SE2832

Lecture Objectives:

Introduction to Software Verification

Dr. Walter Schilling, Instructor

About the instructor

- **Instructor:** Dr. Walter W. Schilling, Jr.
- **Office:** Walter Schroeder Library 335
- **Office Hours:**
  - While I post office hours, I keep an open door policy. If I am in my office and the door is open, please feel free to stop in.
- **Telephone:** 414 277 7370
- **E-mail:** schilling@msoe.edu
  - Best method to contact me during non-class days
  - Please prefix subject with SE2832.
- **Course Web Page:**
  - http://www.walterschilling.us/msoe/spring20132014se2832/spring20132014se2832.php

About the Instructor (Continued)

- Ohio Northern University graduate in Electrical Engineering
  - Computer Science Minor
- Masters and PhD. from University of Toledo
  - Specialized in Computer Systems Design and Software Reliability
- Worked in Automotive Industry for approximately 6 years
  - Audio Software Engineer – Embedded Systems Design
    - US Patent 6,707,768
    - "Randomized Playback of Tracks in a Multimedia Player"
- Personal Website: http://www.walterschilling.org

Catalog Description

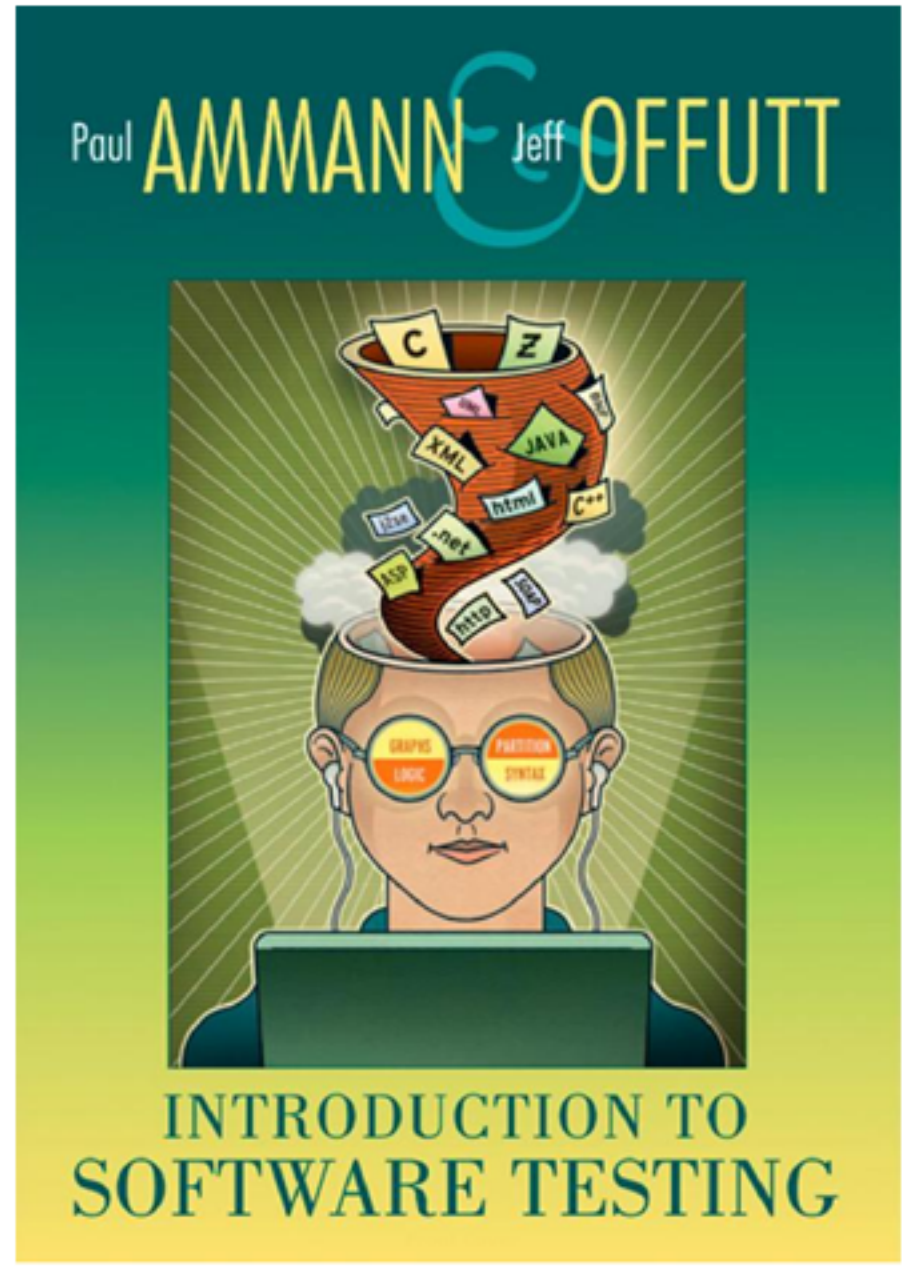
- This course introduces students to the fundamental concepts of software verification. Topics covered include the activities within testing, coverage criteria, basic testing techniques and types, basic testability metrics, and the application of testing tools. Laboratory assignments provide extensive opportunities to apply software verification techniques and tools. (prereq: MA 2310, CS 2852)

Prerequisites

- MA 2310 Discrete Math
- CS 2852 Data Structures

Textbook

- Introduction to Software Testing Paul Ammann (Author), Jeff Offutt (Author)
- Publisher: Cambridge University Press; 1 edition (January 28, 2008)
- Language: English
- ISBN-10: 0324004303
- ISBN-13: 978-0521880381
- ASIN: 0521880386



Class Materials

- Textbook(s)
- Calculator

Grading

General Notes

- **Assignment Due Dates**
  - Late Penalty — Don't Be late!
    - 10% per business day late penalty for all written work
    - No work will be accepted more than 5 business days late for credit.
  - Early Bonus + Be early
    - Early submission bonus will be available for all lab assignments.
    - 10% bonus for lab assignments submitted 48 hours or more in advance of the due date
    - 5% for lab assignments submitted 24 hours or more in advance of due date.

Grading Challenges

- Any grading challenges, unless specifically noted by the professor, shall be submitted in writing within 5 days of the assignment being returned to the student.
- Challenge must clearly delineate the problem with the assignment grade as well as justify the need for the grade change.

Student Integrity

- All students are expected to abide by MSOE's policy on student integrity. If at any point in the semester you have a question about an assignment, please come discuss it with me.
- Violations of this policy will be dealt with seriously, and may result in significant penalty, up to and including failure of the course.

Lecture Notes / Handouts

- Lecture notes will be available online in the ubiquitous presenter system
  - http://up.ucsd.edu/
  - You will need to subscribe to the course
  - You may also follow along with the lecture online
- Non slide lecture material and handouts may be made available on the website.
  - These are for your own personal usage and are not to be circulated outside of the MSOE domain.
- Lecture notes and handouts are subject to copyright law.

Piazza Discussion Board

- There is a discussion board for this class on the service Piazza
  - Usage of this board is purely optional
  - Questions may be answered faster there than via e-mail

Course Coverage

- See Syllabus

Introduction to Software Failure

Lecture Objectives:

1) Explain the Relationship between the cost of fixing a defect and the phase in which the defect is discovered
2) Justify the importance of software testing from an economic standpoint
3) Explain through case studies the root cause of one or more software failures

Introductory Quote

"The most significant problem facing the data processing business today is the software problem that is manifested in two major complaints: software is too expensive and software is unreliable."

-Glenford J. Myers: **Software Reliability: Principles and Practices,** 1976.

A second quote

- ***"...well over half of the time you spend working on a project (on the order of 70 percent) is spent thinking, and no tool, no matter how advanced, can think for you. Consequently, even if a tool did everything except the thinking for you -- if it wrote 100 percent of the code, wrote 100 percent of the documentation, did 100 percent of the testing, burned the CD-ROMs, put them in boxes, and mailed them to your customers -- the best you could hope for would be a 30 percent improvement in productivity. In order to do better than that, you have to change the way you think."***

- *Frederick P. Brooks - [paraphrased], http://www.javaworld.com/javaworld/jw-07-1999/jw-07-toolbox.html*

Introduction – Impact of Failure

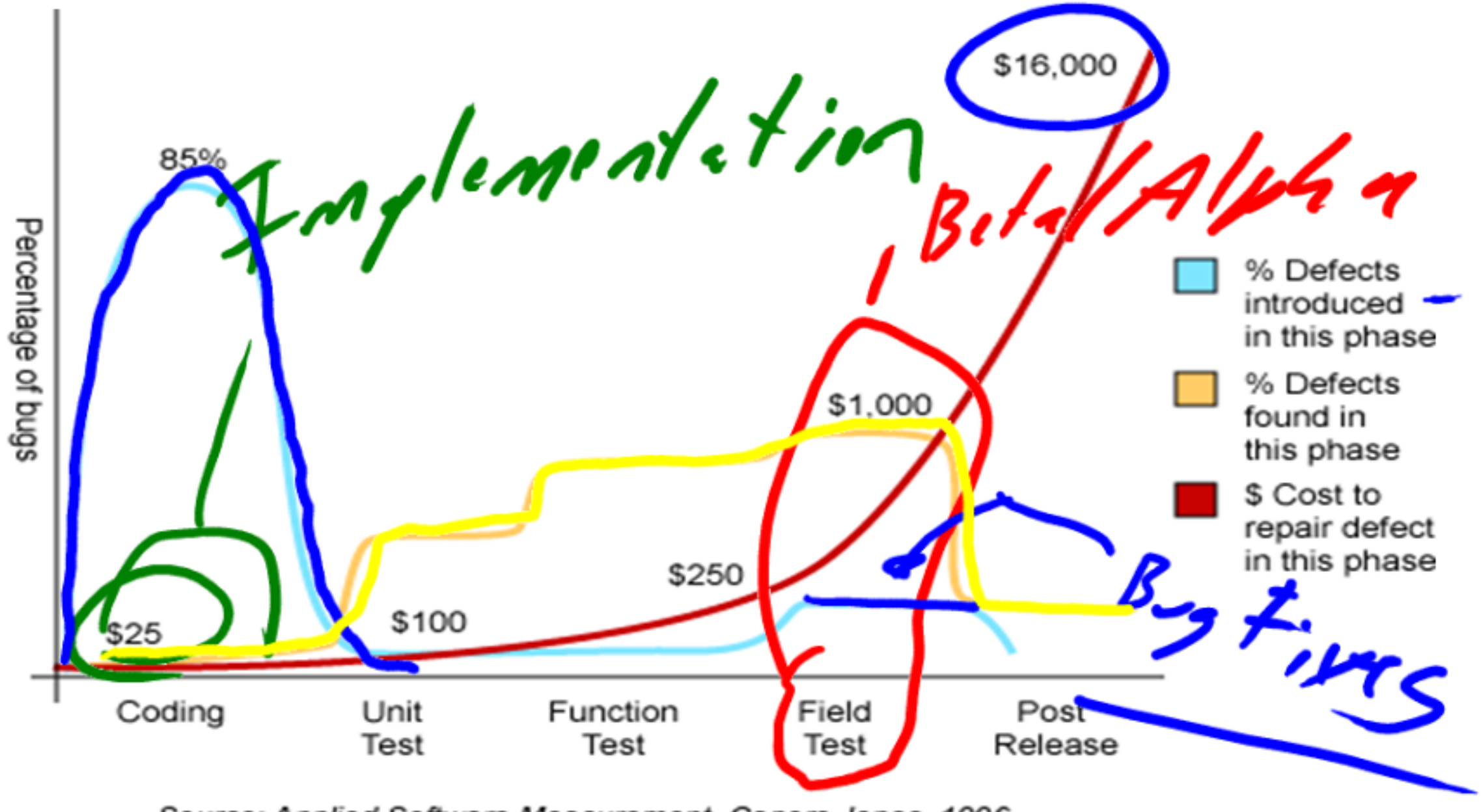
- Large economic impact to software failure
  - $59.5 billion annual cost to economy.
- Fiscal year 2003 DOD spent $21 billion on software development
  - $8 billion (40%) spent to fix reliability problems in software

NIST Survey

Software Failure is expensive!

MSOE

Field Failures are Very expensive!



Source: Applied Software Measurement, Capers Jones, 1996

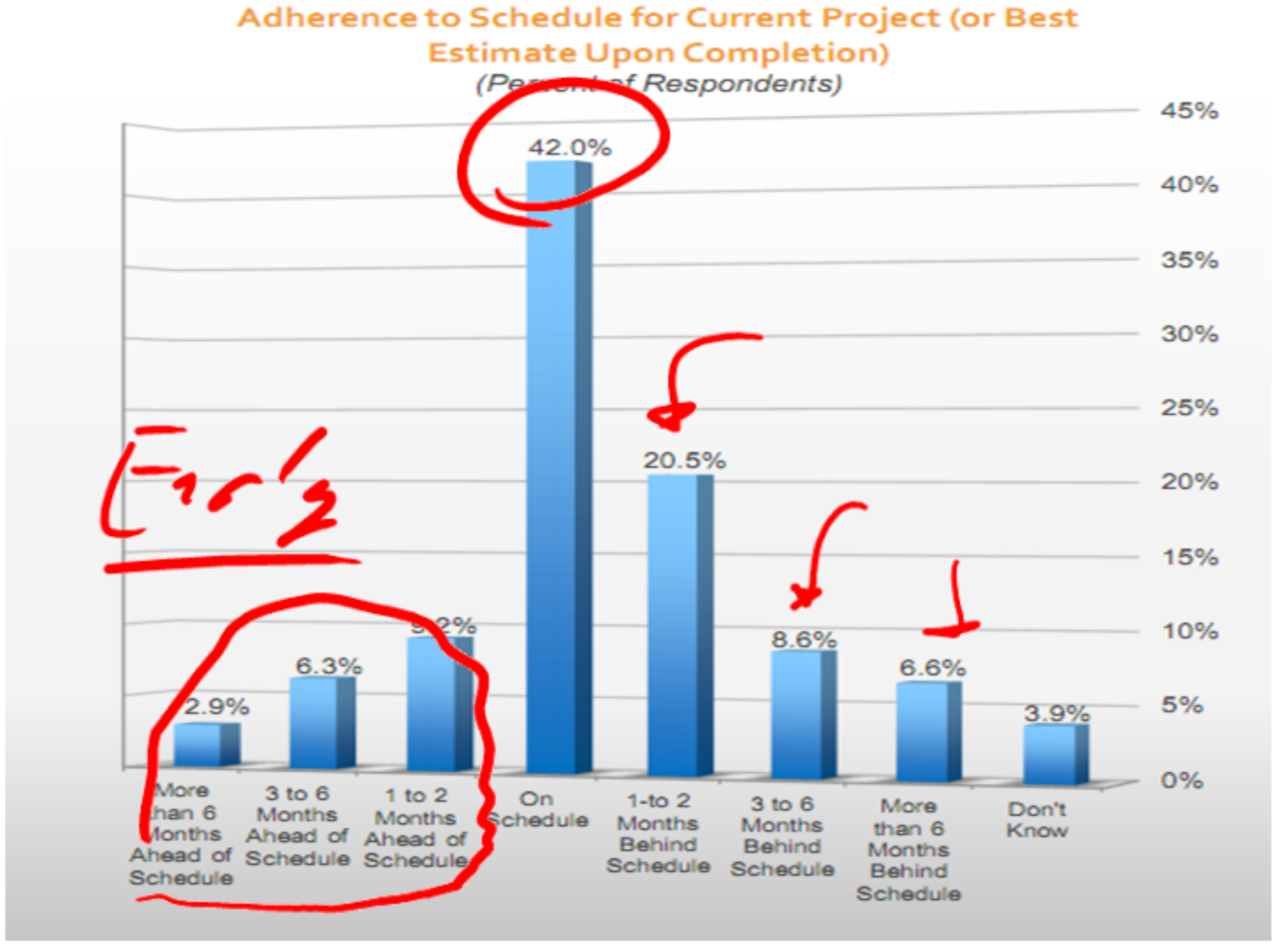
- Avionics
  - 39% of FAA Air-worthiness directives related to software
- Medical Industry
  - 79% of medical device recalls can be attributed to software
    - 41% of pacemaker recalls 1990-2000 related to software
- Automotive Industry
  - Single software failure resulted in recall of 2.2 million cars and $20 million cost.
- Consumer electronics
  - Software has become the principle source for reliability problems
- Overall
  - Software driven outages exceed hardware by a factor 10.

The Crisis in Software

- Software is done when its done
  - Only 29% of **ALL** projects succeed
  - 18% fail outright
  - 53% were challenged
    - Cost overruns
    - Late
    - Fewer than desired features
- And this is considered a huge improvement since 1994
  - 16% succeed, 31% fail, and 53% were challenged
- Management is at best an "Art Form"
  - Skills and Techniques are relatively new
  - It just isn't done

Chaos Report: http://www.standishgroup.com/sample_research/

On time shipment of products



Select Findings: Embedded Engineering Survey, 2011

Windows

A fatal exception 0E has occurred at 0137:BFFA21C9. The current application will be terminated.

* Press any key to terminate the current application.
* Press CTRL+ALT+DEL again to restart your computer. You will lose any unsaved information in all applications.

Press any key to continue _

Failures your have been exposed to?

Red King of Death - XBox

msoft Mail server

HealthCare.gov

MSOE

Zune 30 Software Failure

December 31, 2008

```
while (days > 365)
{
    if (IsLeapYear(year))
    {
        if (days > 366)
        {
            days -= 366;
            year += 1;
        }
    }
    else
    {
        days -= 365;
        year += 1;
    }
}
```

```
while (days > 365)
{
   if (IsLeapYear(year))
   {
      if (days > 366)
      {
         days -= 366;
         year += 1;
      }
   }
   else
   {
      days -= 365;
      year += 1;
   }
}
```

```
while (days > 365)
{
   if (IsLeapYear(year))
   {
      if (days > 366)
      {
         days -= 366;
         year += 1;
      }
   }
   else
   {
      days -= 365;
      year += 1;
   }
}
```

Healthcare.gov

BITWISE | DECODING THE TECH WORLD. | OCT. 8 2013 10:49 AM

Err Engine Down

What really went wrong with healthcare.gov?

By David Auerbach

1.8k 285 153

Photo by Karen Bleier

HealthCare.gov

Learn | Get Insurance

Individuals & Families | Small Businesses | All Topics

The System is down at the mo

We're working to resolve the issue as soon as possible. Please try a

Please include the reference ID below if you wish to contact us at 1-800-318-259

Error from: https%3A//www.healthcare.gov/marketplace/global/en_US/registration%.

Reference ID: 0.cdd73b17.1380636213.edae7e9

Health Insurance Marketplace

181 DAYS LEFT TO ENROLL

OCT 1 Open Enrollment Began

JAN 1 Coverage Can Begin

MAR 31 Open Enrollment Closes

MSOE

Forensic Searches

Software Designer Reports Error in Anthony Trial

Pool photo by Red Huber

Casey Anthony walking out of the Orange County Jail in Orlando, Fla., on Sunday with her lawyer Jose Baez, left.

By LIZETTE ALVAREZ
Published: July 18, 2011

MIAMI — Assertions by the prosecution that Casey Anthony conducted extensive computer searches on the word "chloroform" were based on inaccurate data, a software designer who testified at the trial said Monday.

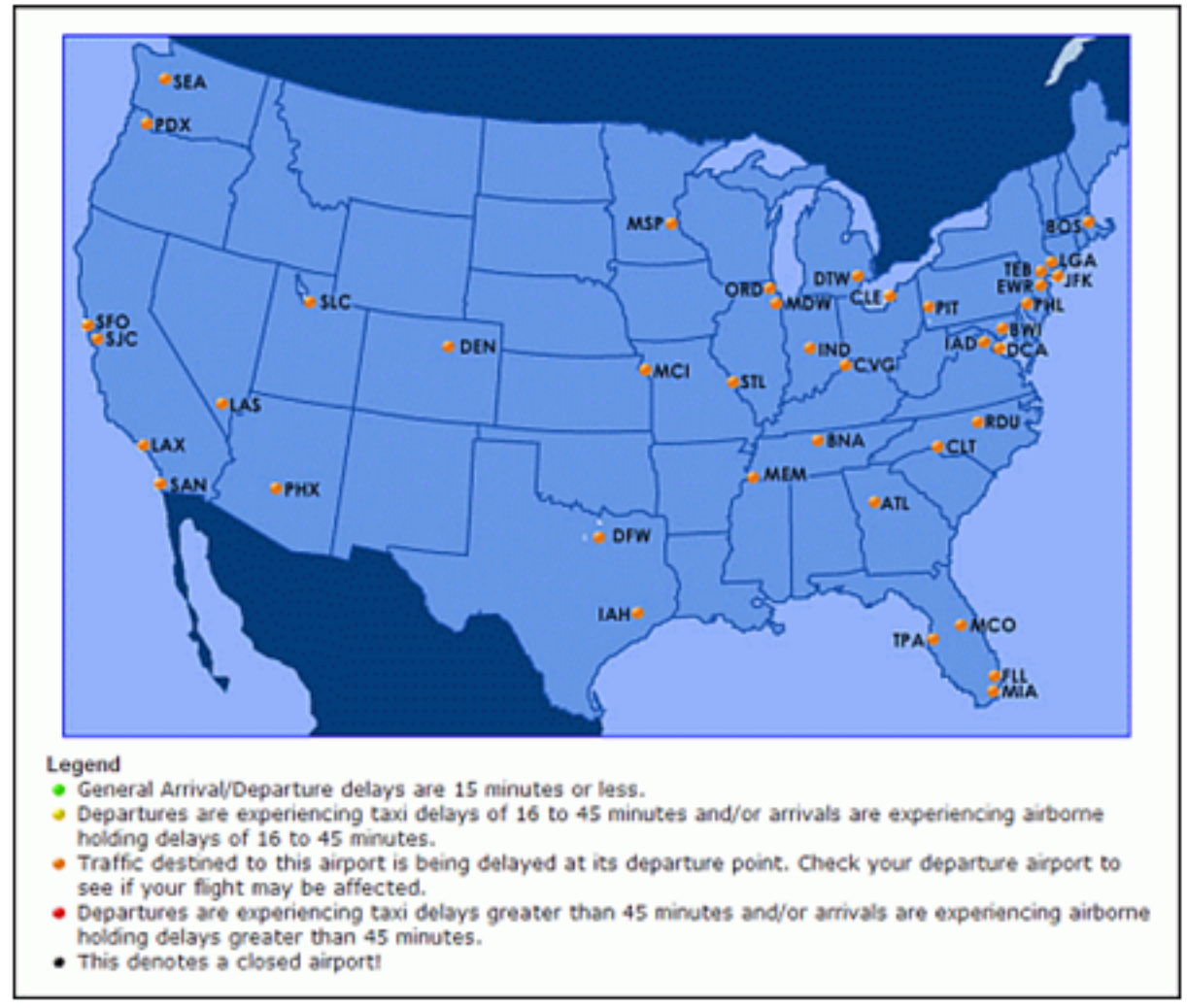
Related

The designer, John Bradley, said Ms. Anthony had visited what the

RECOMMEND
TWITTER
COMMENTS (181)
SIGN IN TO E-MAIL
PRINT

Air Traffic Control -> August 28, 2008

- A corrupt file wasn't caught by validation?
- 2 1/2 hours to restart after the failure?
- The "backup" computer couldn't handle the failover load?
- The restored-to-service computer couldn't clear the accumulated backlog until new transactions were suppressed?

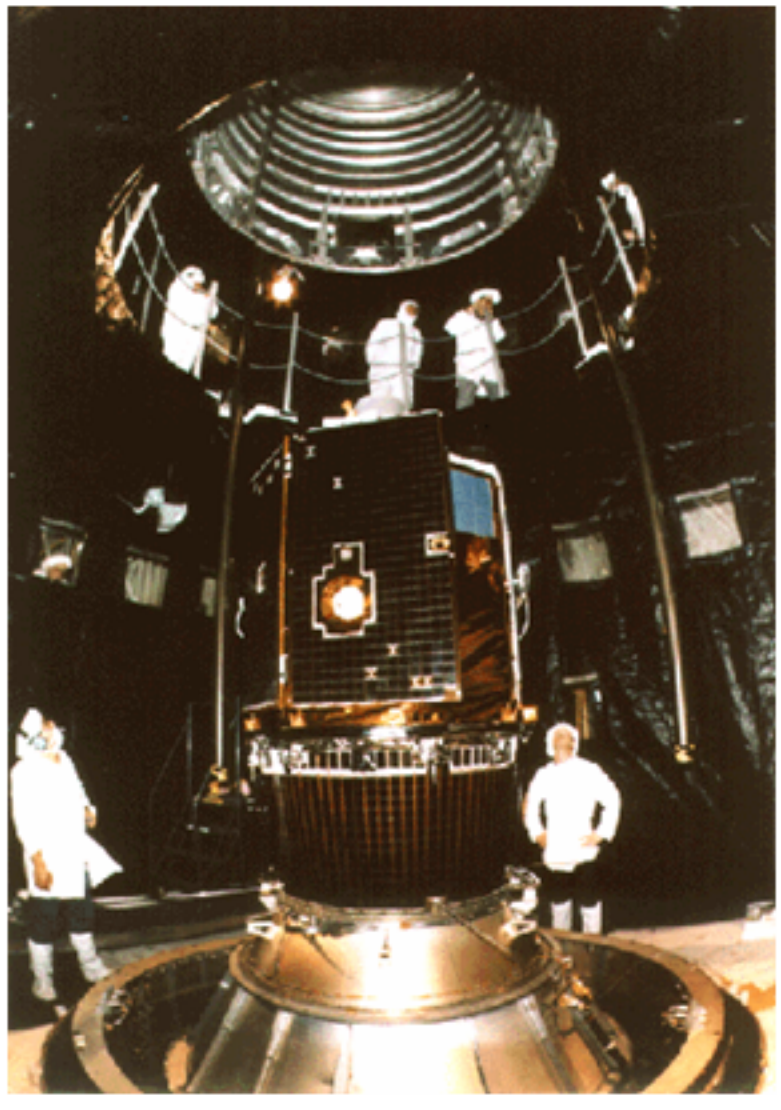


Southern California Air Traffic Control Communications Failure

September 14, 2004

- Communications lost with 400 airplanes in southwest US.
  - Planes visible on radar
  - no voice communications existed.
- Cause(s)
  - Design flaw in application and Windows Server 2000 API caused lockup after 49.7 days continuous operation
  - Failure of technician to reboot system on monthly basis.
  - Backup system incapable of handling demand

Clementine Mission Failure



- Prototype for "Faster, Better, Cheaper" operation.
  - Scientific objectives were secondary
- Many problems occurred during mission.
  - Over 3000 floating point exceptions during mission.
  - Hardware reset required at least 16 times.

- Mission failed May 7, 1994
  - exception occurred. with a thruster stuck on
  - Burned up all fuel and imparted 80 RPM rotation
- Watchdog safety feature of microcontroller not used.

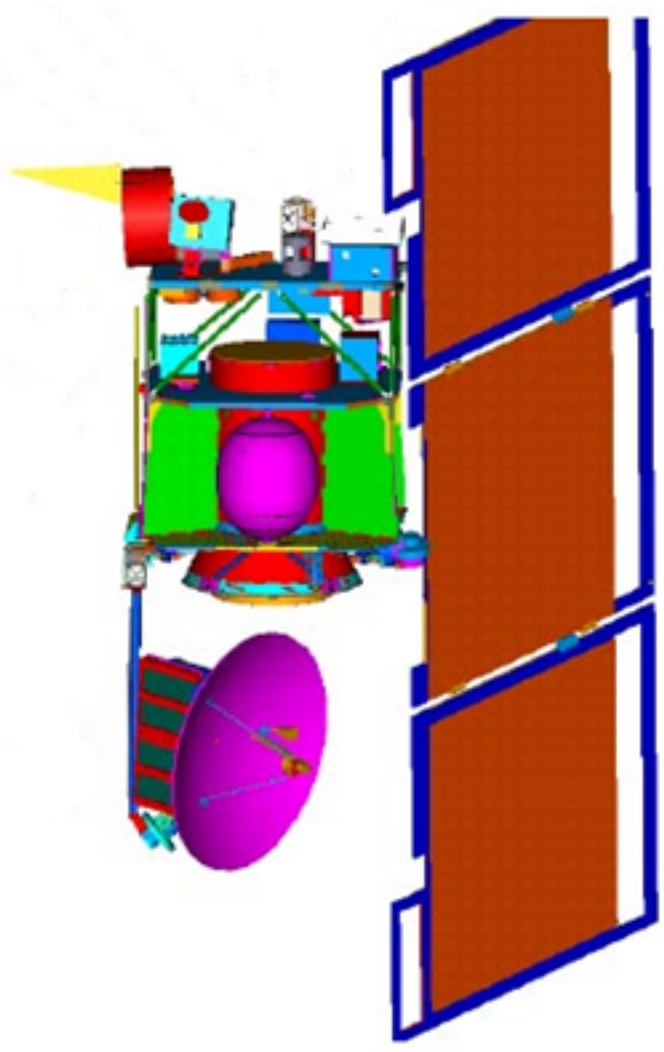
Ariane 5 June 4th, 1996

- Total failure of the Ariane 5 launcher maiden flight
- Caused by a typecast from a 64 bit floating point number to a 16 bit int
  - No exception handler associated with the conversion
- Backup system was identical in all regards
  - 37ms later, backup system failed.
- Software Developed in Ada.
  - Had code been developed in C, problem most likely would not have occurred.

Milstar Launch Failure
April 30, 1999

- ***$433.1 million Titan IV rocket launched from Cape Canaveral with third Milstar Satellite.***
- ***Launch failed***
  - Satellite did not reach necessary geostationary orbit
- ***Why?***
  - ***Table entry of -0.1992476 instead of –1.992476***

Mars Climate Orbiter Failure



- Mars Climate Orbiter Lost
- Causes [Slm+99]
  - Thruster used English units.
  - Model used metric units.

Sea Launch F-1 Satellite Launch Failure

- March 12, 2000
- Zenit-3SL lost with $200 million ICO Global Communications satellite 8 minutes into mission
- Root cause of failure: logic incorrectly changed Resulted in Helium valve not being closed

Original Source Code	`If ((state is Abort) or`
	`  (countdown proceeds past timeA))`
	`{`
	`  close valve a`
	`}`

Intended Source Code	`If ((state is Abort) or`
	`  (countdown proceeds past timeB))`
	`{`
	`  close valve a`
	`}`

Implemented Source Code	`If (state is Abort)`
	`{`
	`  close valve a`
	`}`

Midwestern Blackout

August 14, 2003

- 50 million customers lost power
  - Economic loss between $4.5 and $10 billion. [ELC04]
- Software contribution:
  - Energy Management System Failed

Blackberry Failure

- February, 2008
  - 3.5 hour complete system failure
  - No e-mails sent or received
- Root Cause
  - Unsuccessful infrastructure upgrade by BlackBerry vendor Research In Motion.

- Software failure is expensive!
- Proper software testing can aid in creating a better product
- **KEY POINT:** Software testing is not a solution for all software problems
  - The right process and the right people are also required.

Wrap up