COM4506/6506: Testing and Verification in Safety Critical Systems

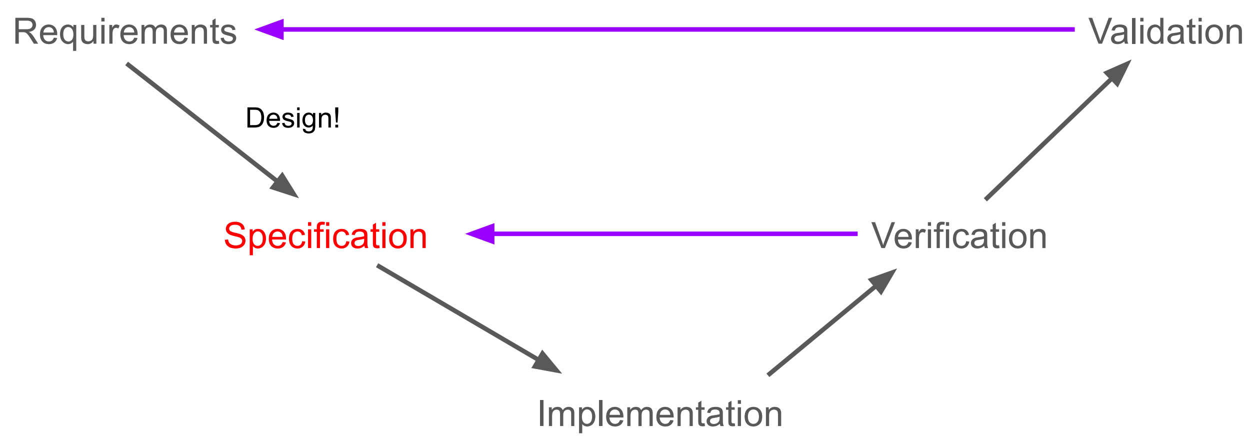
Dr Ramsay Taylor

Contents

- Specifications - Where do they fit in development?
- Some (of many) approaches to specifications
- Traceability

Development Stages

The V model



Requirements

Validation

Design!

Specification

Verification

Implementation

Engineering Design

The step between Requirements and Specifications is called *Design*

In non-safety critical settings, software engineers (and some other engineers) much prefer to mix design and implementation.

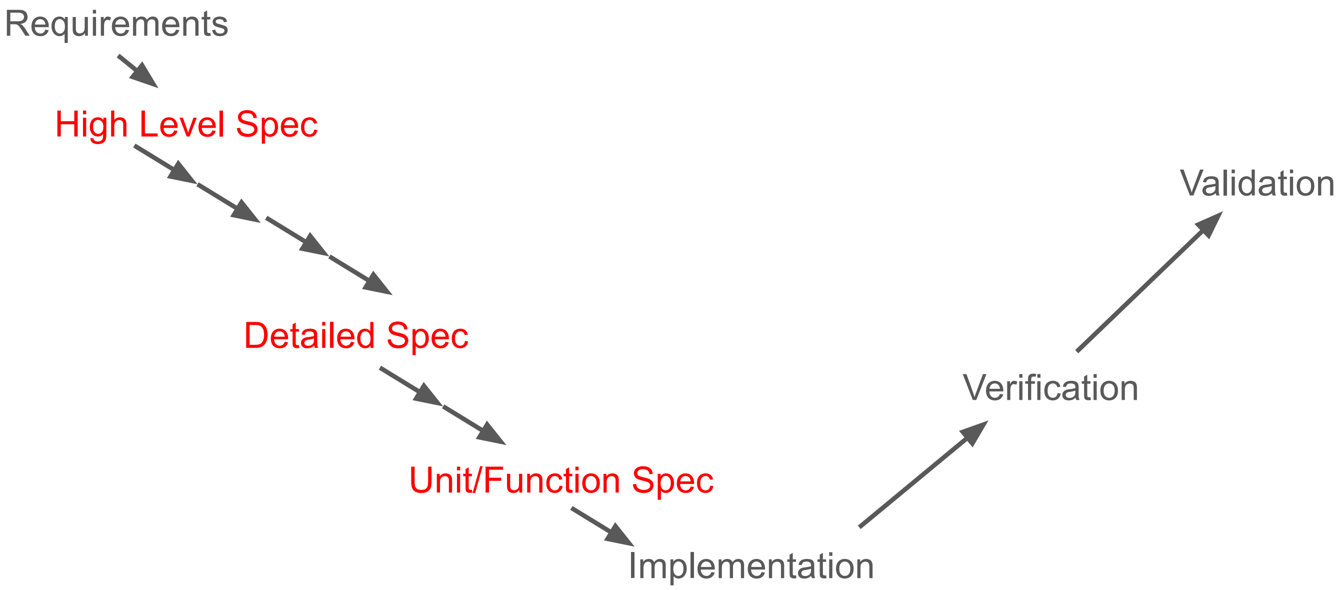
Engineering Design

When the system is safety critical, we can't "get creative" with the implementation!

Parts of the spec will be *mitigating hazards.*

This **doesn't** mean the skills and experience of the implementers should be ignored!

Progressive detail



Requirements

High Level Spec

Detailed Spec

Unit/Function Spec

Implementation

Verification

Validation

Progressive Detail

"I want a plane!"

"I want a *fast* plane!"

© 2016 Ricardo von Puttkammer

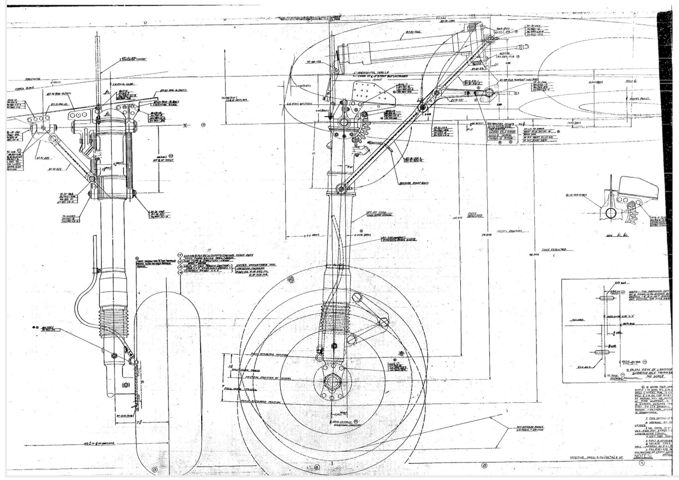
Progressive Detail

"I want a plane!"

"I want a *fast* plane!"

"I probably want to be able to land the fast plane…"

"The plane needs landing gear"



Progressive Detail

“I want a plane!”

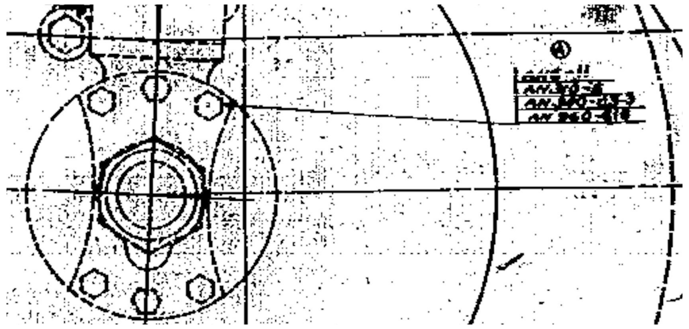
“I want a *fast* plane!”

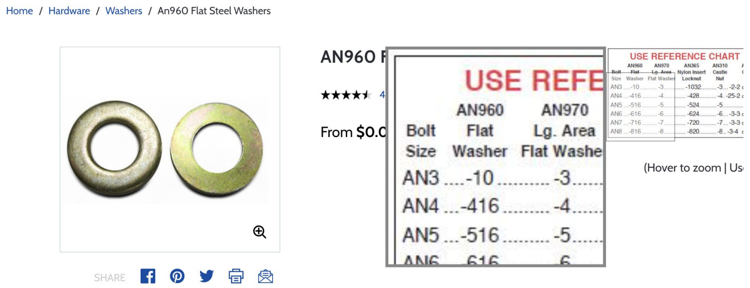
“I probably want to be able to land the fast plane…”

“The plane needs landing gear”

[... some time later…]

“The washers on the bolts holding the wheels on will be type AN960-416”





Home / Hardware / Washers / An960 Flat Steel Washers

AN960 F

★★★★★ 4

From $0.0

USE REFE

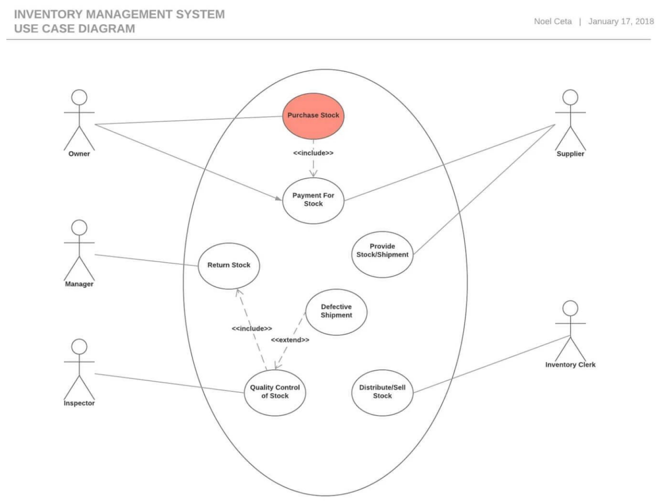
Bolt Size	AN960 Flat Washer	AN970 Lg. Area Flat Washe
AN3	....-10	.... -3.....
AN4	...-416	.... -4.....
AN5	...-516	.... -5.....
AN6	...616	 6

USE REFERENCE CHART

Bolt Size	AN960 Flat Washer	AN970 Lg. Area Flat Washer	AN365 Nylon Insert Locknut	AN310 Castle Nut
AN3	....-10	.... -3	.... -1032	.... -3... -2-2
AN4	...-416	.... -4	.... -428	.... -4. -25-2
AN5	...-516	.... -5	.... -524	.... -5........
AN6	...-616	.... -6	.... -624	.... -6... -3-3
AN7	...-716	.... -7	.... -720	.... -7... -3-3
AN8	...-816	.... -8	.... -820	.... -8.. -3-4

(Hover to zoom | Us

What does a Specification look like?



INVENTORY MANAGEMENT SYSTEM
USE CASE DIAGRAM

Noel Ceta | January 17, 2018

Various informal and semi-formal documents.

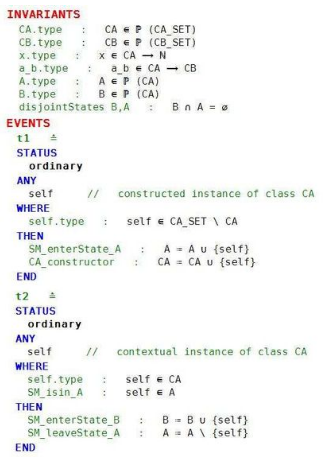
UML?

CAD?

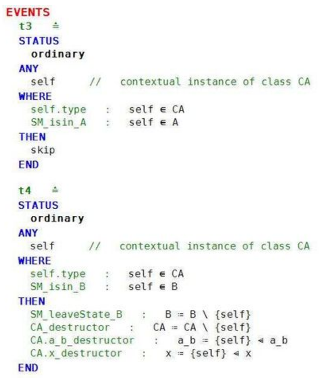
Schematics?

English...

What does a Specification look like?



```
INVARIANTS
  CA.type   :   CA ∈ ℙ (CA_SET)
  CB.type   :   CB ∈ ℙ (CB_SET)
  x.type   :   x ∈ CA → N
  a_b.type   :   a_b ∈ CA → CB
  A.type   :   A ∈ ℙ (CA)
  B.type   :   B ∈ ℙ (CA)
  disjointStates B,A   :   B ∩ A = ∅
EVENTS
 t1   ≙
 STATUS
   ordinary
 ANY
   self     //   constructed instance of class CA
 WHERE
   self.type   :   self ∈ CA_SET \ CA
 THEN
   SM_enterState_A   :   A ≔ A ∪ {self}
   CA_constructor   :   CA ≔ CA ∪ {self}
 END
 t2   ≙
 STATUS
   ordinary
 ANY
   self     //   contextual instance of class CA
 WHERE
   self.type   :   self ∈ CA
   SM_isin_A   :   self ∈ A
 THEN
   SM_enterState_B   :   B ≔ B ∪ {self}
   SM_leaveState_A   :   A ≔ A \ {self}
 END
```



```
EVENTS
 t3   ≙
 STATUS
   ordinary
 ANY
   self     //   contextual instance of class CA
 WHERE
   self.type   :   self ∈ CA
   SM_isin_A   :   self ∈ A
 THEN
   skip
 END

 t4   ≙
 STATUS
   ordinary
 ANY
   self     //   contextual instance of class CA
 WHERE
   self.type   :   self ∈ CA
   SM_isin_B   :   self ∈ B
 THEN
   SM_leaveState_B   :   B ≔ B \ {self}
   CA_destructor   :   CA ≔ CA \ {self}
   CA.a_b_destructor   :   a_b ≔ {self} ⩤ a_b
   CA.x_destructor   :   x ≔ {self} ⩤ x
 END
```

Formal Languages:

CSP, CCS, Pi-Calculus

Z, B, Event-B, Alloy

Programming Language structures:

SPARK-Ada assertions

Java assertions?

Test as Specs?

Test *can* specify how a system should work.

This can either be detailed *unit tests*, or more general *integration tests*.

Tests can be *derived* from (good!) specs.

Test Driven Development is useful for lots of reasons.

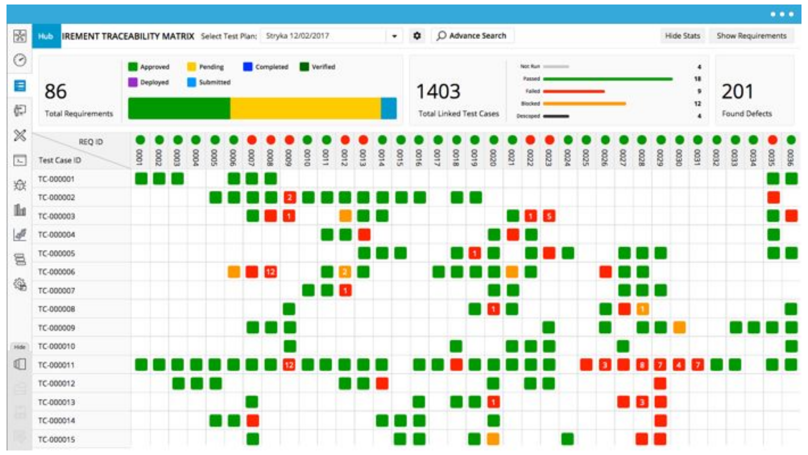
But this should only be *one aspect* of specification!

Traceability

As the spec is developed, we want to keep track of *why* we are building it this way.

Not least, so that we don't change a Spec that is mitigating a hazard!

This will also help with *Validation* later.



Hub IREMENT TRACEABILITY MATRIX Select Test Plan: Stryka 12/02/2017

Advance Search | Hide Stats | Show Requirements

86 Total Requirements

1403 Total Linked Test Cases

201 Found Defects

Summary

- Moving from a set of Requirements to a Specification is the *Design* process!
- The Specification will get more and more specific (but retain all of the documents!)
- There are various different *Specification Languages* - use all that are appropriate.
- Specs and Tests will have a complex and important relationship…
- The more you can maintain *Traceability* the better.