MANICODE

SECURE CODING EDUCATION

Zero to DevSecOps:

Security in a DevOps World

A little background dirt…

@jimmesta

- 10 years of penetration testing, teaching, and building security programs
- OWASP AppSec California organizer and Santa Barbara chapter founder
- Conference speaker
- Been on both sides of the InfoSec fence
- Loves Clouds

Introduction to DevOps and Common Patterns

A Trip Down Memory Lane

Introduction to DevOps

Introducing Security to DevOps Environments

People, Process, and Technology

Infrastructure Security and Infrastructure as Code

Microservices and Containers

Where to Go Next

WELCOME TO DEVSECKUBEOPS
I'LL BE YOUR GUIDE
imgflip.com
HEUSER 2012

We Have a “Situation”

The Situation

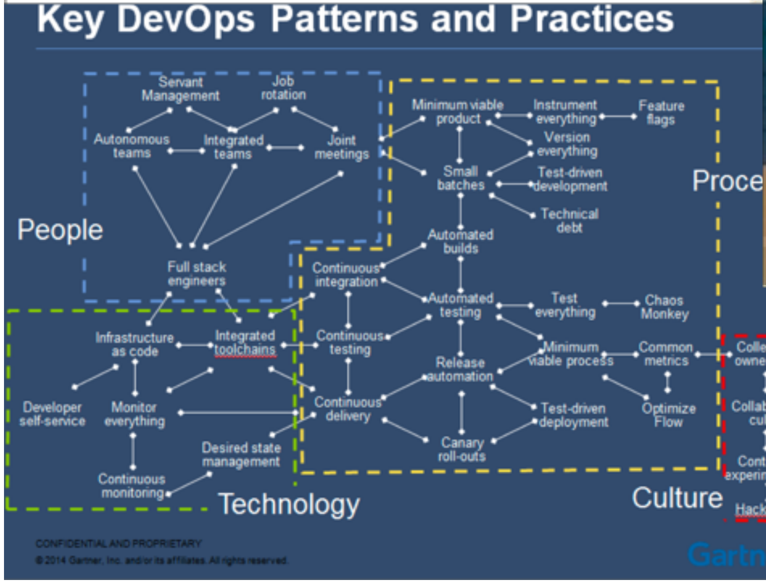
Certified DevOps

Presented to

James Betteley

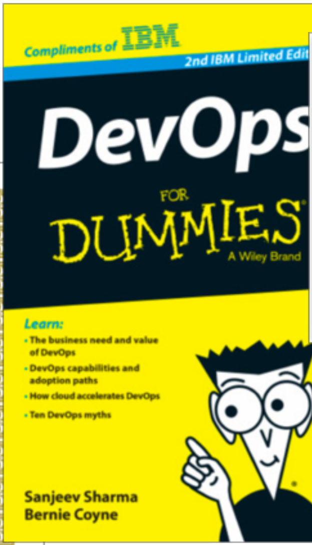
for guessing multiple choice questions reasonably well

10 March 2016



Key DevOps Patterns and Practices

CONFIDENTIAL AND PROPRIETARY
© 2014 Gartner, Inc. and/or its affiliates. All rights reserved.



Compliments of IBM

2nd IBM Limited Edit

DevOps FOR DUMMIES

A Wiley Brand

Learn:

- The business need and value of DevOps
- DevOps capabilities and adoption paths
- How cloud accelerates DevOps
- Ten DevOps myths

Sanjeev Sharma
Bernie Coyne

DevOps Borat
@DEVOPS_BORAT

Follow

In startup we are practice Outage Driven Infrastructure.

5:38 AM - 12 Mar 2013

431 RETWEETS 163 FAVORITES

Is DevOps Bullshit ?

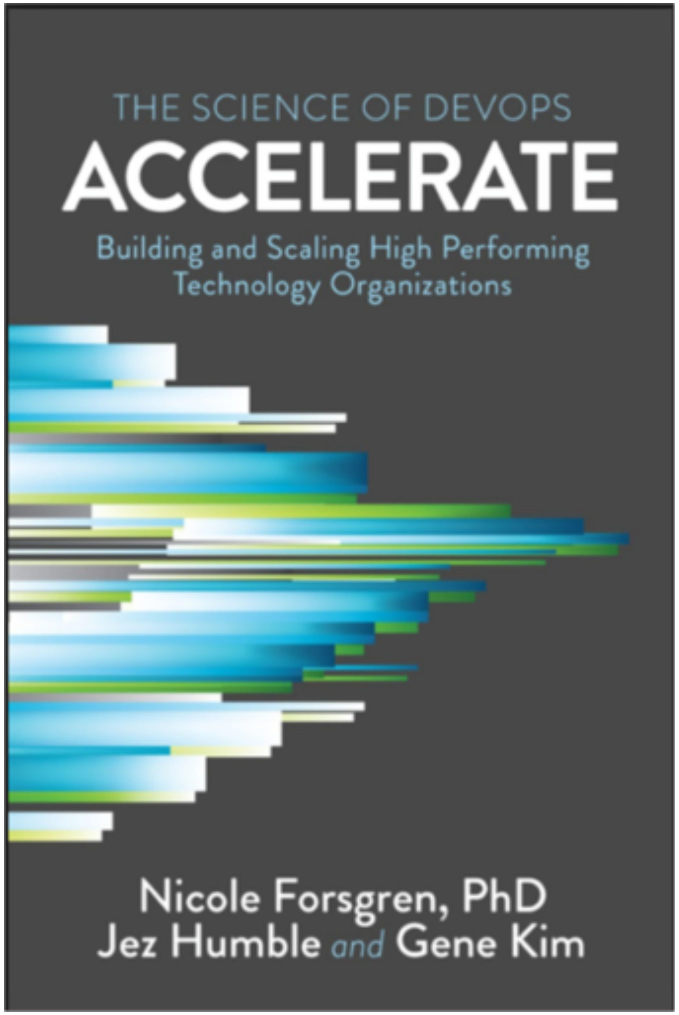
DevOps Is Bullshit: Why One Programmer Doesn't Do It Anymore

Posted on March 8, 2015

EVERYBODY IS OUT DEVOPSING
AND I'M JUST SITTING HERE SYSADMINING

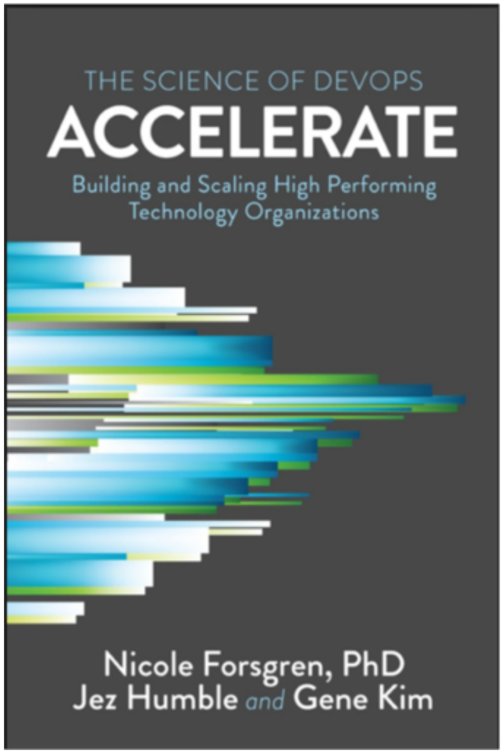
The (Actual) Current State of Affairs

“Our research has uncovered 24 key capabilities that drive improvements in software delivery performance in a statistically significant way.”



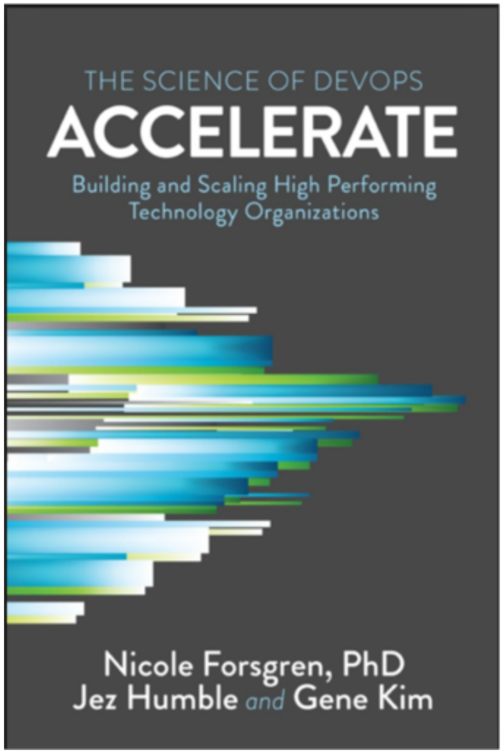
Continuous Delivery Capabilities

- Version Control
- Deployment Automation
- Continuous Integration
- Trunk-Based Development
- Test Automation
- Test Data Management
- ***Shift Left on Security***
- Continuous Delivery



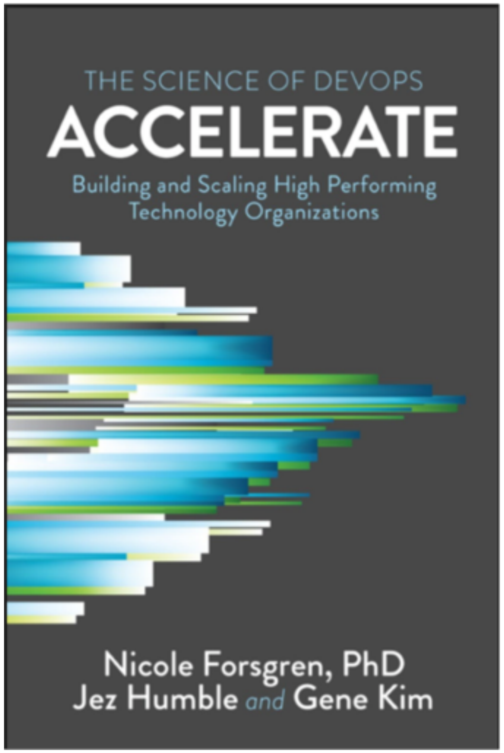
Architecture Capabilities

- Loosely Coupled Architecture
- Empowered Teams
- Customer Feedback
- Working in Small Batches
- Team Experimentation



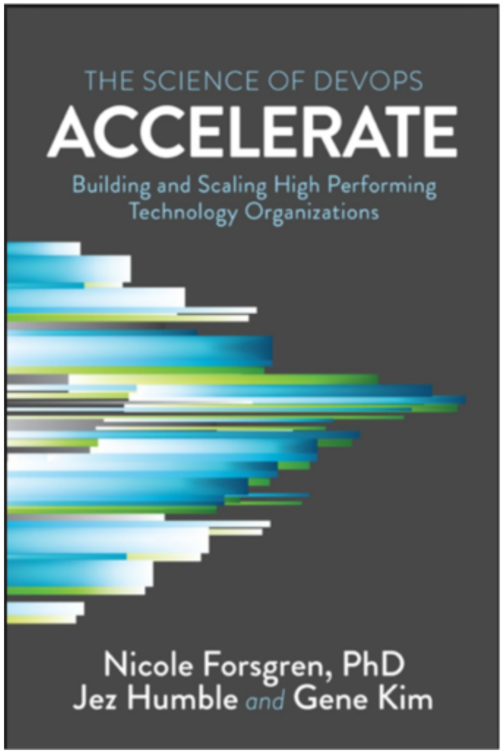
Lean Management and Monitoring Capabilities

- Change Approval Process
- Monitoring
- Proactive Notification
- WIP Limits
- Visualizing Work



Cultural Capabilities

- Supporting Learning
- Collaboration Among Teams
- Job Satisfaction
- Transformational Leadership



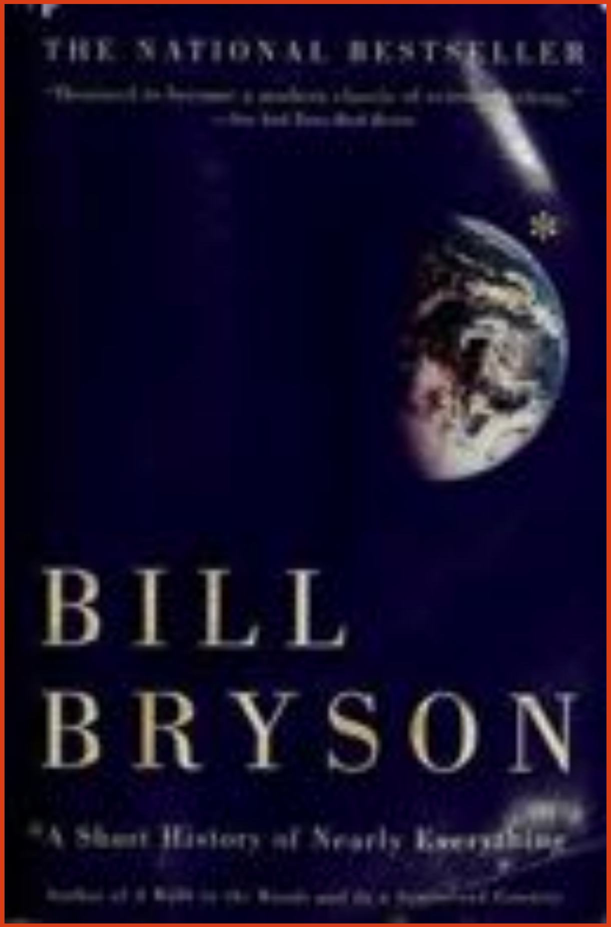
High Performers vs. Low Performers

- 46x more frequent code deployments
- 440x faster lead time from commit to deploy
- 170x faster mean time to recover from downtime
- 5x lower change failure rate

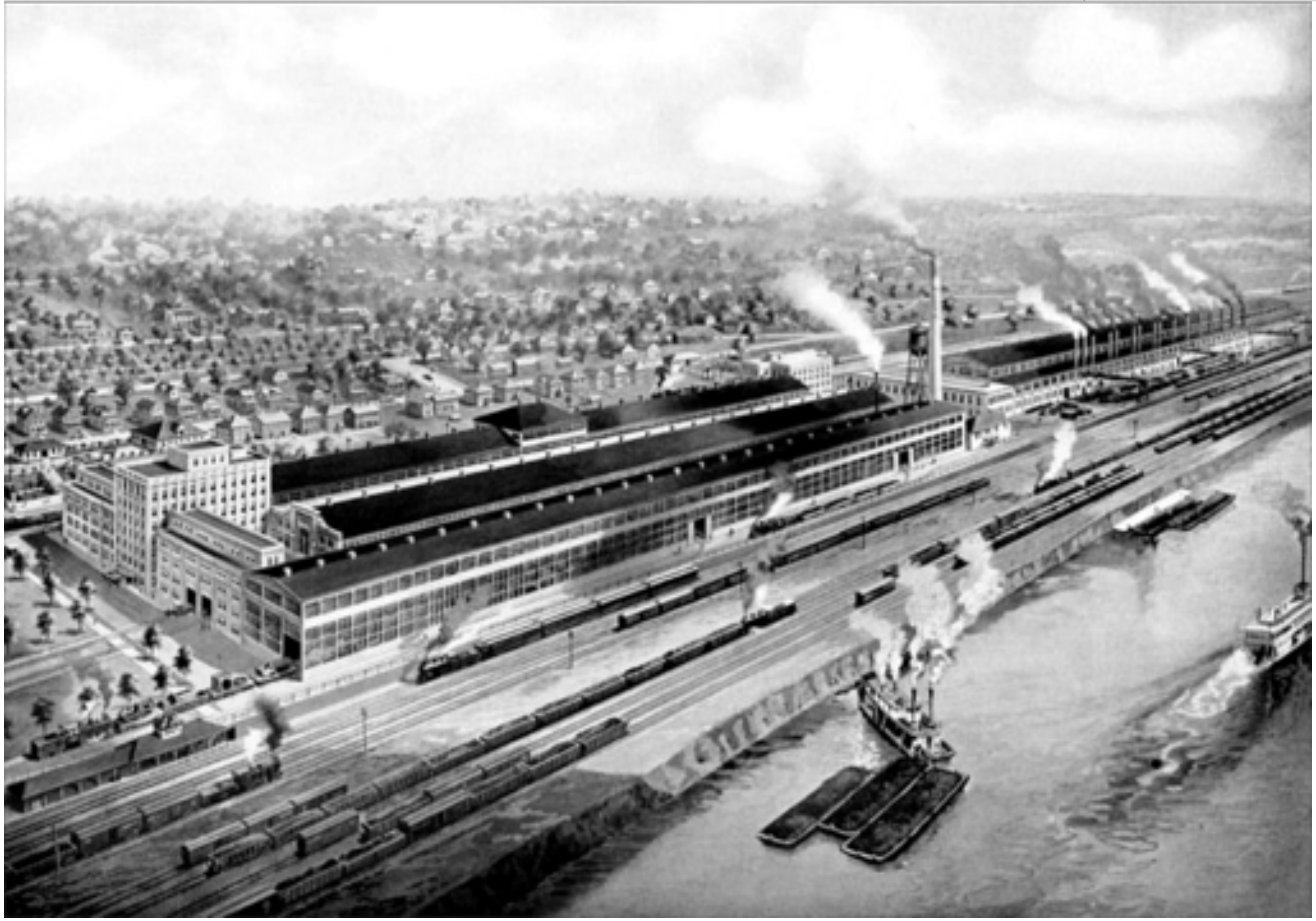
High Performing Security Teams

“High-performing teams were more likely to incorporate information security into the delivery process. Their infosec personnel provided feedback at every step of the software delivery lifecycle, from design through demos to helping out with test automation. However, **they did so in a way that did not slow down the development process**…”

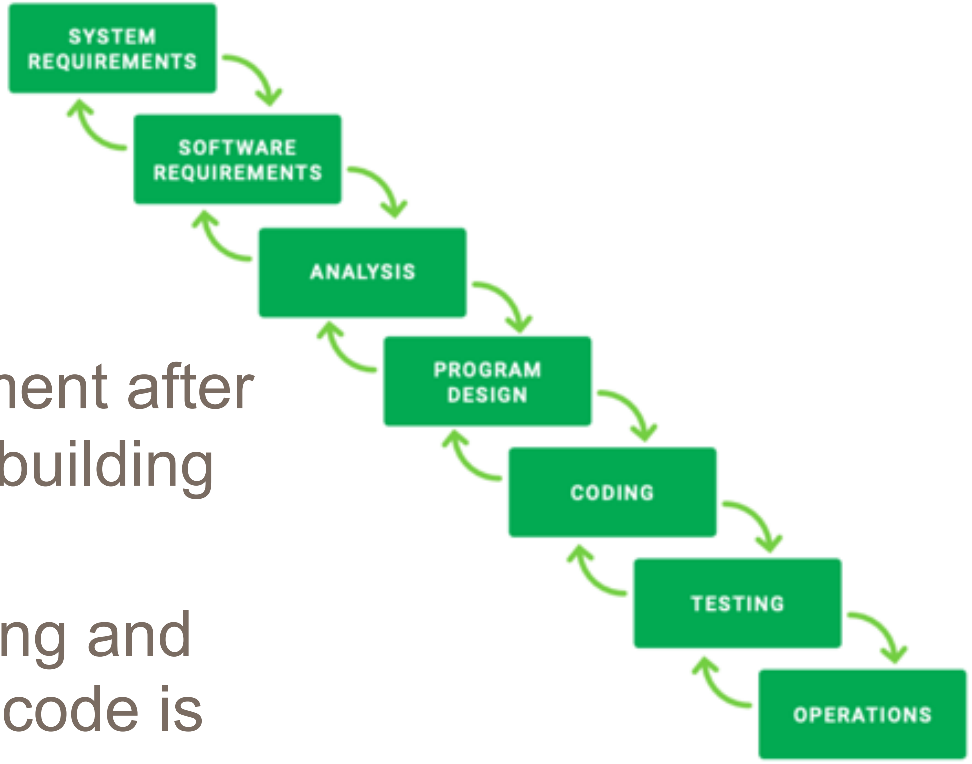
A Brief History of the SDLC



Part 1: The Waterfall Era



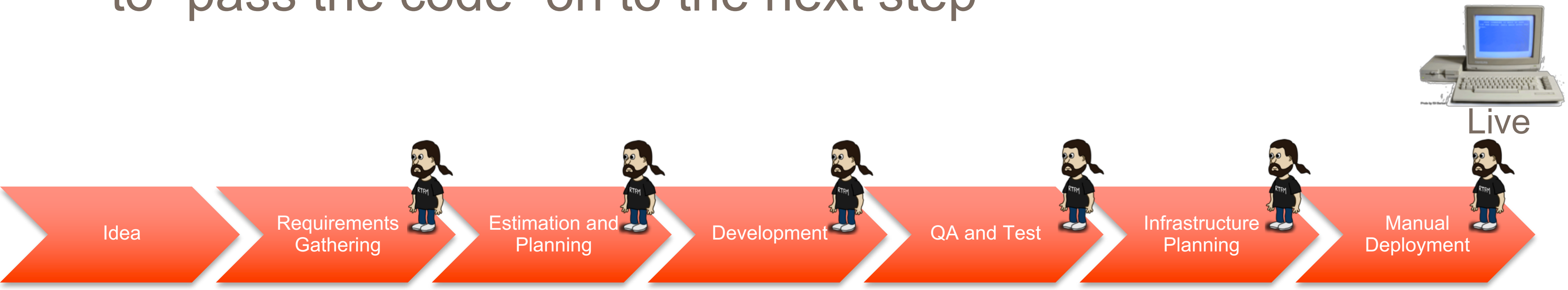
Part 1: The Waterfall Era



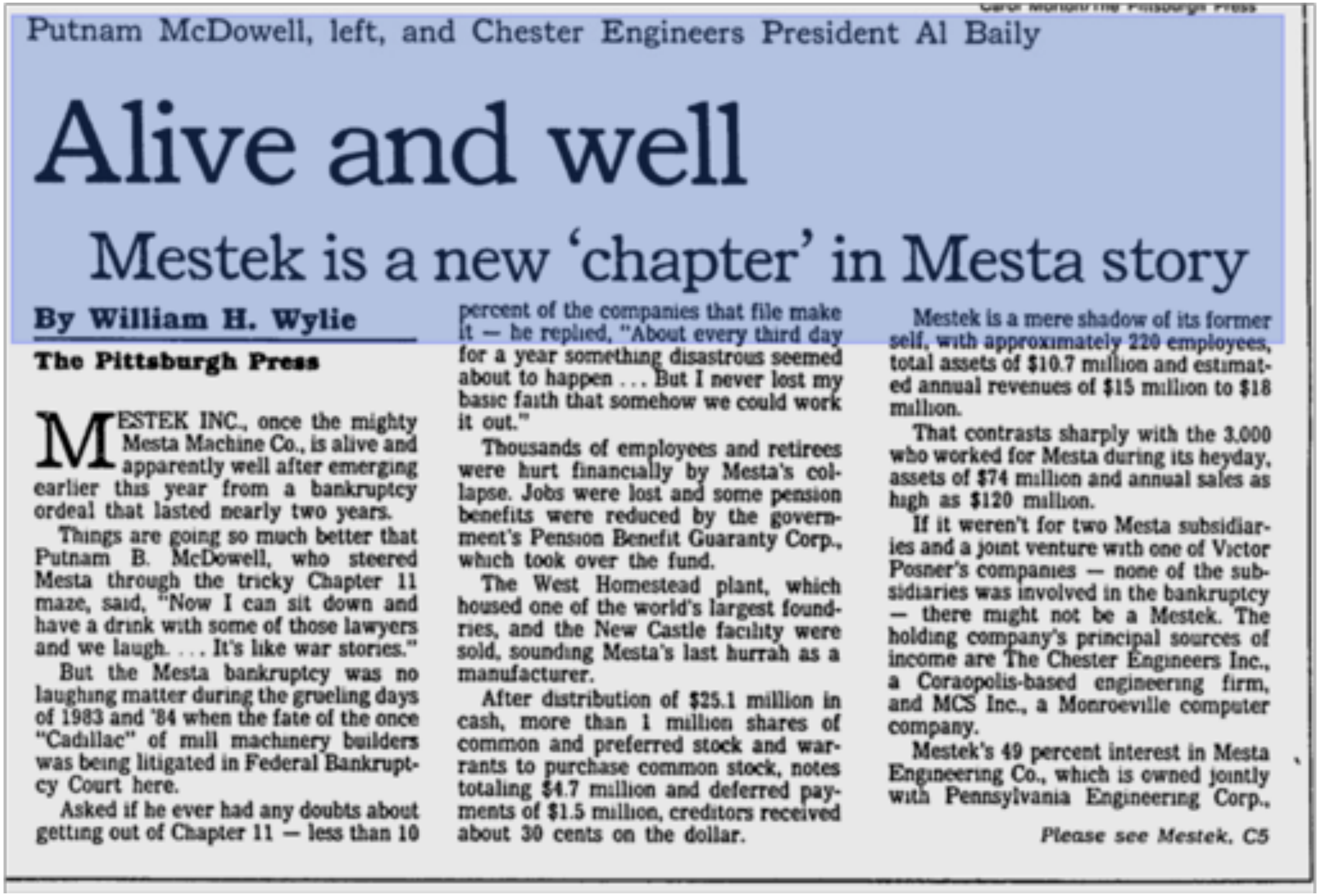
- Modeled software development after what we knew and learned building hardware
- Months (or years!) of planning and preparation before a line of code is written
- All good stories have to start *somewhere*

Traditional SDLC AKA "Waterfall"

- **Optimizes for risk management.** Assuming the cost of a mistake is high and tolerance for risk is low
- Critical services still benefit from certain "waterfall" methodologies
- Linear progression when deploying software
- Relies heavily on human intervention and interaction to "pass the code" on to the next step



Part 2: The Agile Enlightenment



Carol [illegible]/The Pittsburgh Press

Putnam McDowell, left, and Chester Engineers President Al Baily

Alive and well

Mestek is a new 'chapter' in Mesta story

By William H. Wylie

The Pittsburgh Press

MESTEK INC., once the mighty Mesta Machine Co., is alive and apparently well after emerging earlier this year from a bankruptcy ordeal that lasted nearly two years.

Things are going so much better that Putnam B. McDowell, who steered Mesta through the tricky Chapter 11 maze, said, "Now I can sit down and have a drink with some of those lawyers and we laugh. . . . It's like war stories."

But the Mesta bankruptcy was no laughing matter during the grueling days of 1983 and '84 when the fate of the once "Cadillac" of mill machinery builders was being litigated in Federal Bankruptcy Court here.

Asked if he ever had any doubts about getting out of Chapter 11 — less than 10 percent of the companies that file make it — he replied, "About every third day for a year something disastrous seemed about to happen . . . But I never lost my basic faith that somehow we could work it out."

Thousands of employees and retirees were hurt financially by Mesta's collapse. Jobs were lost and some pension benefits were reduced by the government's Pension Benefit Guaranty Corp., which took over the fund.

The West Homestead plant, which housed one of the world's largest foundries, and the New Castle facility were sold, sounding Mesta's last hurrah as a manufacturer.

After distribution of $25.1 million in cash, more than 1 million shares of common and preferred stock and warrants to purchase common stock, notes totaling $4.7 million and deferred payments of $1.5 million, creditors received about 30 cents on the dollar.

Mestek is a mere shadow of its former self, with approximately 220 employees, total assets of $10.7 million and estimated annual revenues of $15 million to $18 million.

That contrasts sharply with the 3,000 who worked for Mesta during its heyday, assets of $74 million and annual sales as high as $120 million.

If it weren't for two Mesta subsidiaries and a joint venture with one of Victor Posner's companies — none of the subsidiaries was involved in the bankruptcy — there might not be a Mestek. The holding company's principal sources of income are The Chester Engineers Inc., a Coraopolis-based engineering firm, and MCS Inc., a Monroeville computer company.

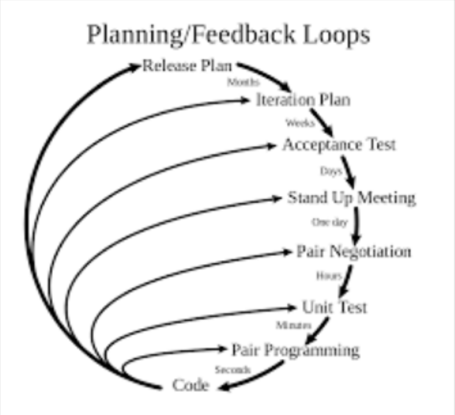
Mestek's 49 percent interest in Mesta Engineering Co., which is owned jointly with Pennsylvania Engineering Corp.,

Please see Mestek, C5

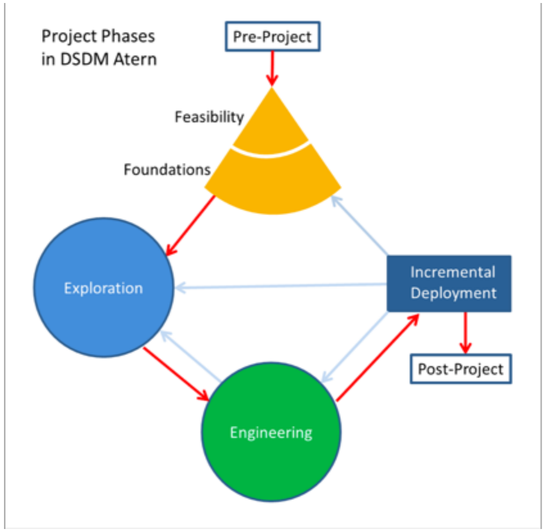
Part 2: The Agile Enlightenment

- Realization that software differs from hardware
- Competition emerges and first-to-market matters
- 90’s was all about experimentations in effective software deployment
- Sprints, daily standups, retrospectives emerge
- Manual testing, QA, and deployment

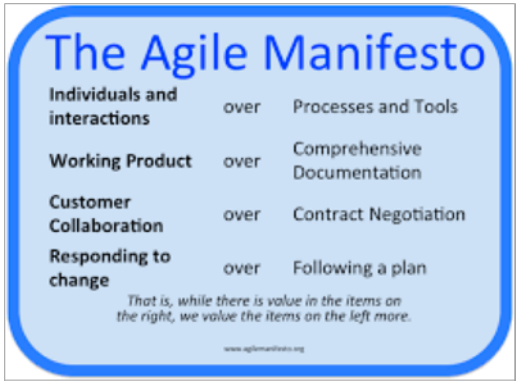
Part 2: The Agile Enlightenment



Extreme Programming



Dynamic Systems Development Method

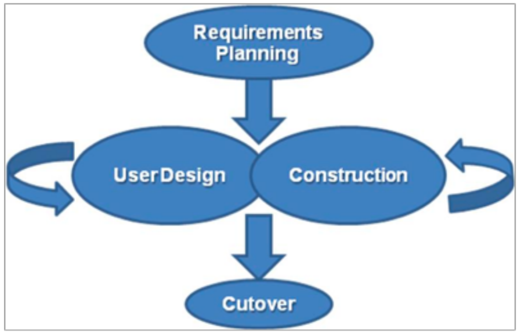


The Agile Manifesto

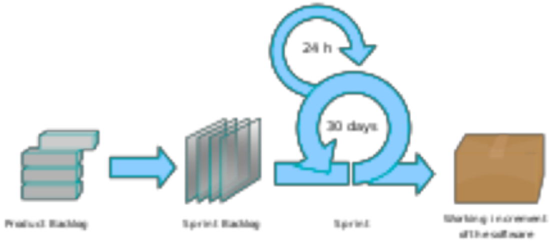
Individuals and interactions	over	Processes and Tools
Working Product	over	Comprehensive Documentation
Customer Collaboration	over	Contract Negotiation
Responding to change	over	Following a plan

That is, while there is value in the items on the right, we value the items on the left more.

www.agilemanifesto.org



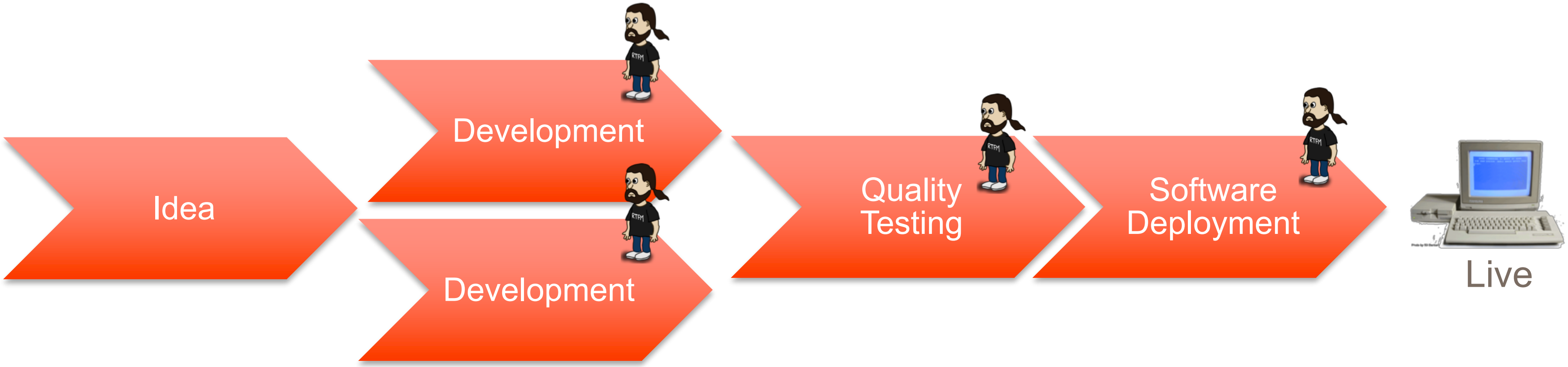
Rapid Application Development (RAD) Model



Scrum

Agile / Scrum / Extreme

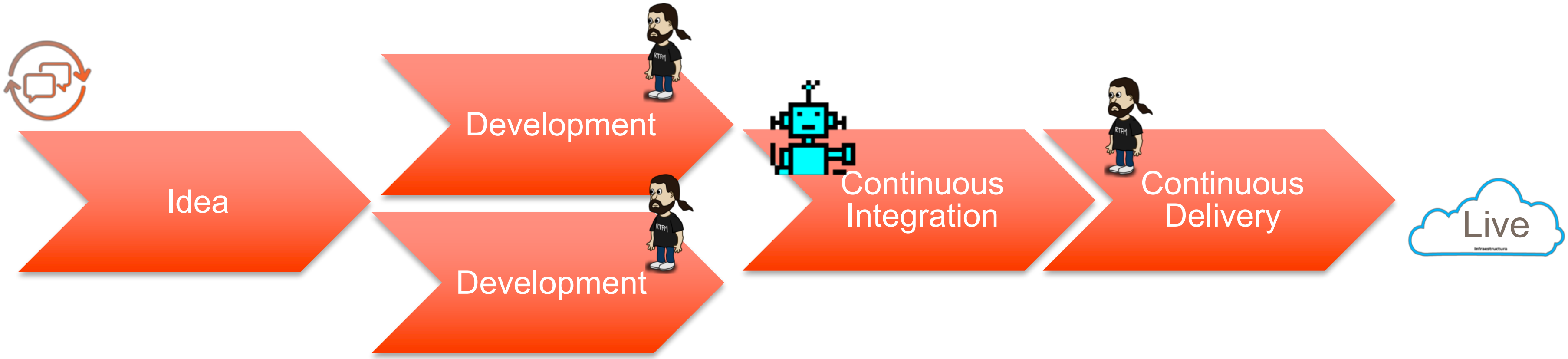
- Begin optimizing for speed and agility
- **Incremental changes**
- Beginning of TDD, timeboxing, stories, pair-programming, etc.
- We begin *thinking* about and measuring the effectiveness of our SDLC



Part 3: Invasion of the Robots

Continuous Integration and Delivery

- Optimizes for speed and agility. Assuming the cost of a mistake is low and tolerance for risk is high
- Parallel and incremental changes
- Automation and upfront work makes this possible
- **Self-testing code and early days of automated QA**

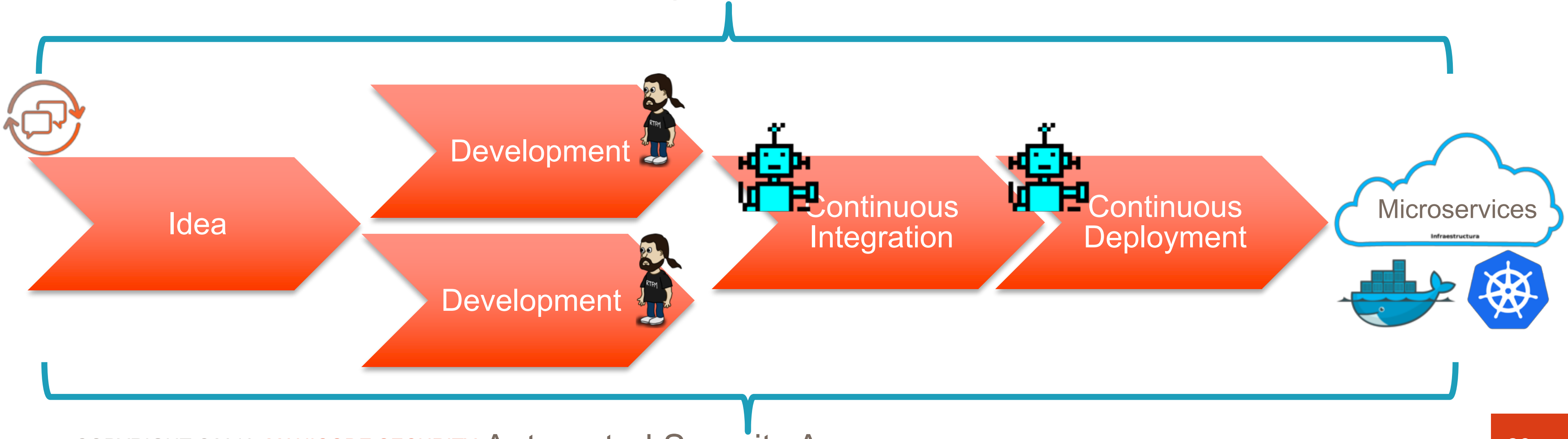


Part 4: The Current State of Affairs

DevSecOps

- Cultural shift towards end-to-end ownership of code
- Zero-downtime, automated deployments
- Emergence of containers, serverless, and zero-downtime deployments
- ”Everything-as-Code” is the new standard
- **Security is no longer a blocker or silo**

Dev + Ops Collaboration



Idea

Development

Development

Continuous Integration

Continuous Deployment

Microservices

Infraestructura

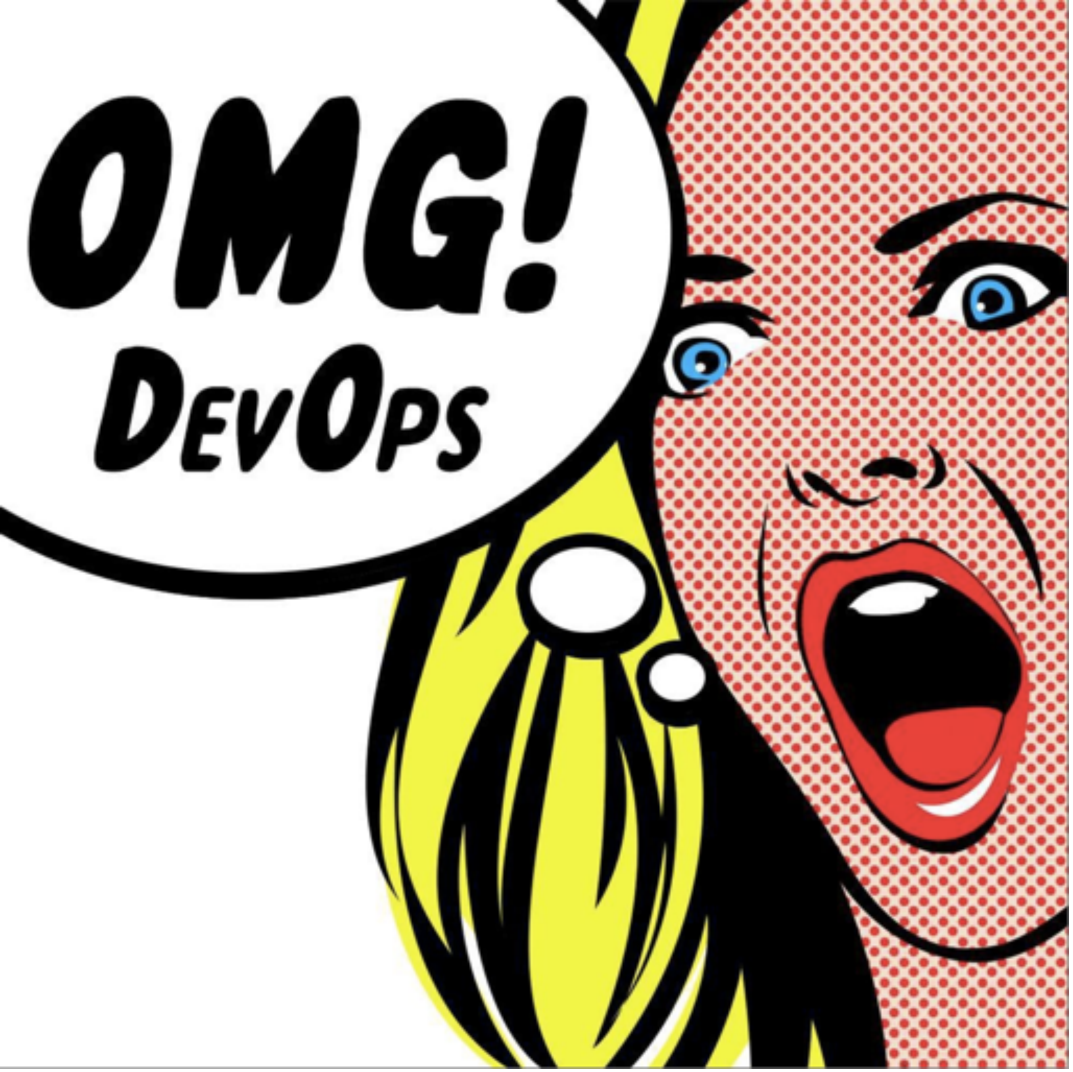
Automated Security Awesomeness

DevSecOps Advantages

- Add customer value
- Puts security in everyone’s job description
- Eliminate “black box” security teams and tools
- Ability to measure security effectiveness
- Reduce attack surface and vulnerabilities
- Increase recovery speed
- Save $$$
- Secure by default mentality

The Rest is History…

Introduction to DevOps



What *is* DevOps?