




---

---

---

---

---

---

---

---

### Introduction

- Why Aerospace?
  - Life sustaining systems
  - Decades of knowledge from larger industry
- Software errors in aerospace systems responsible for:
  - >50 deaths
  - >\$700,000,000 in losses

---

---

---

---

---

---

---

---



### Introduction

#### Top 4

- Chinook Helicopter Crash
- V-22 Osprey Crash
- Ariane 5 Flight 501
- Mars Climate Orbiter




---

---

---

---

---

---

---

---



**Introduction**

**Top 4**

- Chinook Helicopter Crash
- V-22 Osprey Crash
- Ariane 5 Flight 501
- Mars Climate Orbiter



**LIVE** THE UNIVERSITY OF ALABAMA AT BIRMINGHAM  
 Knowledge that will change your world

---

---

---

---

---

---

---

---

---

---

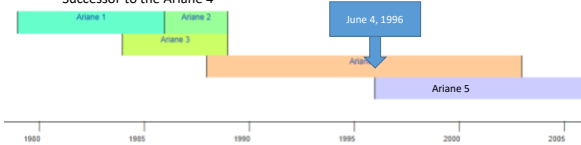
---

---

**Introduction**

**What is Ariane 5?**

- 7 Billion Investment 10 years to develop
- Heavy lift launch vehicle for placing payloads in low-Earth orbit.
- Successor to the Ariane 4



**LIVE** THE UNIVERSITY OF ALABAMA AT BIRMINGHAM  
 Knowledge that will change your world

---

---

---

---

---

---

---

---

---

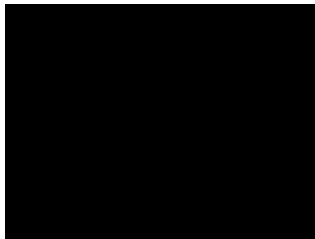
---

---

---

**Ariane 5 Flight 501 Catastrophe**

- Good Weather
- Initial launch as expected
- For 36 seconds behaved normally
- T = 37s, Veered off flight path
- Broke up and Exploded



**LIVE** THE UNIVERSITY OF ALABAMA AT BIRMINGHAM  
 Knowledge that will change your world

---

---

---

---

---

---

---

---

---

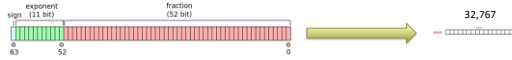
---

---

---

**Why The Failure?**

- Horizontal Bias stored as 64 bit floating point number
- Operand Error
- Inertial Reference System Shutdown



Lions, Jacques-Louis, et al. "Ariane 5 flight 501 failure report by the inquiry board." (1996).




---

---

---

---

---

---

---

---

---

---

A problem has been detected and system has been shutdown to prevent damage to your computer.

DRIVER\_IRQL\_NOT\_LES\_OR\_EQUAL

If this is the first time you've seen this stop error screen, restart your computer, if this screen appears again, follow these steps:

Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer for any system updates you might need.

If problems continue, disable or remove any newly installed hardware or software. Disable BIOS memory options such as caching or shadowing. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to select Advanced Startup Options, and then select Safe Mode.

Technical information:

\*\*\* STOP: 0x000000D1 (0x00000000, 0x00000007, 0x00000000, 0xG74H2S74)

\*\*\* str1.sys - Address G74H2S74 base at G74H0000, DateStamp 4eh2534df

Beginning dump of physical memory

Physical memory dump complete.

Contact your system administrator or technical support group for further assistance.

---

---

---

---

---

---

---

---

---

---

**Ariane 5 Flight 501 Catastrophe : Impacts**

- One of the most expensive software bugs in history
- \$370 million dollar loss (in 1996 dollars)
- 4 year delay on the payload mission




---

---

---

---

---

---

---

---

---

---



### Solution 2

#### Anticipate a Crash

- Try/Catch
- Logging

```
try
{
  //do anything
}
catch(error)
{
  //don't forget errors
}
```

Cristian, Flaviu. *Exception handling*. IBM Thomas J. Watson Research Division, 1987.




---

---

---

---

---

---

---

---

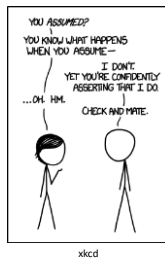
---

---

### Primary Failures: Cause 3

#### Assumed Code Correct Until Proven Otherwise

- It worked before, it will work this time
- Especially vulnerable on code changes during an added feature or bug fix



xicd




---

---

---

---

---

---

---

---

---

---

### Solution 3

#### Assume Erroneous Code Until Proven Otherwise

- Independent Code Review
- Unit Testing
- Integration Testing
- System Testing




---

---

---

---

---

---

---

---

---

---

### Unit Testing



- Unit testing is testing of individual units or groups of related units.
- An automated sanity check

Dustin, E. (2002). *Effective Software Testing: 50 Ways to Improve Your Software Testing*. Addison-Wesley Longman Publishing Co., Inc..  
 Runeson, P. (2006). A survey of unit testing practices. *IEEE software*, 23(4), 22-29.




---

---

---

---

---

---

---

---

---

---

### Integration Testing

- Testing on larger components or groups
- Making sure units work together

Meyer, Bertrand. "Seven principles of software testing." *Software Technology: 10 Years of Innovation in IEEE Computer* (2018).




---

---

---

---

---

---

---

---

---

---

### Systems Testing

- Final cohesive testing of entire system
- Tested against realistic inputs to achieve desired output
- "End To End" equivalent

Meyer, Bertrand. "Seven principles of software testing." *Software Technology: 10 Years of Innovation in IEEE Computer* (2018).




---

---

---

---

---

---

---

---

---

---

**Conclusion**

- Medical Physicists should embrace/adopt best practices learned from other industries
- Initiate best practices within our own domain
- Types of Errors Possible in RT
- 82 Successful Launches of the Ariane 5
- Ariane 6 to launch in 2020



---

---

---

---

---

---

---

---

