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

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

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

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
Why The Failure?

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

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

**DVI**RER**_ID**OL **NOT** _LET**_OE**_AL.

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

1. 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 updates you might need.
2. If problems continue, disable or remove any newly installed hardware or software. Disable memory options such as caching or debugging. 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: bx00000001 (0x00000000, 0x00000000, 0x00000000, 0x00000000)
*** event.exe - Address G74H57F7h at G74H57F7h, BadDump 4k/1024k/4k/
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
Primary Failures: Cause 1

Copy and Paste
- Inertial Reference System code copied from Ariane 4
- Ariane 4 horizontal bias never higher than 32,767
- Ariane 5 had different trajectory with higher horizontal velocity

Solution 1

Be cautious about copy/pasted or reused code
- Have clear specifications
- Separate and isolate critical components

"The fact that software has been used safely in another environment provides no information about its safety in the current one"


Primary Failures: Cause 2

Insufficient Error Handling
Solution 2

Anticipate a Crash

- Try/Catch
- Logging

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


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

![xkcd comic](https://xkcd.com/314/)

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

Integration Testing

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

Systems Testing

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


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