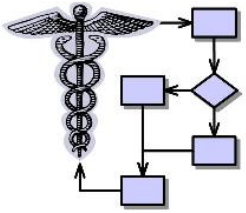


ShoeBar Associates

Lean-Agile Partners

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**
- Iterative approach shifts the planning culture
- Risk management benefits from iteration
- Team Autonomy forces a rethink on interactions
- Iterations → Safer product, Happy auditors

ShoeBar Associates

Lean-Agile Partners

Software Can Compromise Safety

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

Safety Critical = Regulated

- Some industries (e.g. aviation): regulations prescribe methodology
- FDA-regulated (medical devices, blood banks): use any method, but show the outputs

S/W Safety Examples Abound

- **September 16, 2008: Automated External Defibrillator recalled**
  http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfRES/res.cfm?ID=73249
  Device was configured with the incorrect software, for semi-automatic instead of fully automatic use. When needed for a cardiac arrest emergency, device will require user to press the shock button instead of automatically delivering a shock (but the shock button is covered).
- **August 2, 2008: MultiLeaf Collimator recalled**
  http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfRES/res.cfm?ID=68342
  Charged-particle radiation therapy system. ***Dose Calculation Error***: Software anomaly may result in failure of a MLC leaf to reach planned position, potentially resulting in misadministration of dose to a patient.
- **July 29, 2008: Cardiac Resynchronization Therapy Defibrillator (CRT-D) recalled**
  http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfRES/res.cfm?ID=68220
  Timing Feature Error: An implementation error allows the usage of the V-V timing feature, which is not approved for use in the U.S.

ShoeBar Associates Lean-Agile Partners

S/W Safety Examples Abound

- **March 6, 2007: AEDs recalled**
  http://www.fda.gov/oc/po/firmrecalls/defibtech03_07.html
  Self-test software may allow a self-test to clear a previously detected low battery condition
- **September 2006: Infusion pump**
  http://www.fda.gov/cdrh/recalls/recall-081006.html
  Touch-sensitive keypad used to program the pump sometimes registers a number twice when it has been pressed only once ("key bounce"). Thus the pump would deliver more than the intended amount of medication, leading to over-infusion and serious harm or death to the patient.
- **June 6, 2006: Ventilators recalled**
  http://www.fda.gov/oc/po/firmrecalls/hamilton06_06.html
  Older generation software - incorrect oxygen cell calibration (without compressed air supply) - can ***disable*** all alarms
- **March 6, 2006: Dialysis device recalled**
  http://www.fda.gov/cdrh/recalls/recall-081605.html
  Class I recall of dialysis device (11 injuries, 9 deaths): excessive fluid loss may result if caregiver overrides device's "incorrect weight change detected" alarm. (Device used for continuous solute and/or fluid removal in patients with acute renal failure.)

ShoeBar Associates Lean-Agile Partners

S/W Safety Examples Abound

- **June 2001: Radiation treatment planning software**
  http://www-pub.iaea.org/MTCD/publications/PDF/Pub1114_scr.pdf
  Software used to calculate dose duration for radiation treatment of cancer would allow use of no more than four protective blocks (stated in the user guide). Physicians at Natl. Cancer Institute in Panama devised a way to "fool" the software into using five blocks, by entering data as if they were a single shape. If coordinates entered a specific way, the calculated dose would be as much as twice that intended. Users did not confirm calculated results; at least five patients died as a direct result of overexposure to radiation.

Right problem, wrong solution

- Software issues prompt significant number of recalls
- Many still claim solution lies in rigorous, stepwise development

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

- *Software too often contributes to poor safety*
- **Iterative approach shifts the planning culture**
- Risk management benefits from iteration
- Team Autonomy forces a rethink on interactions
- Iterations → Safer product, Happy auditors

ShoeBar Associates

Lean-Agile Partners

Planning: Reframe the Questions

- We always hear:
  "How long will it take?" and
  "How much will it cost?"
- Hear the assumption – marketing / customer says what they want (once!) then engineers go build it
- *Make no mistake*: for safety-critical, there's no substitute for a clear idea of where you're going
- A list of planned features is not the same as a rigid Work Breakdown Structure!

Why Agile?

- Agile's two great strengths:
  - Fast time to market
  - Ability to hit a moving target - "tracer bullets"

Image is from: www.army.mil.nz/.../365/image-gallery/16.htm

ShoeBar Associates Lean-Agile Partners

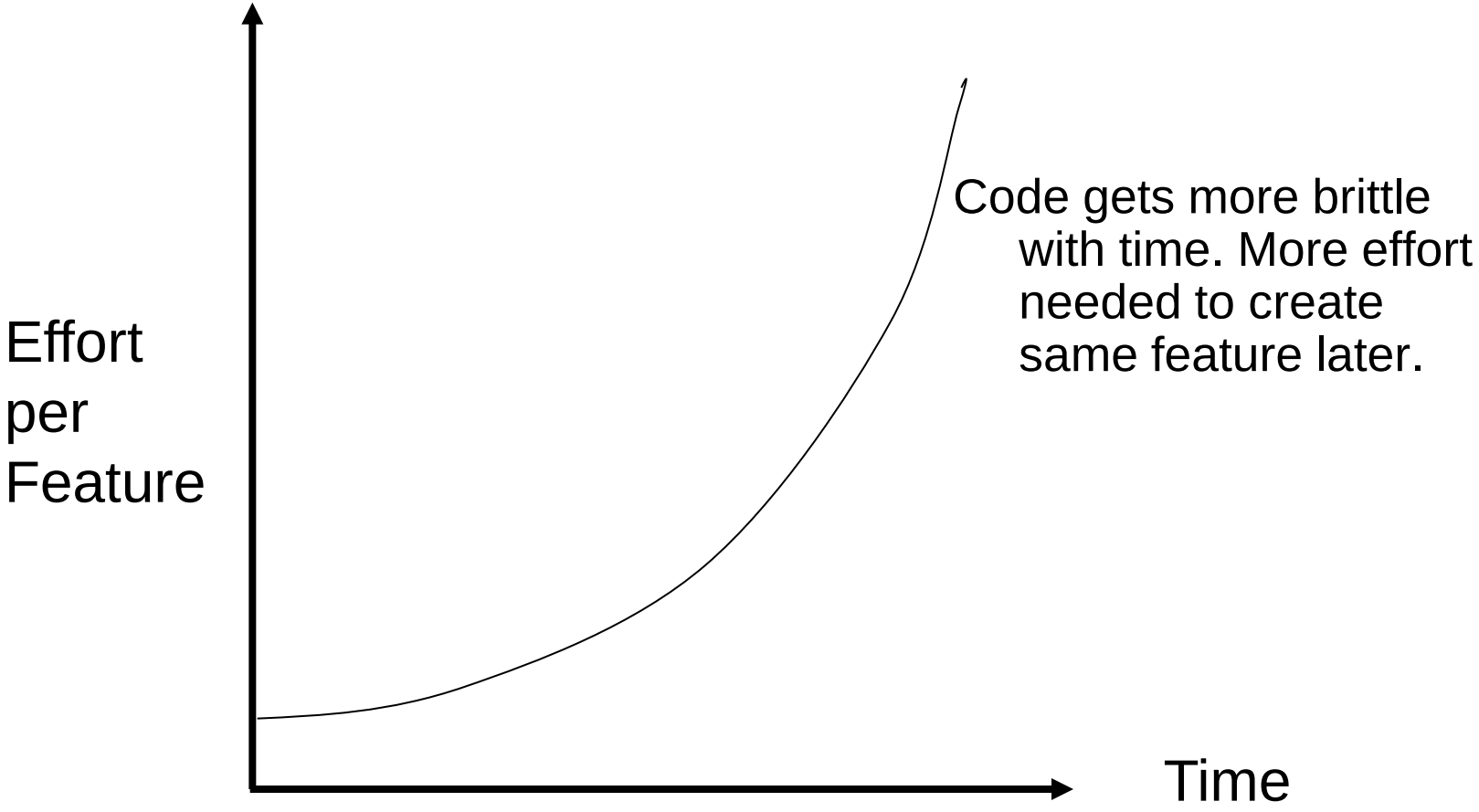
First, A Question…

- When do you know for certain how much a project costs?
- Agile teams bring that certainty forward in time

ShoeBar Associates

Lean-Agile Partners

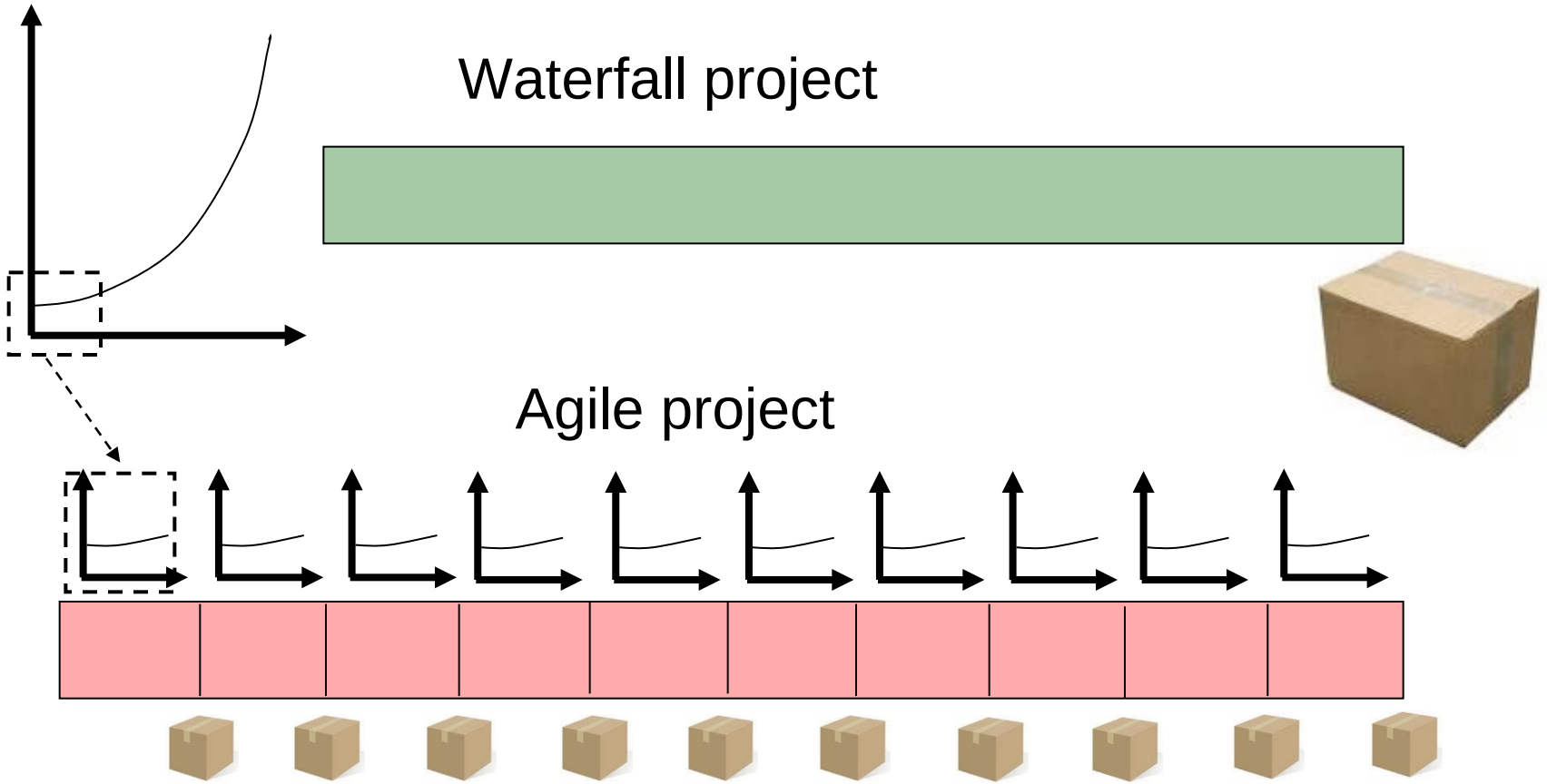
Non-Linear Effort vs. Results



ShoeBar Associates

Lean-Agile Partners

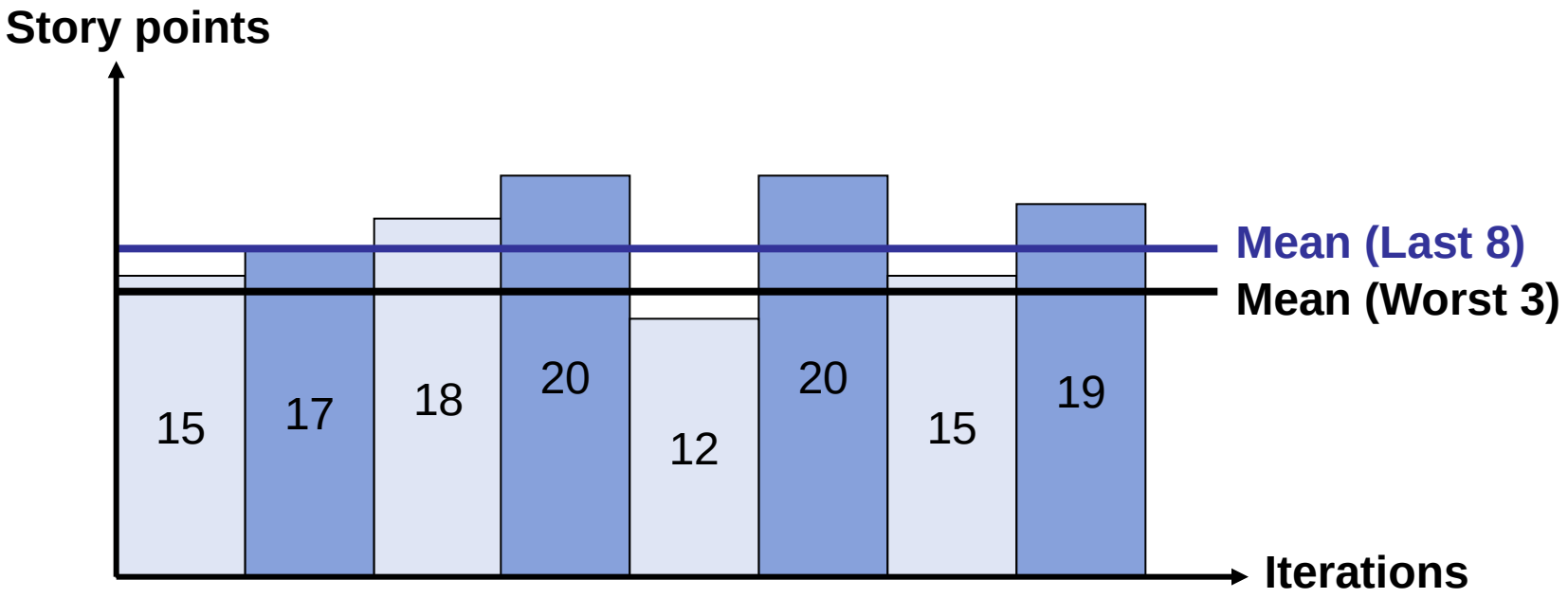
Linear Effort vs. Results



ShoeBar Associates

Lean-Agile Partners

Velocity



Allows us to calibrate iteration commitments (*yesterday's weather*) and forecast future progress

Ref: Mike Cohn, *Agile Estimating and Planning*

ShoeBar Associates Lean-Agile Partners

Questions?

ShoeBar Associates

Lean-Agile Partners

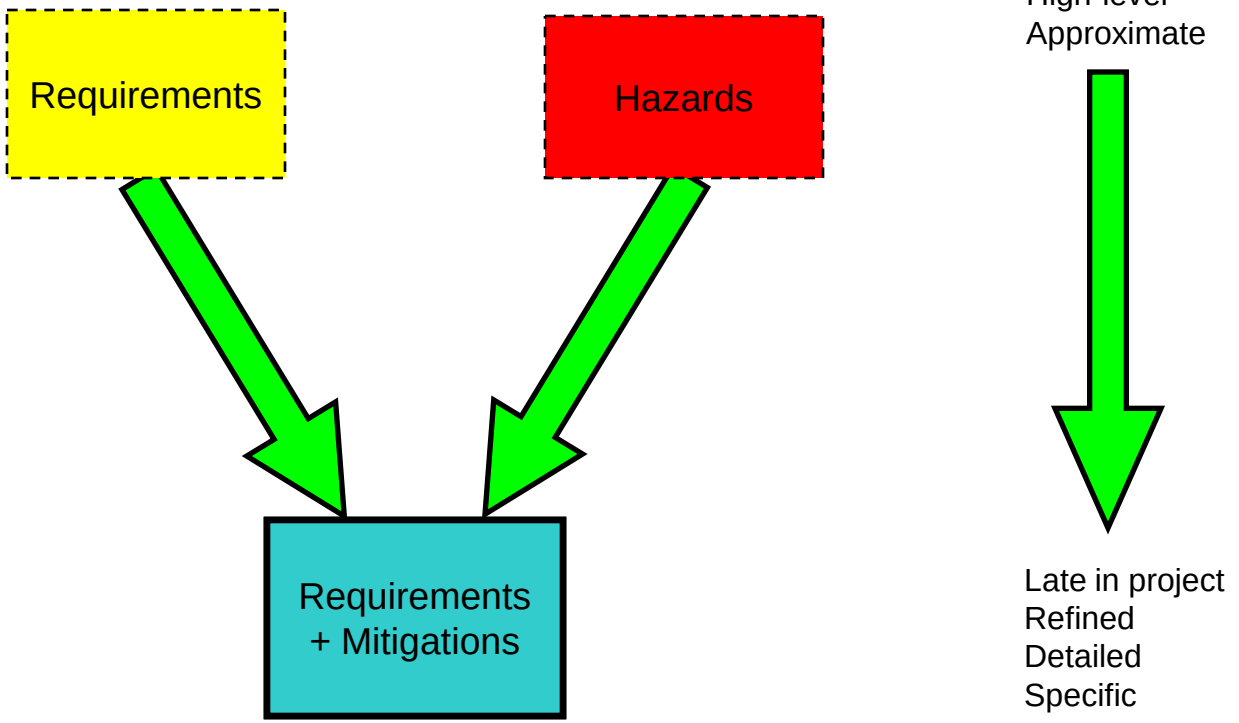
When it just ***has*** to work: Agile Development in Safety-Critical Environments

- *Software too often contributes to poor safety*
- *Iterative approach shifts the planning culture*
- **Risk management benefits from iteration**
- Team Autonomy forces a rethink on interactions
- Iterations → Safer product, Happy auditors

ShoeBar Associates

Lean-Agile Partners

Requirements / Hazards: Converging Analyses



ShoeBar Associates

Lean-Agile Partners

Classical Risk Ranking

	Probability:			
Severity:	High	Occasional	Low	Remote
Major	U	U	U	A
Moderate	U	A	A	N
Minor	A	A	N	N

Acceptability is ranked as follows:

U = unacceptable – mitigation required

A = ALARP (as low as reasonably practicable) – mitigate as reasonable; risk decision must be documented and reviewed

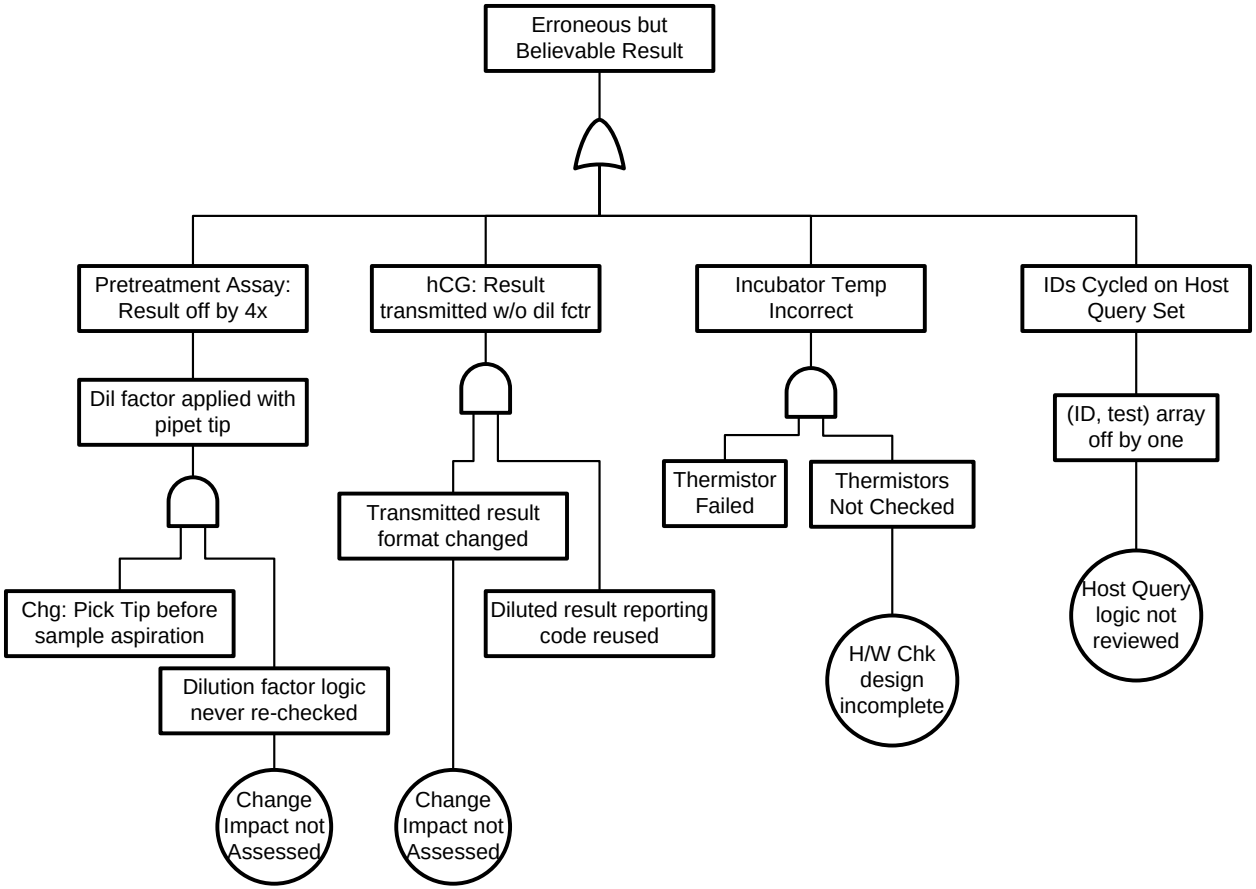
N = negligible – acceptable without review

Risks: Analyze Early and Often

- Hazards identified through systematic methods (FMEA, FMECA, or FTA)
- Requirements: become more refined as design evolves
- Hazards: evaluate repeatedly throughout project
- Systematic analysis: best if we know the design
- Hazard mitigation: changing or adding to requirements

ShoeBar Associates Lean-Agile Partners

FTA: Work Back from Potential Hazards



ShoeBar Associates Lean-Agile Partners

FMEA: Build Up from Component Failures

Failure Mode	Effect	Causes	S1	Mitigation	S2
Sample ID / results array off by one	Wrong results reported	Inconsistent array logic; incorrect initialization	5	Optional – operator approve results before saving	2
Initialization fails to warm up lamp	Can't perform analyses	Startup logic can be set to skip steps and left that way	4	Reset all startup parameters on initialization	1
Dilution factor associated with pipet tip, picked in advance	Wrong result reported (dilution applied to wrong sample)	Counting logic not rechecked when pick-in-advance process introduced	5	(a) Track dilution and pipet tip separately; (b) show dilution with reported result	1

S1 = Severity rating before mitigation; S2 = severity rating after mitigation
Severity (sample values only): 5 = critical; 1 = nuisance
Note this analysis does not include two of the standard engineering estimates: occurrence (probability) or detection.

ShoeBar Associates Lean-Agile Partners

Hazards: Often Caught in Context

- Direct failure
  Software flaw in normal, correct use of system causes or permits incorrect dosage or energy to be delivered to patient.
- Permitted misuse
  Software does not reject or prevent entry of data in a way that (a) is incorrect according to user instructions, and (b) can result in incorrect calculation or logic, and consequent life-threatening or damaging therapeutic action.
- User Complacency
  Although software or system clearly notes that users must verify results, common use leads to over-reliance on software output and failure to cross-check calculations or results.

Hazards: Often Caught in Context

- User Interface confusion

  Software instructions, prompts, input labels, or other information is frequently confusing or misleading, and can result in incorrect user actions with potentially harmful or fatal outcome.

- Security vulnerability

  Attack by malicious code causes device to transmit incorrect information, control therapy incorrectly, or cease operating. No examples in medical-device software known at this time, but experience in personal computers and "smart" cellular phones suggests this is a serious possibility.

Consider an example

- System: life-sustaining device (must run continuously to keep patient alive).
- Design: main control program on computer board, multiple components (motors, valves) driven by controller firmware communicating with main CPU
- Issue: firmware ends transmission with null, not terminator string and checksum as expected. Main program cannot detect dropped bits and request retransmit.
- Effect: system malfunctions if internal comm is noisy
- Action (possible): for testing, read full controller response string at each communication – confirm vendor firmware fix
- Result: Direct observation allows monitoring fix of late-learned hazard

Grain Monitor System

- Measures protein, oil in corn, wheat, etc. in seconds
- Based on new science, new CPU, new OS port, new NIR sensor, new algorithm…
- Agile team delivered 1st field units in 6 months

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

Questions?

ShoeBar Associates

Lean-Agile Partners

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

- *Software too often contributes to poor safety*
- *Iterative approach shifts the planning culture*
- *Risk management benefits from iteration*
- **Team Autonomy forces a rethink on interactions**
- Iterations → Safer product, Happy auditors

ShoeBar Associates Lean-Agile Partners

Accountability

- “When everyone’s accountable, no one’s accountable.” - True?
- Experienced, healthy agile teams report that each individual feels accountability for all team commitments
- Is this real? Can it be replicated?

Agile Team as Virtual Brain

- Specialized yet coordinated
- Cooperating
- Decisions made & carried out smoothly

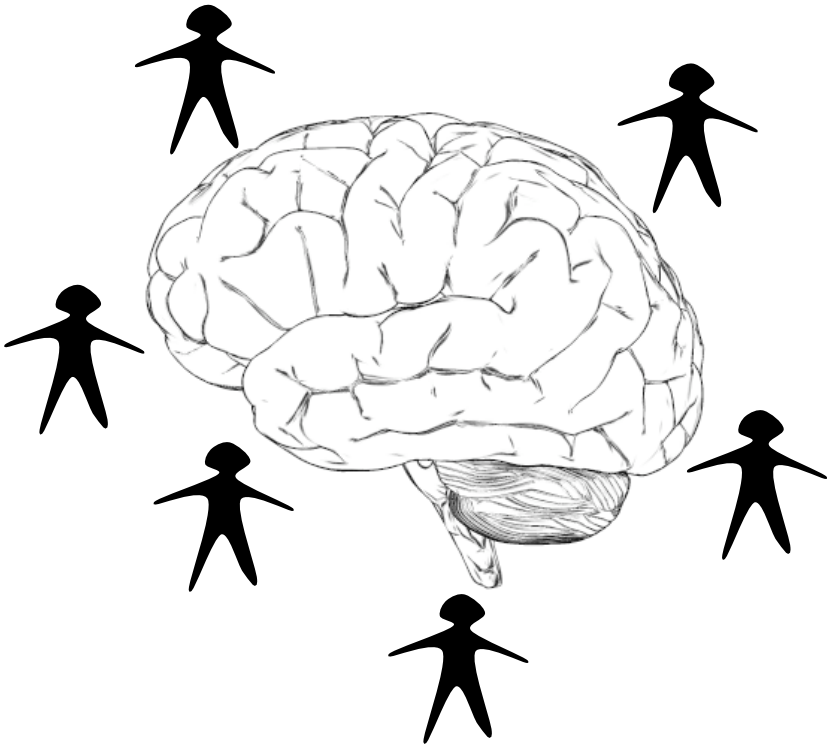
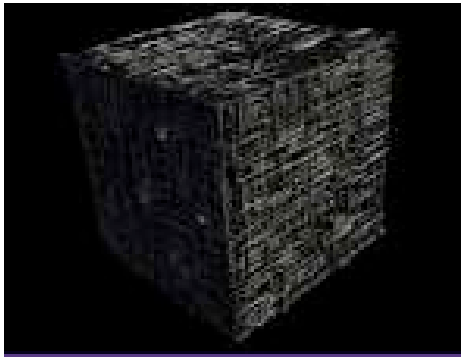


Image source: www.cs.princeton.edu/gfx/proj/sugcon/models/

ShoeBar Associates Lean-Agile Partners

Negative examples…



Borg, from Star Trek

Many-headed Hydra

"hive mind"

War room, Dr. Strangelove

Borg graphic from www.startrek-gamers.com
Hydra image from: libcom.org/library/many-headed-hydra-sailors-...
War room image from at: www.archis.org/volume/category/volume-news/

ShoeBar Associates Lean-Agile Partners

But Positive Ones too…

Cooperation, *with* individuality

Fantastic Four image from: www.jerrykatz.cc/?p=103
LOTR image from: www.ew.com/ew/article/0,,187102,00.html
Star Wars image at: www.jerrykatz.cc/?p=103

ShoeBar Associates Lean-Agile Partners

Agile “Hyper-accountability”

- Contributes enormously to safety
- Emerges when there is
  - Trust
  - Group renewal, group learning
  - Team decision-making mechanism that does not “split the difference”
  - Clear mission

Tips for Managers

- Set clear bounds for team autonomy
- Manage team membership with a light touch
- Stakeholder decisions needed rapidly
- Honest estimates expected - transparency

More Tips for Managers

- Allocate team members 100%
  - *Focus* makes a big difference!
- Clear blockages promptly
- Participate in Retrospectives - *sometimes*, but never facilitate
- Get a coach! Training is not enough

ShoeBar Associates Lean-Agile Partners

Questions?

ShoeBar Associates

Lean-Agile Partners

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

- *Software too often contributes to poor safety*
- *Iterative approach shifts the planning culture*
- *Risk management benefits from iteration*
- *Team Autonomy forces a rethink on interactions*
- **Iterations → Safer product, Happy auditors**

ShoeBar Associates Lean-Agile Partners

Objections / Advantages

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)

Key Elements?

- Collaborate / communicate with customer
- Deliver working system – early and often
- Automated testing: augment with each addition to the code
- Review hazards often as system becomes better understood
- Document, but effectively and flexibly
  - Docs as deliverables vs. as process support

Questions?

ShoeBar Associates

Lean-Agile Partners

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

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

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