Rigorous Development: An Introduction [1]

Manuel Carro
manuel.carro@upm.es

IMDEA Software Institute &
Universidad Politécnica de Madrid

[1] Many slides borrowed from J. R. Abrial and M. Butler

Take notes

TECHNOLOGY

To Remember a Lecture Better, Take Notes by Hand

Students do worse on quizzes when they use keyboards in class.

Picture & headline ©*The Atlantic*

https://www.theatlantic.com/technology/archive/2014/05/to-remember-a-lecture-better-take-notes-by-hand/361478/

I will make notes / slides available *after* the lectures
I will ask you to work during the lectures

Purpose of the Course

- To give you some insights about modelling and formal reasoning
- To show that programs can be correct by construction
- To show that modelling can be made practical
- To illustrate this approach with many examples

What You Will Learn

By the end of the course you should be comfortable with:

- Modelling (versus programming)
- Abstraction and Refinement
- Some mathematical techniques used for reasoning on programs
- The practice of proving as a means to construct (provably) correct programs
- The usage of some tools to help in the above

Software is omnipresent in everyday life

Today's car: typically 100 microprocessors, 100 M. lines of code, 20.000 programmer years.

Software is omnipresent in everyday life

Plane: computers manage controls, calculate routes, ...

Software is omnipresent in everyday life

Large interconnected systems: independent, isolated, automatic decision making, which must be globally correct.

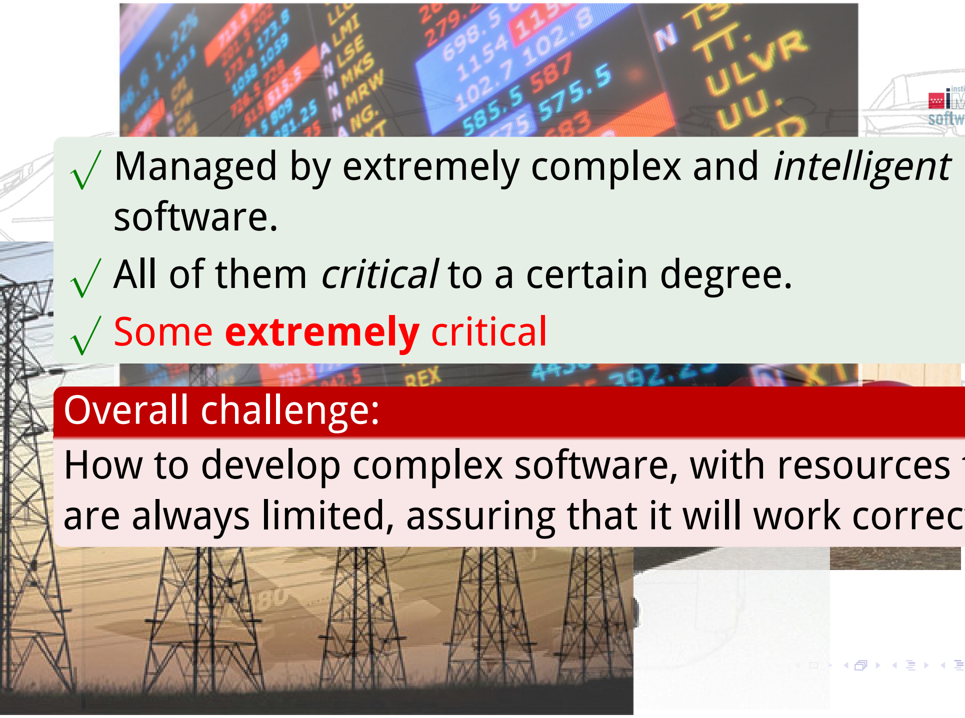
Software is omnipresent in everyday life

- Cell phones (from O.S. to compression algorithms to user interfaces).
- HDTV (routing, encoding and decoding)... Netflix!
- Buy and sell on the Internet (web interfaces, databases, encryption).
- Stock market (algorithmic trading, high frequency trading).
- Skype, Whatsapp, AirBnB, idealista, GroupOn, FB, Steam, Spotify, E-Banking, Google Maps / Waze, Uber / Lyft, ...

√ Managed by extremely complex and *intelligent* software.

√ All of them *critical* to a certain degree.

√ Some **extremely** critical



√ Managed by extremely complex and *intelligent* software.

√ All of them *critical* to a certain degree.

√ Some **extremely** critical

Overall challenge:

How to develop complex software, with resources that are always limited, assuring that it will work correctly?

Growth in Complexity and Expectations

- Processes managed by computing systems increasingly complex.
- Same software is to run in more platforms.
- Computing systems to interact more and more with other systems.
- They should stay autonomous for longer.
- They become reactive.

Then and Now

Yesterday | **Today** | **Tomorrow**

It's nice that I can see my account through my web browser!

Then and Now

Yesterday | **Today** | **Tomorrow**

It's nice that I can see my account through my web browser!

I <u>need</u> to make this bank transfer <u>now</u> and I am not even in my country!

Then and Now

Yesterday | **Today** | **Tomorrow**

It's nice that I can see my account through my web browser!

I <u>need</u> to make this bank transfer <u>now</u> and I am not even in my country!

- Operating System
- Browser
- Network protocols
- Encoding / cryptography
- Web server
- Database (parallelism, concurrency)

Then and Now

Yesterday | **Today** | **Tomorrow**

It's nice that I can see my account through my web browser!

I <u>need</u> to make this bank transfer <u>now</u> and I am not even in my country!

?

(but we need to be ready to build it)

- Operating System
- Browser
- Network protocols
- Encoding / cryptography
- Web server
- Database (parallelism, concurrency)

How Far Are We from Giving Reasonable Guarantees?
(Only showing some types of problems)

- Skype bug sends messages to unintended recipients.

How Far Are We from Giving Reasonable Guarantees?
(Only showing some types of problems)

- Skype bug sends messages to unintended recipients.
- Apple's "in-app purchase" service for iOS bypassed by Russian hacker.

How Far Are We from Giving Reasonable Guarantees?
(Only showing some types of problems)

- Skype bug sends messages to unintended recipients.
- Apple's "in-app purchase" service for iOS bypassed by Russian hacker.
- German security experts find major flaw in credit card terminals.

How Far Are We from Giving Reasonable Guarantees?
(Only showing some types of problems)

- Skype bug sends messages to unintended recipients.
- Apple's "in-app purchase" service for iOS bypassed by Russian hacker.
- German security experts find major flaw in credit card terminals.
- Defects leave critical military, industrial infrastructure open to hacks (Niagara Framework, linking 11+ million devices in 52 countries).

How Far Are We from Giving Reasonable Guarantees?

(Only showing some types of problems)

- Skype bug sends messages to unintended recipients.
- Apple's "in-app purchase" service for iOS bypassed by Russian hacker.
- German security experts find major flaw in credit card terminals.
- Defects leave critical military, industrial infrastructure open to hacks (Niagara Framework, linking 11+ million devices in 52 countries).
- Hackers expose 453,000 credentials allegedly taken from Yahoo service.

How Far Are We from Giving Reasonable Guarantees?

(Only showing some types of problems)

- Skype bug sends messages to unintended recipients.
- Apple's "in-app purchase" service for iOS bypassed by Russian hacker.
- German security experts find major flaw in credit card terminals.
- Defects leave critical military, industrial infrastructure open to hacks (Niagara Framework, linking 11+ million devices in 52 countries).
- Hackers expose 453,000 credentials allegedly taken from Yahoo service.

- Mountain Lion (Mac OS X version) sends some 64-bit Macs to sleep (related to graphics drivers).

How Far Are We from Giving Reasonable Guarantees?

(Only showing some types of problems)

- Skype bug sends messages to unintended recipients.
- Apple's "in-app purchase" service for iOS bypassed by Russian hacker.
- German security experts find major flaw in credit card terminals.
- Defects leave critical military, industrial infrastructure open to hacks (Niagara Framework, linking 11+ million devices in 52 countries).
- Hackers expose 453,000 credentials allegedly taken from Yahoo service.
- Mountain Lion (Mac OS X version) sends some 64-bit Macs to sleep (related to graphics drivers).

- Still infected, 300,000 PCs to lose Internet access.

How Far Are We from Giving Reasonable Guarantees?

(Only showing some types of problems)

- Skype bug sends messages to unintended recipients.
- Apple's "in-app purchase" service for iOS bypassed by Russian hacker.
- German security experts find major flaw in credit card terminals.
- Defects leave critical military, industrial infrastructure open to hacks (Niagara Framework, linking 11+ million devices in 52 countries).
- Hackers expose 453,000 credentials allegedly taken from Yahoo service.
- Mountain Lion (Mac OS X version) sends some 64-bit Macs to sleep (related to graphics drivers).
- Still infected, 300,000 PCs to lose Internet access.

- Apple fixes App Store DRM error, crash-free downloads resume.

How Far Are We from Giving Reasonable Guarantees?

(Only showing some types of problems)

Skype bug sends messages to unintended recipients.

Apple's "in-app purchase" service for iOS bypassed by Russian hacker.

German security experts find major flaw in credit card terminals.

Defects leave critical military, industrial infrastructure open to hacks (Niagara Framework, linking 11+ million devices in 52 countries).

Hackers expose 453,000 credentials allegedly taken from Yahoo service.

Mountain Lion (Mac OS X version) sends some 64-bit Macs to sleep (related to graphics drivers).

Still infected, 300,000 PCs to lose Internet access.

Apple fixes App Store DRM error, crash-free downloads resume.

"Find and Call" app becomes first trojan to appear on iOS App Store.

How Far Are We from Giving Reasonable Guarantees?

(Only showing some types of problems)

Skype bug sends messages to unintended recipients.

Apple's "in-app purchase" service for iOS bypassed by Russian hacker.

German security experts find major flaw in credit card terminals.

Defects leave critical military, industrial infrastructure open to hacks (Niagara Framework, linking 11+ million devices in 52 countries).

Hackers expose 453,000 credentials allegedly taken from Yahoo service.

Mountain Lion (Mac OS X version) sends some 64-bit Macs to sleep (related to graphics drivers).

Still infected, 300,000 PCs to lose Internet access.

Apple fixes App Store DRM error, crash-free downloads resume.

"Find and Call" app becomes first trojan to appear on iOS App Store.

iOS, Mac app crashes linked to botched FairPlay DRM.

How Far Are We from Giving Reasonable Guarantees?

(Only showing some types of problems)

July 16, 2012: Skype bug sends messages to unintended recipients.

July 13, 2012: Apple's "in-app purchase" service for iOS bypassed by Russian hacker.

July 13, 2012: German security experts find major flaw in credit card terminals.

July 13, 2012: Defects leave critical military, industrial infrastructure open to hacks (Niagara Framework, linking 11+ million devices in 52 countries).

July 12, 2012: Hackers expose 453,000 credentials allegedly taken from Yahoo service.

July 12, 2012: Mountain Lion (Mac OS X version) sends some 64-bit Macs to sleep (related to graphics drivers).

July 7, 2012: Still infected, 300,000 PCs to lose Internet access.

July 6, 2012: Apple fixes App Store DRM error, crash-free downloads resume.

July 5, 2012: "Find and Call" app becomes first trojan to appear on iOS App Store.

July 5, 2012: iOS, Mac app crashes linked to botched FairPlay DRM.

Just two weeks

The Ariane 5 Incident

Example: effect of a *single* integer overflow

The Ariane 5 Incident

Example: effect of a *single* integer overflow

- June 4, 1996: After launch, the Ariane 5 rocket exploded.
- This was its maiden voyage.
- It flew for about 37 Sec only in Kourou's sky.
- No injury in the disaster.

The Story

- Normal behavior of the launcher for 36 Sec after lift-off
- Failure of both Inertial Reference Systems almost simultaneously
- Strong pivoting of the nozzles of the boosters and Vulcan engine
- Self-destruction at an altitude of 4000 m (1000 m from the pad)

More Details

- Both inertial computers failed because of overflow on one variable
- This caused a software exception that stopped these computers
- These computers sent post-mortem info through the bus
- Normally, main computer receives velocity info through the bus
- The main computer was confused and pivoted the nozzles

More Details

- The faulty program was working correctly on Ariane 4
- The faulty program was not tested for A5 (since it worked for A4)
- But the velocity of Ariane 5 is far greater than that of Ariane 4
- That caused the overflow in one variable
- The faulty program happened to be useless for Ariane 5

Messages

- Clear, up to date, realistic requirements
- Relationship requirements / programs
- Proof that programs was built according to requirements

Note: we will not deal with requirement engineering*, which is related and very interesting in itself.*

How?

- How can we **ensure** that a program does what it is supposed to do?

How?

- How can we **ensure** that a program does what it is supposed to do?
  1. How do we state what is it supposed to do?
     (usually via *specifications*)

How?

- How can we **ensure** that a program does what it is supposed to do?
  1. How do we state what is it supposed to do?
     (usually via *specifications*)
  2. How do we build the program?

How?

- How can we **ensure** that a program does what it is supposed to do?
  1. How do we state what is it supposed to do? (usually via *specifications*)
  2. How do we build the program?
  3. How do we prove that the program performs according to specifications?

How?

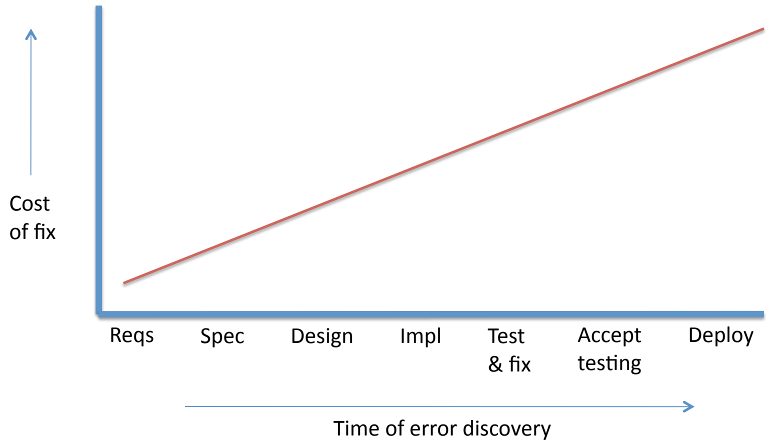
- How can we **ensure** that a program does what it is supposed to do?
  1. How do we state what is it supposed to do? (usually via *specifications*)
  2. How do we build the program?
  3. How do we prove that the program performs according to specifications?

How?

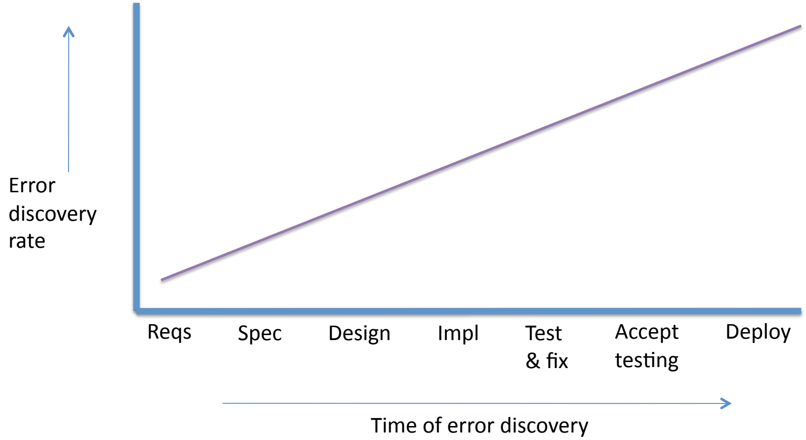
- How can we **ensure** that a program does what it is supposed to do?
  1. How do we state what is it supposed to do? (usually via *specifications*)
  2. How do we build the program?
  3. How do we prove that the program performs according to specifications?

...in a way that is (a) dependable and (b) cost-effective?

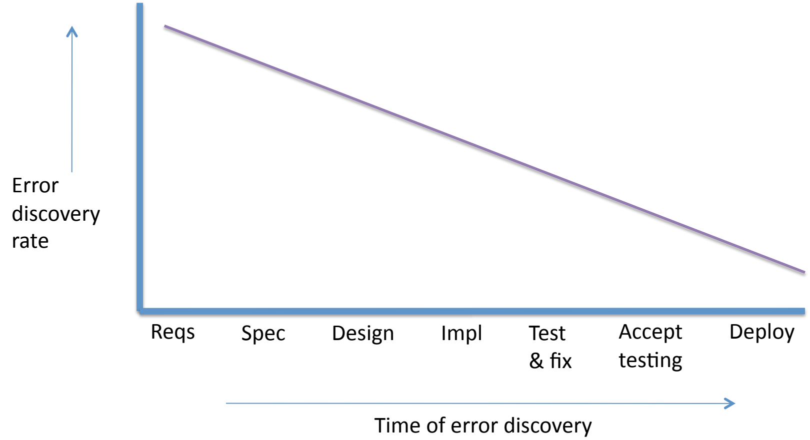
Cost of error fixes



Rate of error discovery

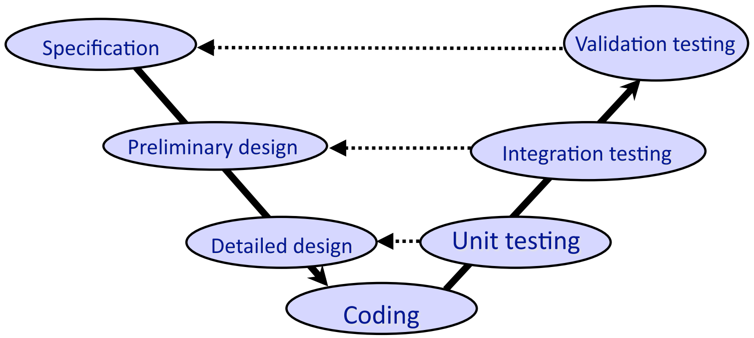


Reverse error identification rate!



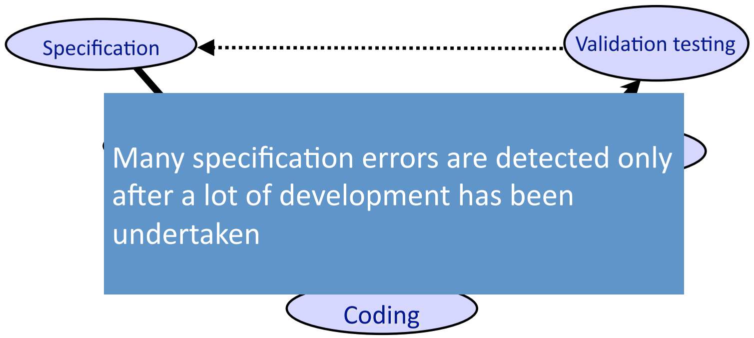
The V model

When are errors discovered in the V Model?



The V model

When are errors discovered in the V Model?



Many specification errors are detected only after a lot of development has been undertaken

Some sources of errors

- Lack of precision
  - Ambiguities
  - Inconsistencies
- Too much complexity
  - Complexity of requirements
  - Complexity of operating environment
  - Complexity of designs

Some sources of errors

- Lack of precision
  - Ambiguities
  - Inconsistencies
- Too much complexity
  - Complexity of requirements
  - Complexity of operating environment
  - Complexity of designs

Some preventive measures

- Early stage analysis
  - Precise descriptions of intent
  - Amenable to analysis by tools
  - Identify and fix ambiguities and inconsistencies as early as possible
- Mastering complexity
  - Encourage abstraction
  - Focus on what a system does
  - Early focus on key / critical features
  - Incremental analysis and design

Formal methods

- Rigorous techniques for formulation and analysis of systems
- They facilitate:
  - Clear specifications (contract)
  - Rigorous validation and verification

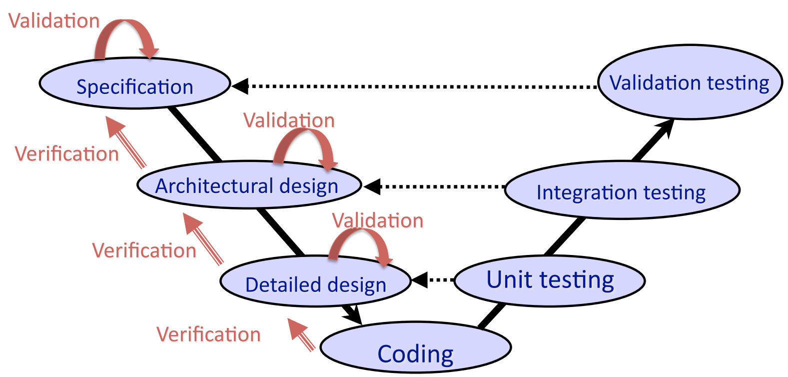
Validation: does the contract specify the right system?

- Answered informally

Verification: does the finished product satisfy the contract?

- Can be answered formally

Early stage analysis



Specifications and Programs

How can we relate specifications and computations?

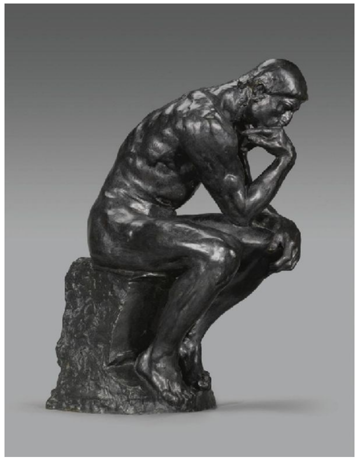
- Use a specification to build tests
- Use a specification to check that a program computes what it should (verification, model checking)
- Use a specification to compute (functional / logic / equational programming)
- Use specifications to generate the program (automatic code generation, correctness by construction)

How Can Guarantees be Given?

- Enlightened management: of little help.
- Convincing arguments beyond any reasonable doubt:
  - Formal basis.
  - Proofs based on rigorous methods.
- Carefully prove that programs will behave as expected.

How Can Guarantees be Given?

- Enlightened management: of little help.
- Convincing arguments beyond any reasonable doubt:
  - Formal basis.
  - Proofs based on rigorous methods.
- Carefully prove that programs will behave as expected.
- For **every** single program?



It's too Difficult for Humans to Do!

- Methodologies
- Mechanization
- Automation
- Computer-aided software development
  - Correctness by construction
  - Automatic analysis
  - Verification (model checking, deductive verification)
  - Automated testing

A Termination Problem: Collatz's Conjecture

This is just a humbling example. Not terribly useful by itself, but illustrative.

```
input n;

while n > 1 do
    if n mod 2 = 0 then
        n:= n / 2
    else
        n:= 3*n + 1
    end if
end while
```

Question: will it finish for any input value n?
Note: termination is often a basic property!

A Specification Example

```
procedure whoAmI(A: Array)
   repeat
     swapped := false
     for i := 1 to length(A) - 1 do
       if A[i-1] > A[i] then
         swap(A[i-1], A[i])
         swapped := true
       end if
     end for
   until not swapped
end procedure
```

- What does this program do?

A Specification Example

```
procedure whoAmI(A: Array)
   repeat
     swapped := false
     for i := 1 to length(A) - 1 do
       if A[i-1] > A[i] then
         swap(A[i-1], A[i])
         swapped := true
       end if
     end for
   until not swapped
end procedure
```

- What does this program do?
- Can you specify the property that characterizes a sorted array?

A Specification Example

```
procedure whoAmI(A: Array)
   repeat
     swapped := false
     for i := 1 to length(A) - 1 do
       if A[i-1] > A[i] then
         swap(A[i-1], A[i])
         swapped := true
       end if
     end for
   until not swapped
end procedure
```

- What does this program do?
- Can you specify the property that characterizes a sorted array?
- Can we prove that, after executing the code above, array A meets that property?

- Jean-Raymond Abrial.
  Faultless systems: Yes we can!
  IEEE Computer, 42(9):30–36, 2009.
- Jean-Raymond Abrial.
  Modeling in Event-B - System and Software Engineering.
  Cambridge University Press, 2010.