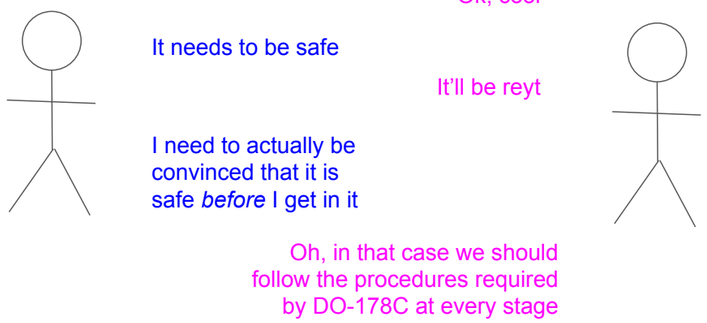
COM4506/6506: Testing and Verification in Safety Critical Systems

Dr Ramsay Taylor

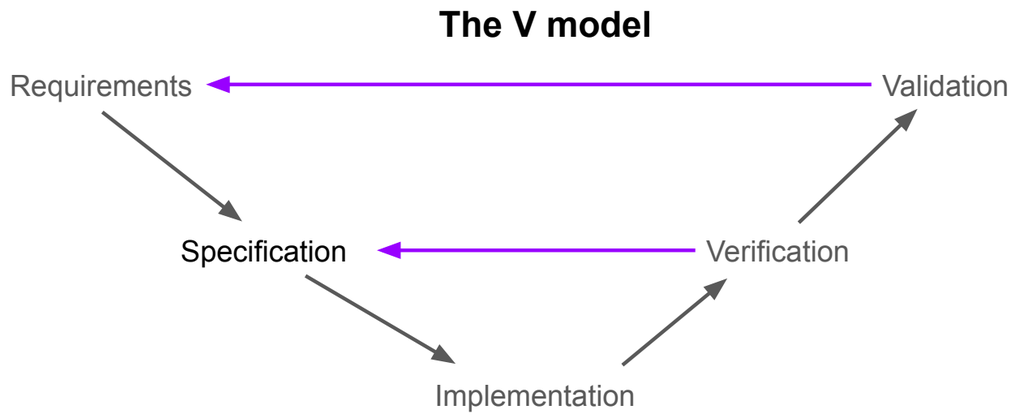
Contents

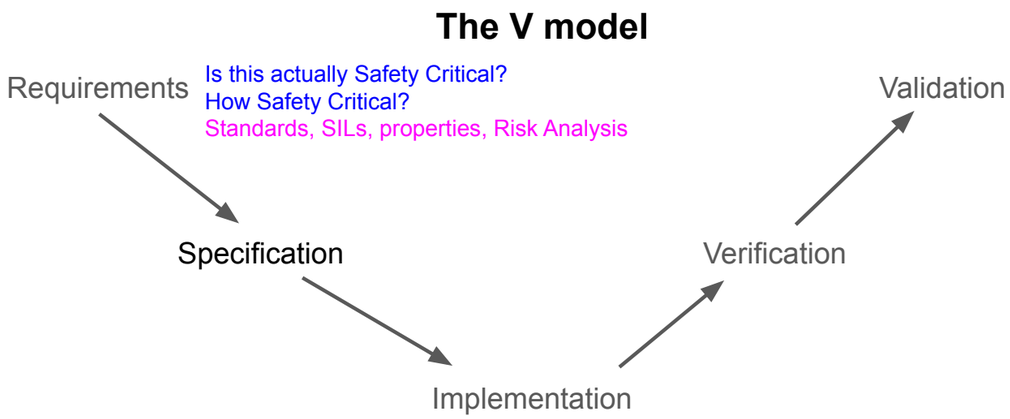
- Everything!

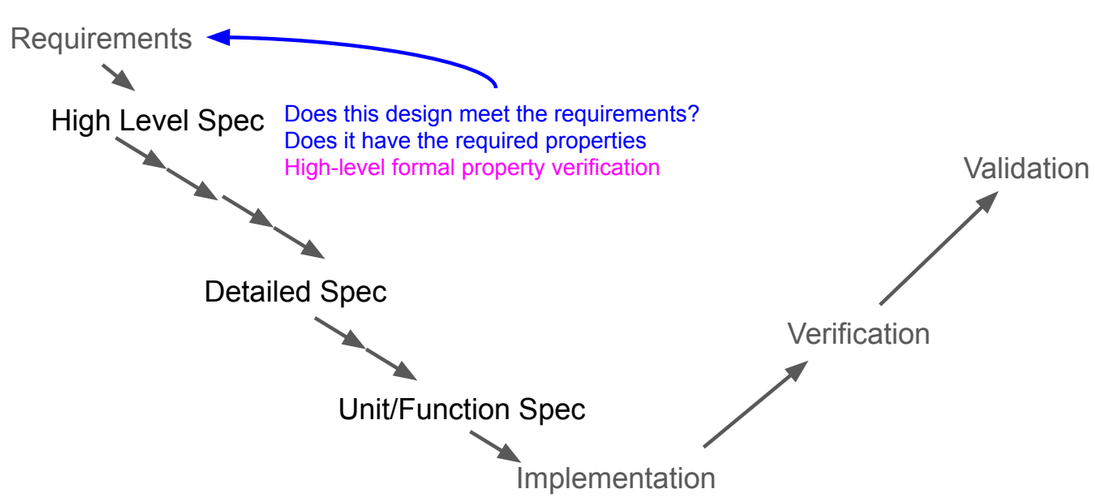
Safety Critical Software Engineering

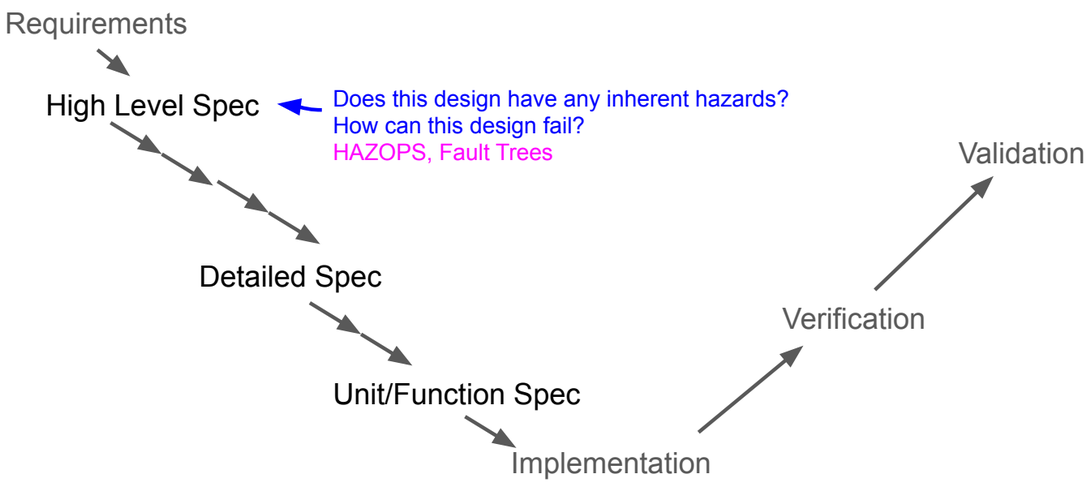


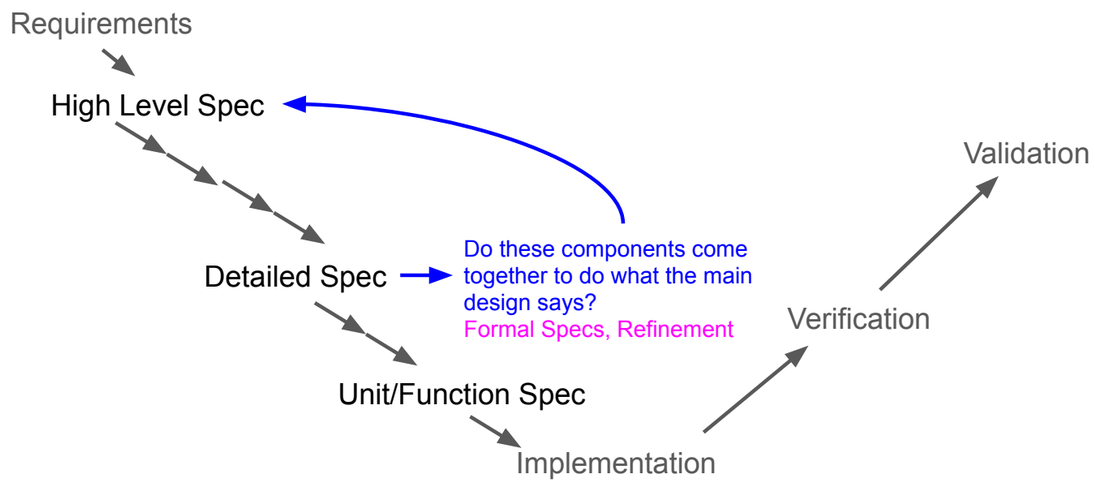
The V model

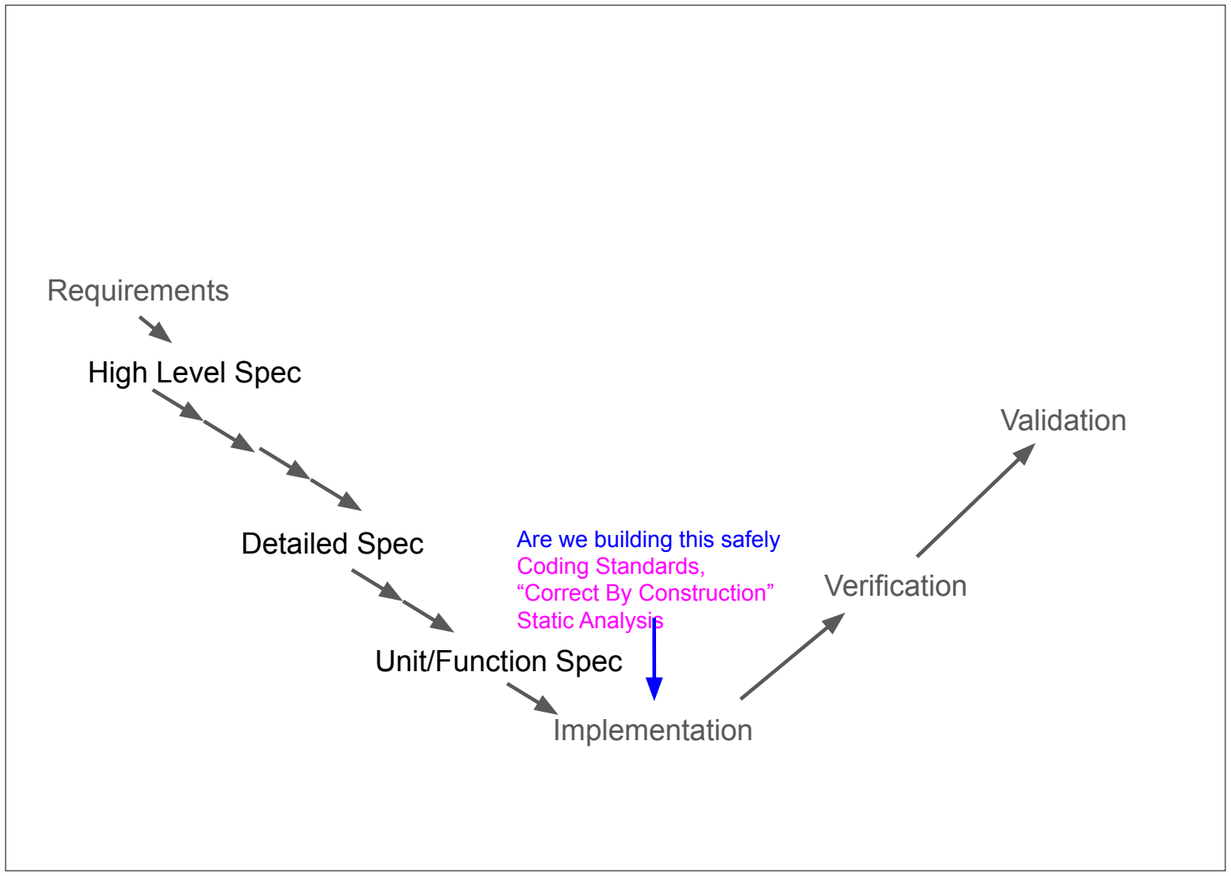


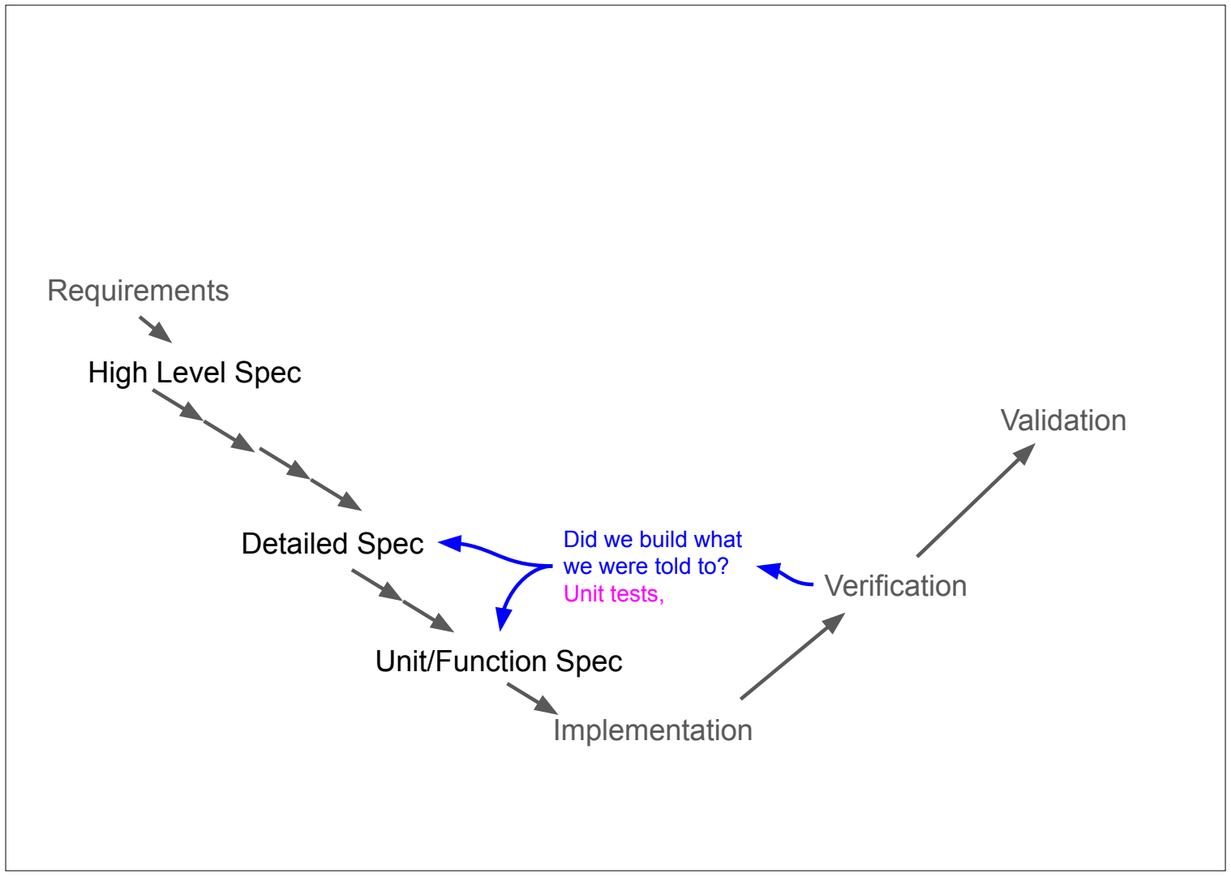

The V model
Requirements
Is this actually Safety Critical?
How Safety Critical?
Standards, SILs, properties, Risk Analysis
Validation
Specification
Verification
Implementation

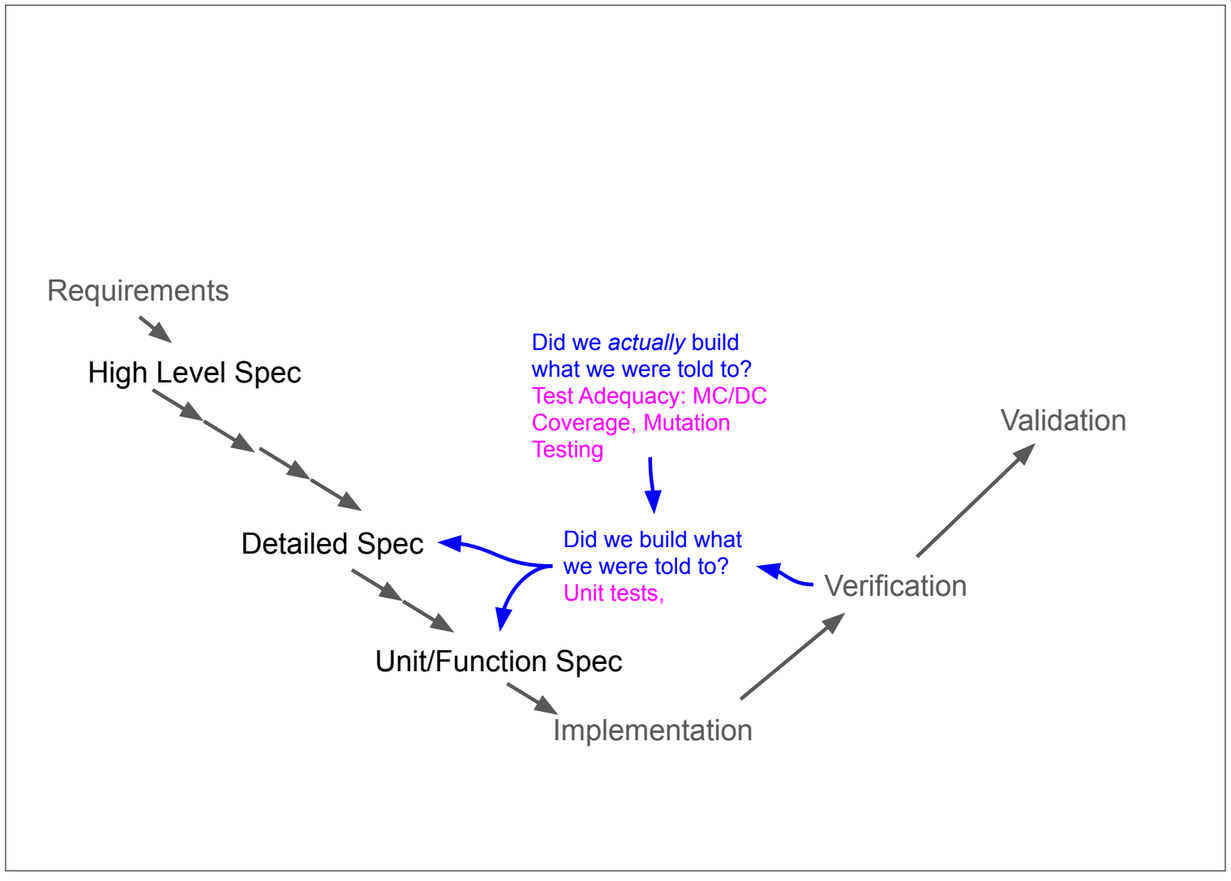

Requirements
High Level Spec
Does this design meet the requirements?
Does it have the required properties
High-level formal property verification
Validation
Detailed Spec
Verification
Unit/Function Spec
Implementation

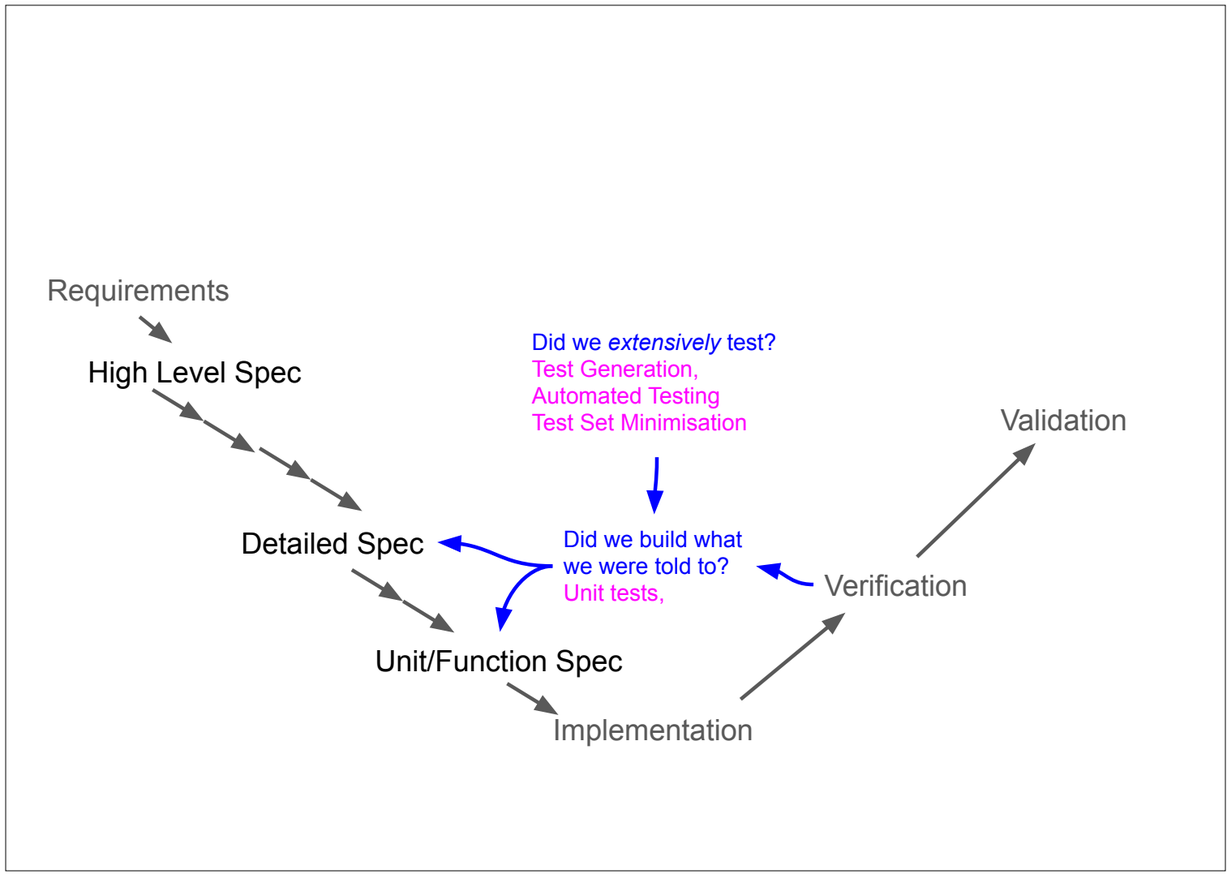

Requirements
High Level Spec
Does this design have any inherent hazards?
How can this design fail?
HAZOPS, Fault Trees
Validation
Detailed Spec
Verification
Unit/Function Spec
Implementation

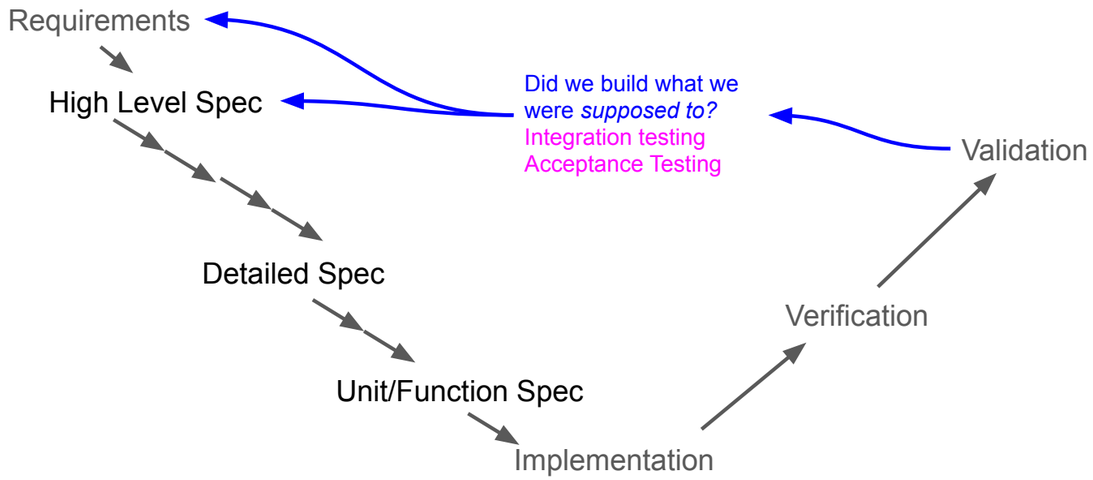

Requirements
High Level Spec
Validation
Detailed Spec
Do these components come together to do what the main design says?
Formal Specs, Refinement
Verification
Unit/Function Spec
Implementation

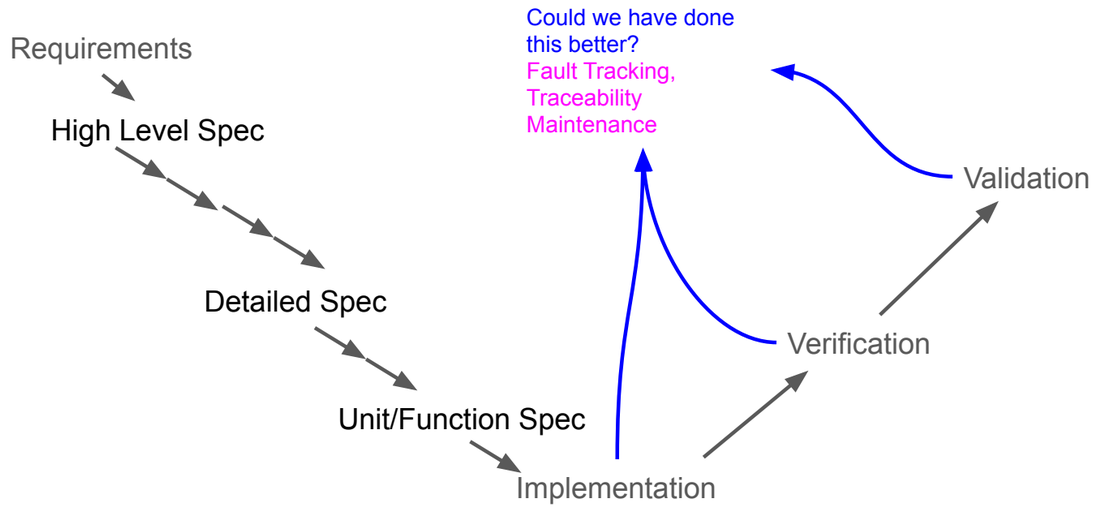

Requirements
High Level Spec
Detailed Spec
Unit/Function Spec
Implementation
Verification
Validation
Are we building this safely
Coding Standards,
“Correct By Construction”
Static Analysis

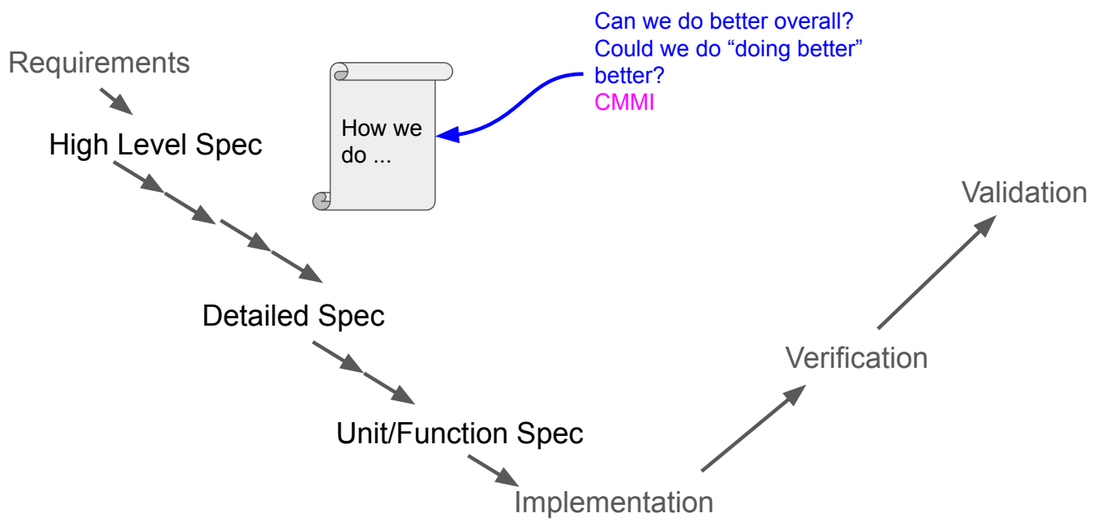

Requirements
High Level Spec
Detailed Spec
Unit/Function Spec
Implementation
Verification
Validation
Did we build what
we were told to?
Unit tests,


Requirements
High Level Spec
Detailed Spec
Unit/Function Spec
Implementation
Verification
Validation
Did we *actually* build
what we were told to?
Test Adequacy: MC/DC
Coverage, Mutation
Testing
Did we build what
we were told to?
Unit tests,


Requirements
High Level Spec
Detailed Spec
Unit/Function Spec
Implementation
Verification
Validation
Did we *extensively* test?
Test Generation,
Automated Testing
Test Set Minimisation
Did we build what
we were told to?
Unit tests,







Safety Critical Systems

Any engineered system *will* have flaws.

In Safety Critical Systems those flaws can hurt or kill people.

We *can't* remove all flaws.

We *can* put time and effort into reducing flaws, identifying flaws, and mitigating flaws.

We can also use processes that make it clear that we have done our best.

The End!