying hazard mitigations is changing or adding to requirements
- *Think of a hazard as a negative user story*

ShoeBar Associates Lean-Agile Partners

Partnership: Business - Technical

Agile process has strong internal control loops



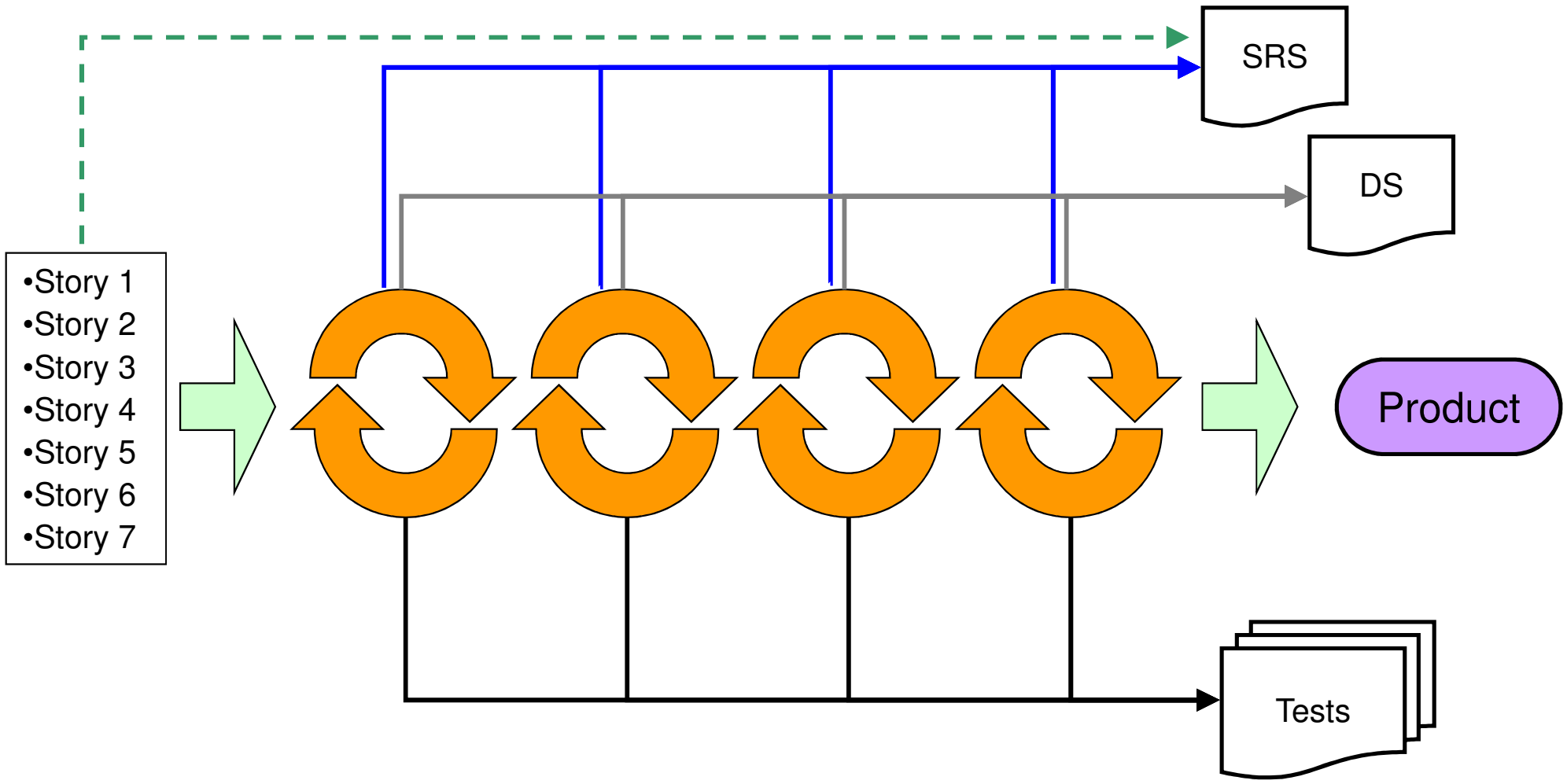
ShoeBar Associates Lean-Agile Partners

When it just ***has*** to work: Agile Development in Safety-Critical Environments

- *Software too often contributes to poor safety*
- *Lean principles → new style of organization & new tools*
- *Risk management benefits from iteration*
- **Essential elements: flexibility and learning, but rigor and documentation**
- Teams report positive experiences

ShoeBar Associates Lean-Agile Partners

Capture knowledge as work proceeds



ShoeBar Associates Lean-Agile Partners

Specs as a “push” system

- Large spec documents queue information and let it become stale
- Queues and large batches are signs of trouble in lean systems
- Lean-Agile teams “pull” the information they need from a product owner
  - By writing user stories together
  - Through questions raised when estimating
- Each story is a mini-spec, and its “Condition of Satisfaction” (CoS) is a criterion to test against

Lean documentation

- Many forms – models, simulation, text, and tests as ‘executable specs’
- Written at team’s level
- Like fresh fruit – best used soon after created
- “pulled” from product owner as needed – to avoid rework
- Traditional documentation does not scale adequately

When it just ***has*** to work: Agile Development in Safety-Critical Environments

- *Software too often contributes to poor safety*
- *Lean principles → new style of organization & new tools*
- *Risk management benefits from iteration*
- *Essential elements: flexibility and learning, but rigor and documentation*
- **Teams report positive experiences**

ShoeBar Associates Lean-Agile Partners

What Do Defect Outcomes Suggest?

Team	Defects/Function Point	
Follett Software[1]	0.0128	agile
BMC Software[1]	0.048	agile
GMS[2]	0.22	agile
Industry Best[3]	2.0	traditional
Industry average[3]	4.5	traditional

1 Computed from data reported in Cutter IT Journal, Vol. 9, No. 9 (Sept 2008), page 10
2 "Newbies" paper presented at Agile 2006. See last slide for full reference.
3 Capers Jones presentation for Boston SPIN, Oct., 2002

ShoeBar Associates Lean-Agile Partners

Case: Device Software

- Authors compared one Agile and one non-Agile project: found that Agile gave lower cost, shorter development time, better accommodation of change, better test cases, and higher quality
- Considered risk as integral part of development
- Iterative approach helped manage scope and limit feature creep
- Initial version was launched *without* a number of features thought essential at first (some took up to 3 yrs to add) – but product was successful and trading off nice-to-have features for 3 years of sales was easy.

Quote for the Day

"It is not the strongest of the species that survive, not the most intelligent, but the one most responsive to change."

- Charles Darwin

ShoeBar Associates Lean-Agile Partners

Recommended Reading

- *Implementing Lean Software Development* by Mary & Tom Poppendieck
- *Agile Estimating & Planning* by Mike Cohn
- *The Elegant Solution* by Matthew May
- *The Goal* by Eliyahu Goldratt
- *Release It!* by Michael Nygard
- *Safeware* by Nancy Leveson

ShoeBar Associates Lean-Agile Partners

References

- Cutter article by Michael Mah (on Follett, BMC Software), available by emailing him at michael.mah@qsma.com
- 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 (Gives statistics reported for GMS team), presented at Agile 2006
- Weyrauch, Kelly, “Safety-Critical. XP Rules.”, *Better Software*, July/August 2004.
- EduQuest, Inc., "FDA Auditing of Computerized Systems and Part 11," notes from course given July 2005.

ShoeBar Associates Lean-Agile Partners

Standards – Software Safety

- AAMI TIR32:2004 Medical device software risk management
- IEC 60812:2006 (2nd ed) Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)
- IEC 60601-1: 2005 (3rd ed) Medical electrical equipment – Part 1: General requirements for basic safety and essential performance *(60601-1-4 "Programmable Electrical Medical Systems" is available standalone, but will not be in the future)*
- IEC 62304:2006 Medical Device Software – Software Life Cycle Processes
- ISO 13485:2003 (2nd ed) Medical devices – Quality management systems – Requirements for regulatory purposes
- ISO 14971:2007 (2nd ed) Medical devices – Application of risk management to medical devices

References – FDA Documents

Design Control Guidance For Medical Device Manufacturers (March 11, 1997), http://www.fda.gov/cdrh/comp/designgd.html

General Principles of Software Validation (January 11, 2002), http://www.fda.gov/cdrh/comp/guidance/938.html

Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices (May 11, 2005), http://www.fda.gov/cdrh/ode/guidance/337.html

Off-The-Shelf Software Use in Medical Devices (Sep. 9, 1999), http://www.fda.gov/cdrh/ode/guidance/585.html

Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software (Jan. 14, 2005), http://www.fda.gov/cdrh/comp/guidance/1553.html

ShoeBar Associates Lean-Agile Partners

Contact Information

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

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