High Integrity Software

Industrial

Formal Methods

SWEN421-2016

Trust me I am a programmer!

- For some projects speed is more important than correctness.

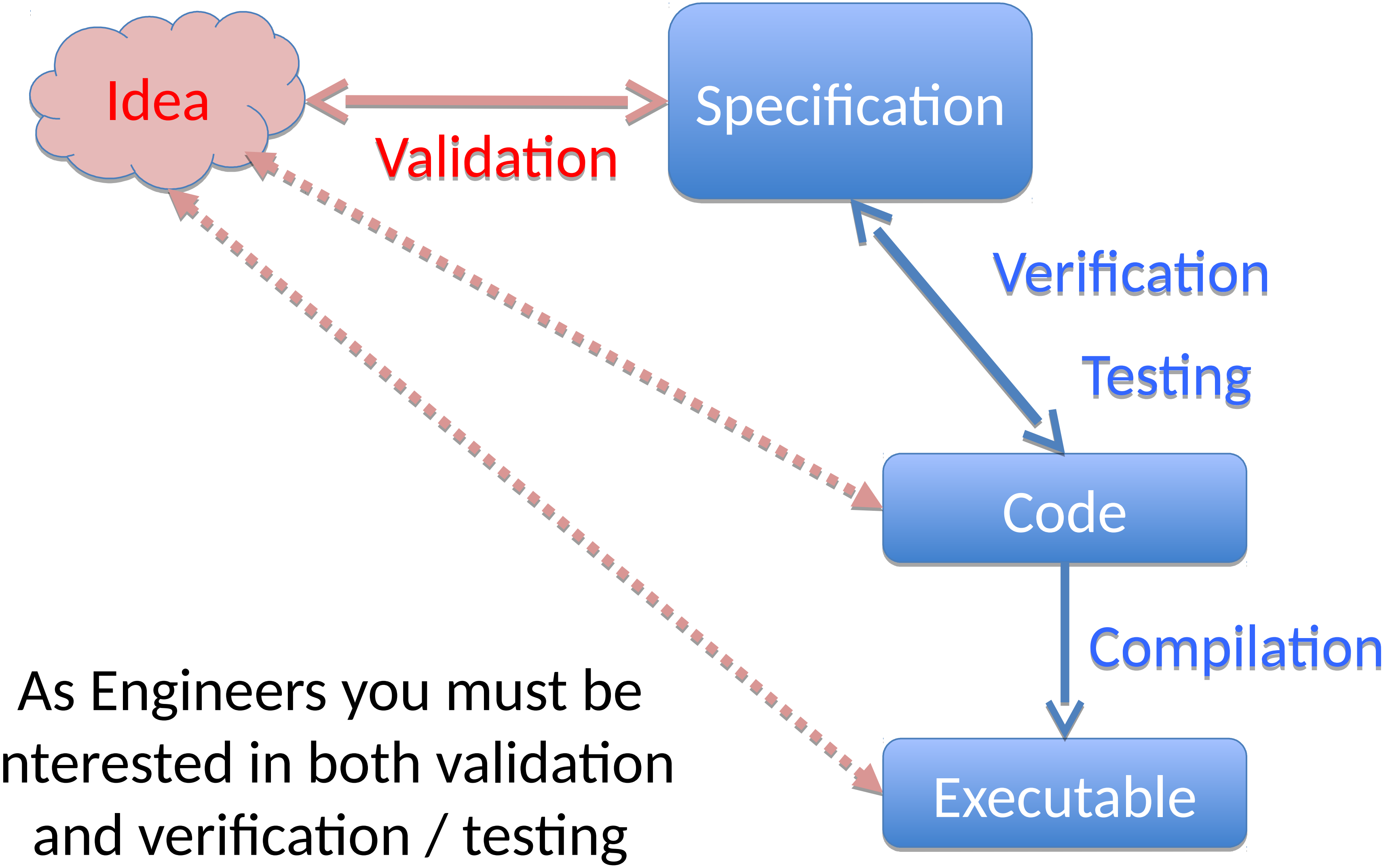
- Critical projects require correctness
  1. Safety Critical
  2. Economically Critical

- Gallagher charge more than others because they have the reputation of getting it right.

Not business as usual

- Writing correct code requires doing things differently not doing the usual better.
- Use a language designed for verification
- Write a specification that can be executed and / or verified.

Specifications and testing



As Engineers you must be interested in both validation and verification / testing

Quality Assurance

- Not all software can be Verified, even less software can be verified cost effectively.
- Quality is assured by auditing the process use in building, testing, verifying, maintenance,…
- International standards and certification exist in different domains: military, avionics, motor, rail, …..

Ada

- The Ada Language was designed for writing high Integrity software
- SPARK Ada is a subset of Ada (as of 2014) designed to help with Verification.

- Used by military, avionics industry, automotive industry, …
- Gallagher in NZ want to write soft ware for petrol pumps

Ada Features

- Strong Type checking
- Specifications and Contracts
- Strong information hiding
- Flow specification and automatic analysis
- No garbage collection or pointer arithmetic
- Strict control of “inheritance”
- Fixed point and floating point arithmetic

Its the detail that kills

- 1991 patriot missile missed an incoming Scud with loss of 28 lives. Floating point inaccuracy caused by running the system continuously for 100 hours.
- Ariane 5 was faster than Ariane 4 and hence known software “feature” caused loss of $500,000,000 rocket.
- EDS Child support system + DWI system were incompatible cost UK over $1,000,000,000.
- American NorthEast blackout 2004 – race condition

Spark Ada

- Meets the requirements of many international standards.
- Integrated proof and testing, using Why3 and a collection of SMT provers.

This week!

- Go To Ada Core Libre down load and install GNAT 2016 and SPARK 2016
- Windows no problems
- Mac OS you need to follow: MacOS debugger codesign and beware MacOS right click as control click did not work for me but using a three button mouse the debug er worked.

This Week

- Run GPS from a terminal
- Complete the tutorial in   Help>GPS>tutorial.
- Users Guide Help>SPARK> SPARK 2014