

“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](http://www.javaworld.com/javaworld/jw-07-1999/jw-07-toolbox.html) - [paraphrased],
<http://www.javaworld.com/javaworld/jw-07-1999/jw-07-toolbox.html>

Mythical
Man Month

Introduction – Impact of

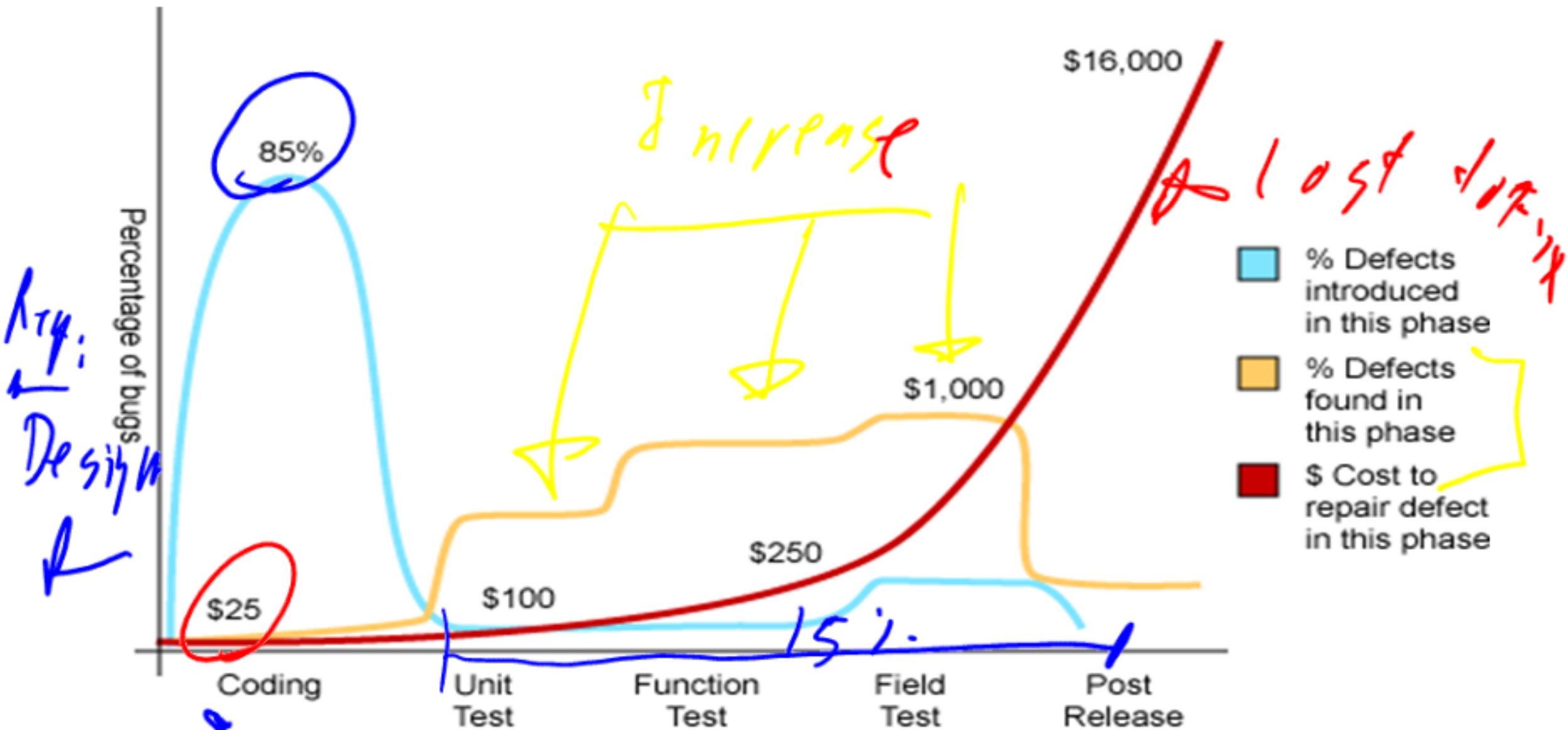
Failure

- 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

Software
Failure is
expensive!



Field Failures are Very expensive!



Source: Applied Software Measurement, Capers Jones, 1996

Introduction – Impact of

Failure

- 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
- Majority*
- Doubled*
- half*

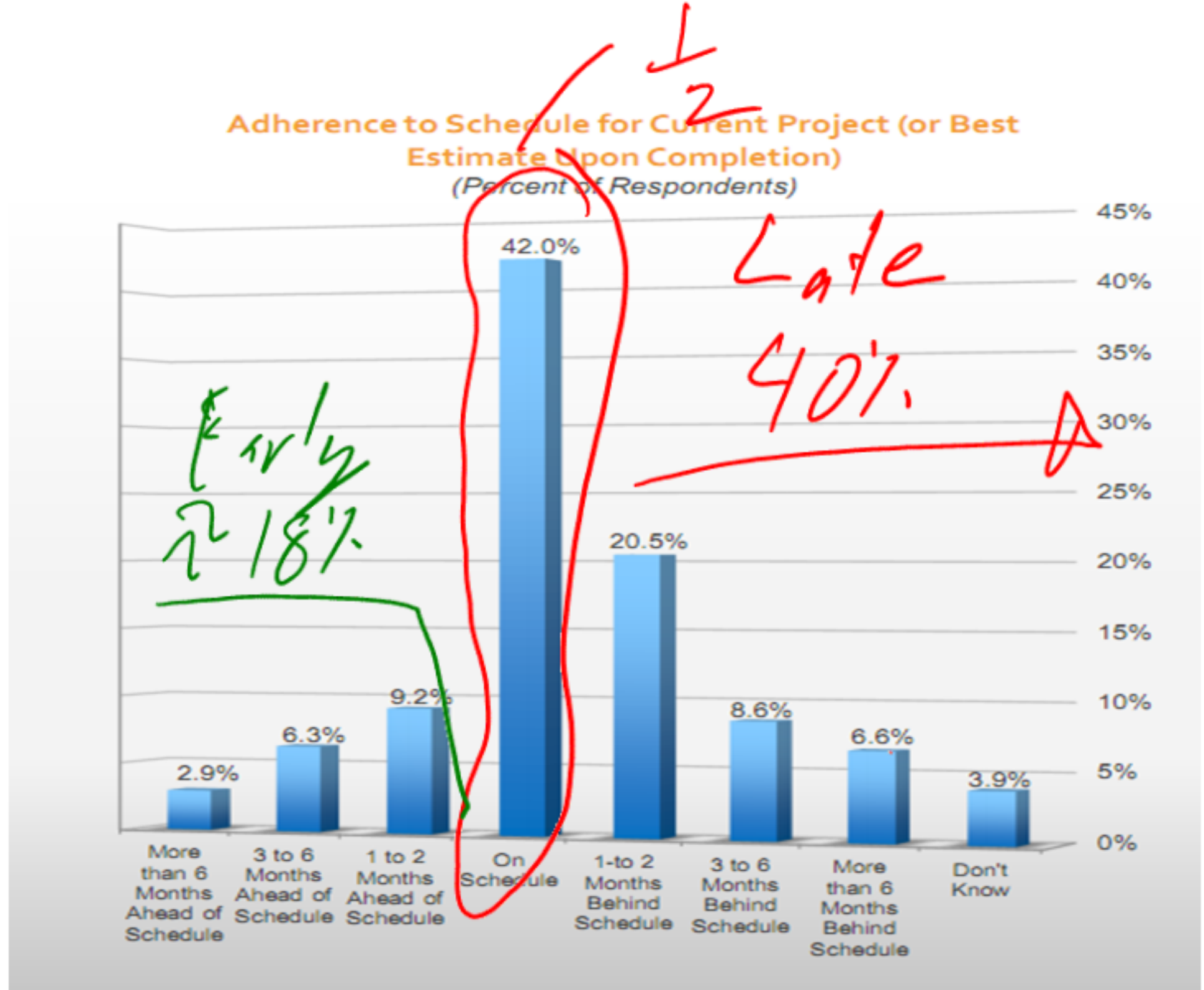
Chaos Report: http://www.standishgroup.com/sample_research/

Introduction to Software Verification

Copyright 2012-2013



On time shipment of products



Select Findings: Embedded Engineering Survey, 2011

Hi

in

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 you have been

exposed to?

Every program crashes ..

Screen Locking (w/ graphics drivers)

Keyboard driver failure.

Mouse drivers fail

Network drivers flakey

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;
  }
}
```

↓ Copy

→ # of days from
5-1-08 to 12-31-08

Microsoft
Zune



→ Last day of a Leap year.

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

True

True

December
31
366

→ else ... days = 366


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

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?



Shutting

crashed a server.

Text file w/ invalid character.

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

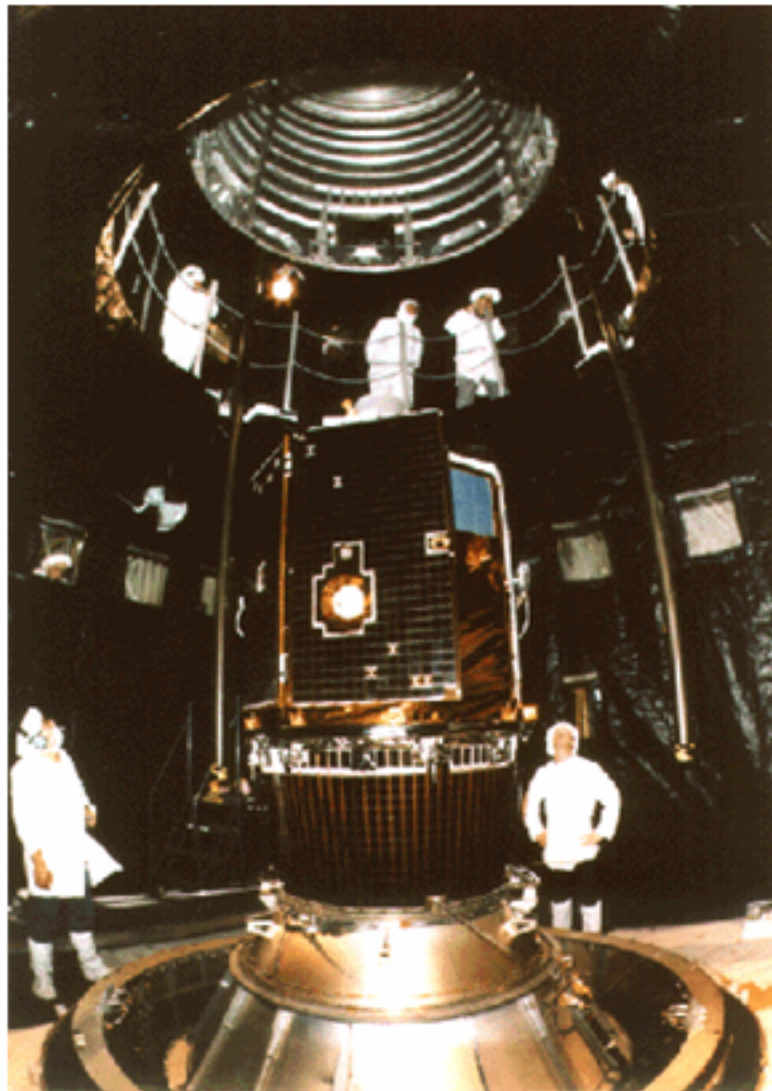


32

2 ms

NASA

Clementine Mission Failure



- Prototype for “Faster, Better, Cheaper” operation. *Failure*
 - 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

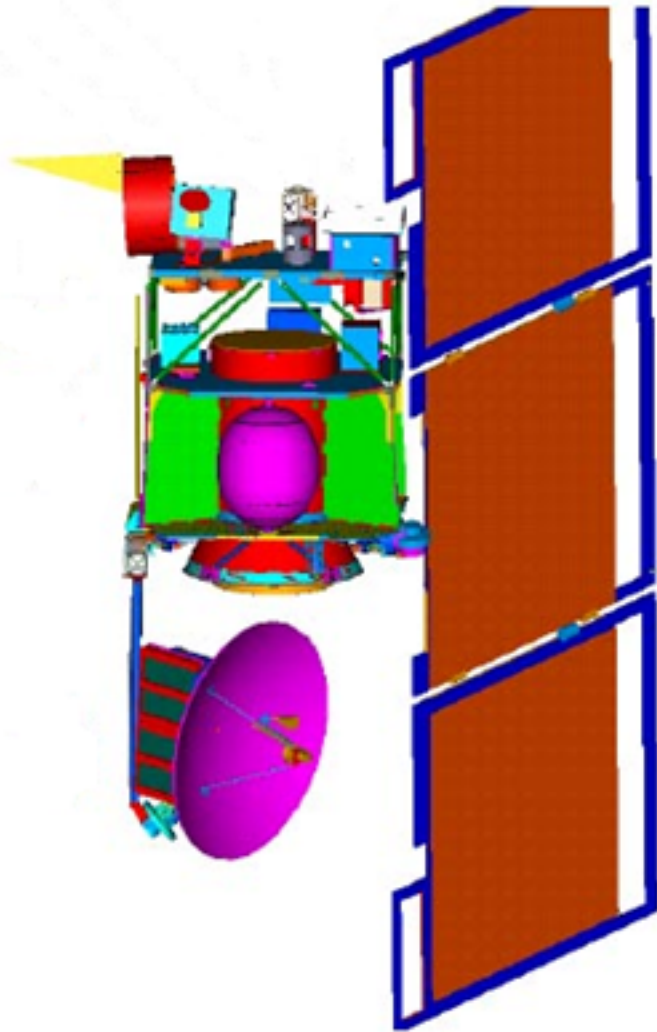
April 30, 1999



- *\$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	<pre>If ((state is Abort) or (countdown proceeds past timeA)) { close valve a }</pre>
Intended Source Code	<pre>If ((state is Abort) or (countdown proceeds past timeB)) { close valve a }</pre>
Implemented Source Code	<pre>If (state is Abort) { close valve a }</pre>

Missing
logic

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.



*Upgrade to
infrastructure.*

Wrapup

- 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.