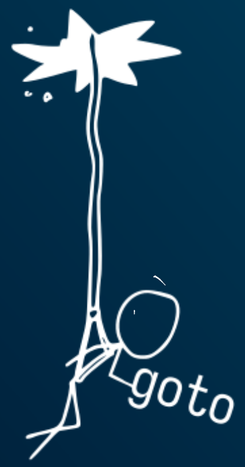
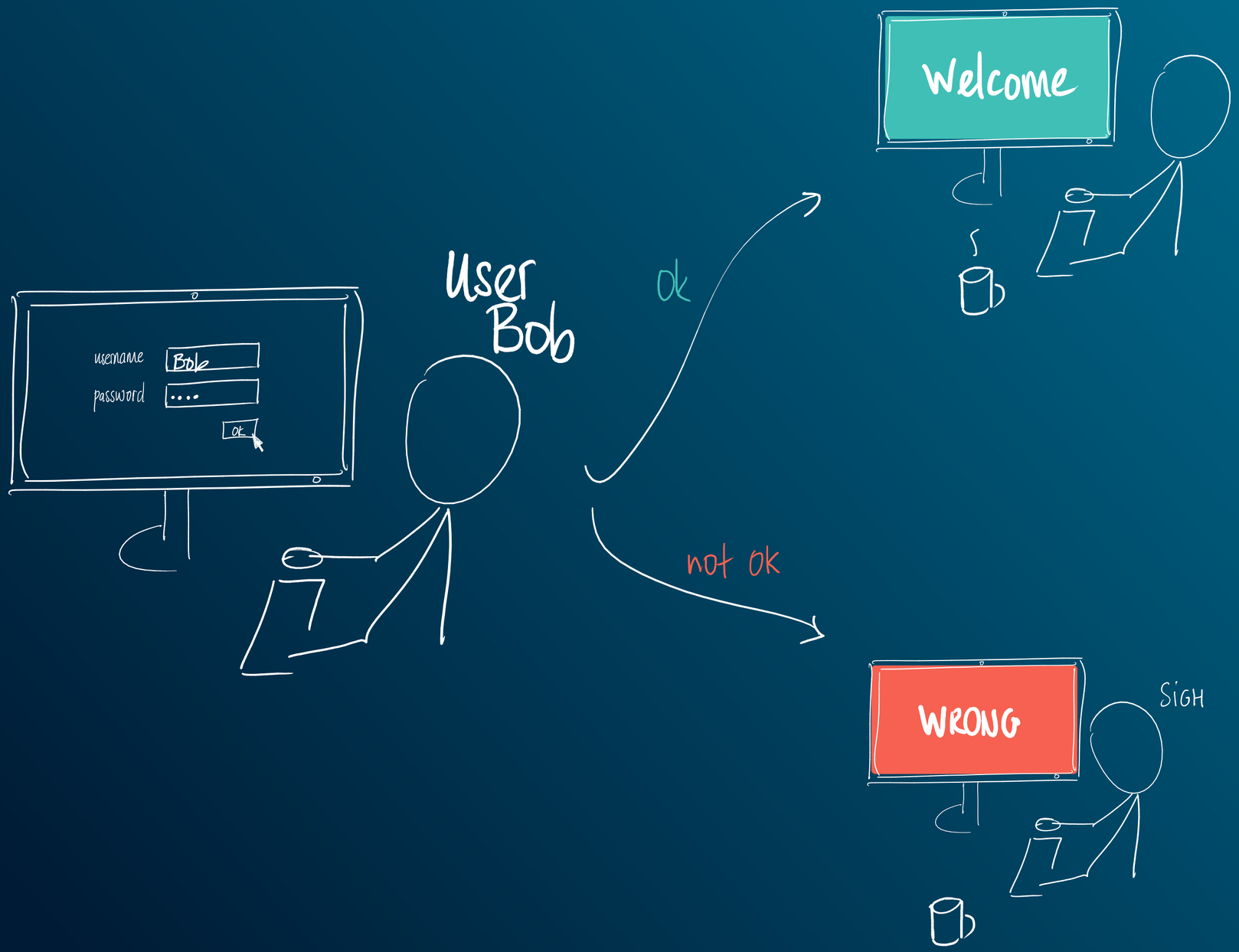
TU Delft



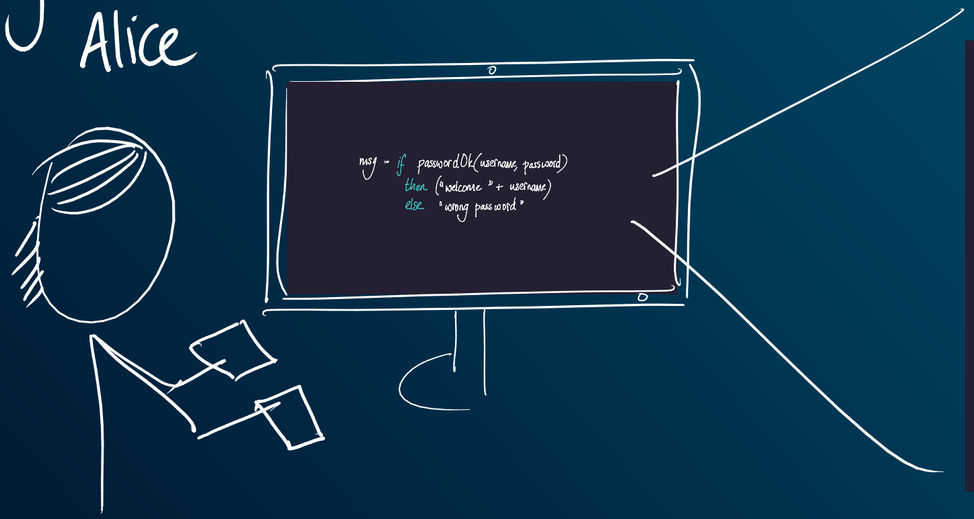
CORRECT BY CONSTRUCTION LANGUAGE IMPLEMENTATIONS

14 October 2021

Main ~~Characters~~ Nerds of this story...


Welcome
User
Bob
ok
username
Bob
password
....
ok
not ok
WRONG
SIGH

Progammer Alice




```
msg = if passwordOk(username, password)
      then ("welcome " + username)
      else "wrong password"
```

Language Developer
Ritchie

A **specification**

Language Implementation

```
msg = if passwordOk(username, password)
      then ("welcome " + username)
      else "wrong password"
```

Alice's program

(Type) Checker

✗

Inform Alice

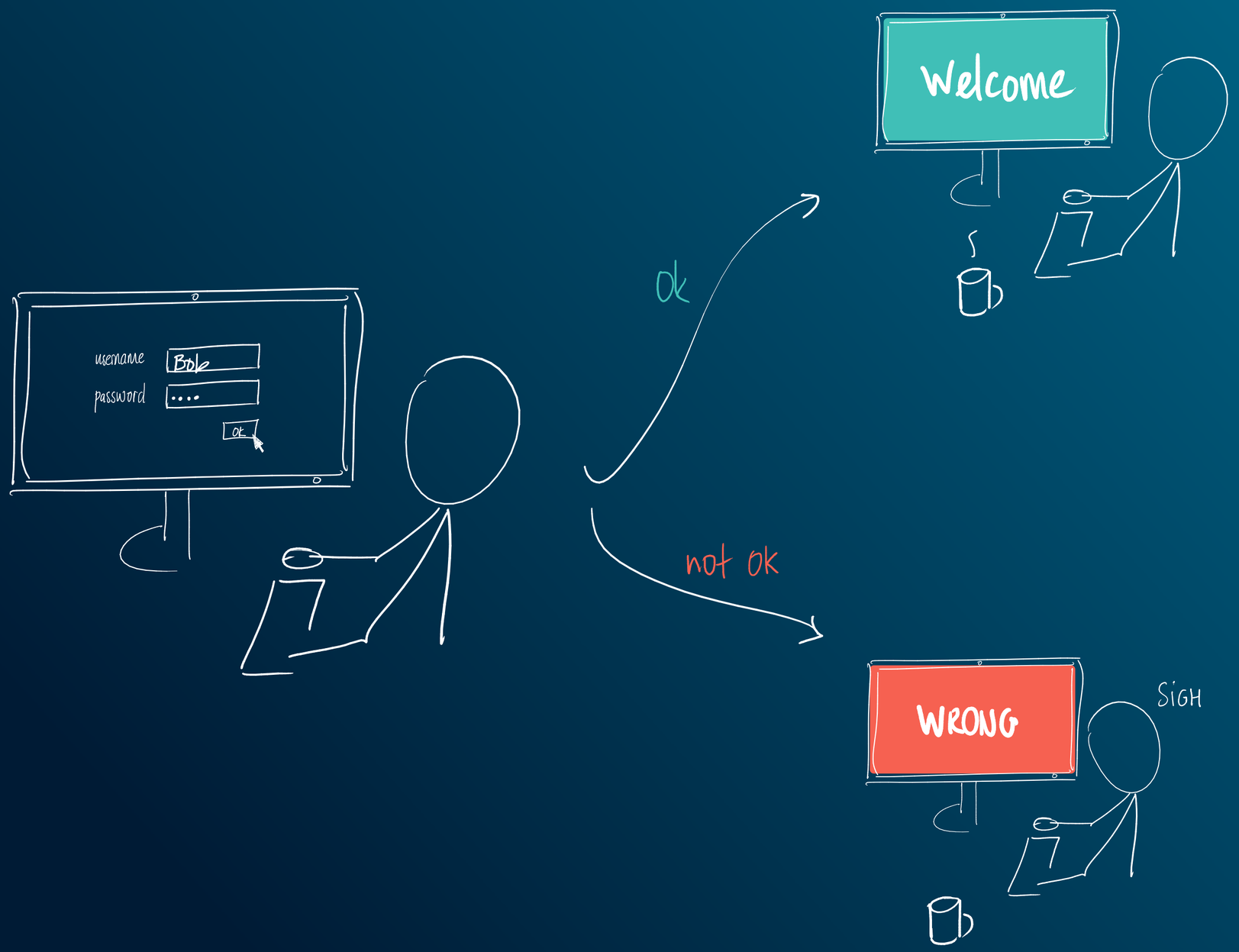
✓

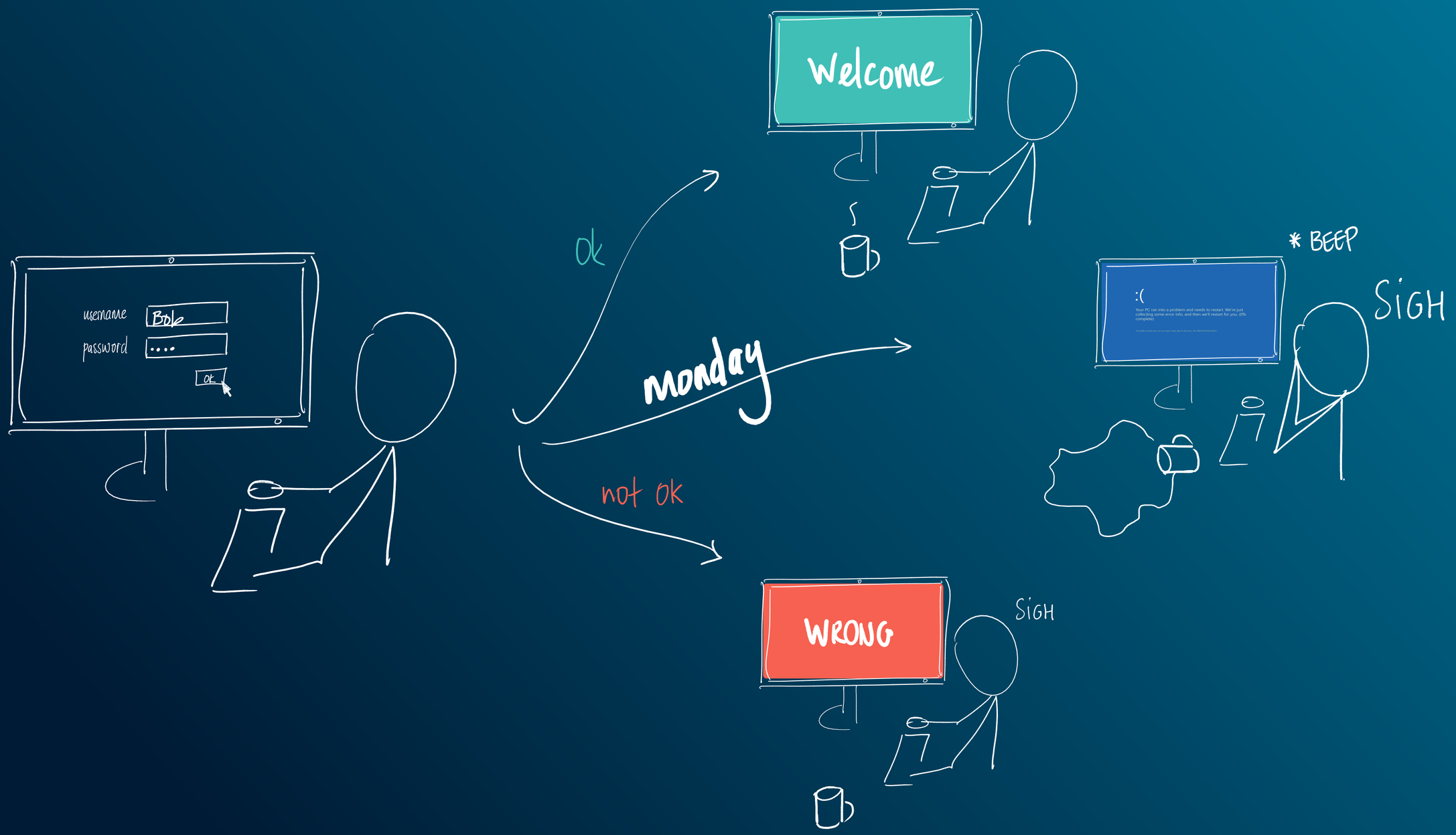
Interpreter

Compiler

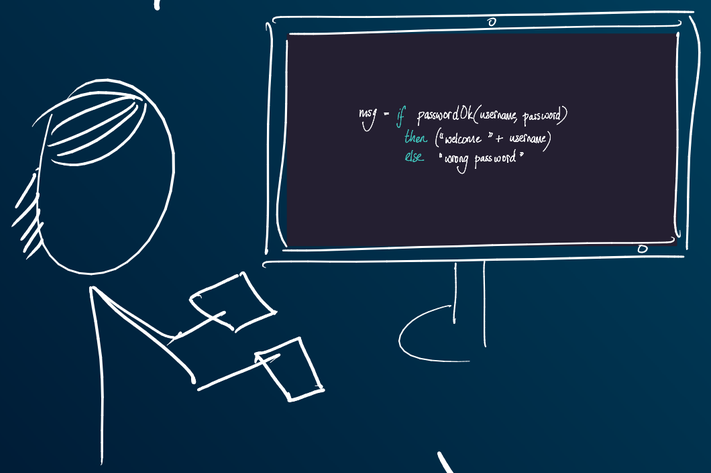
```
40: load  rbp
    mov   rbp esp
    sub
    jmp   42
41: ite
```

instructions for Bob's computer

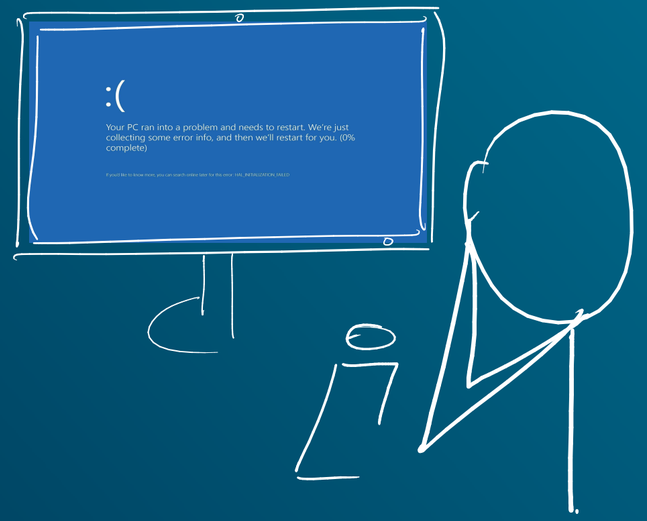

username
Bob
password
....
ok
ok
not ok
Welcome
WRONG
SIGH


username
Bob
password
....
ok
ok
monday
not ok
Welcome
WRONG
SIGH
* BEEP
:(
Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you. (0% complete)
SIGH

Did you read the manual

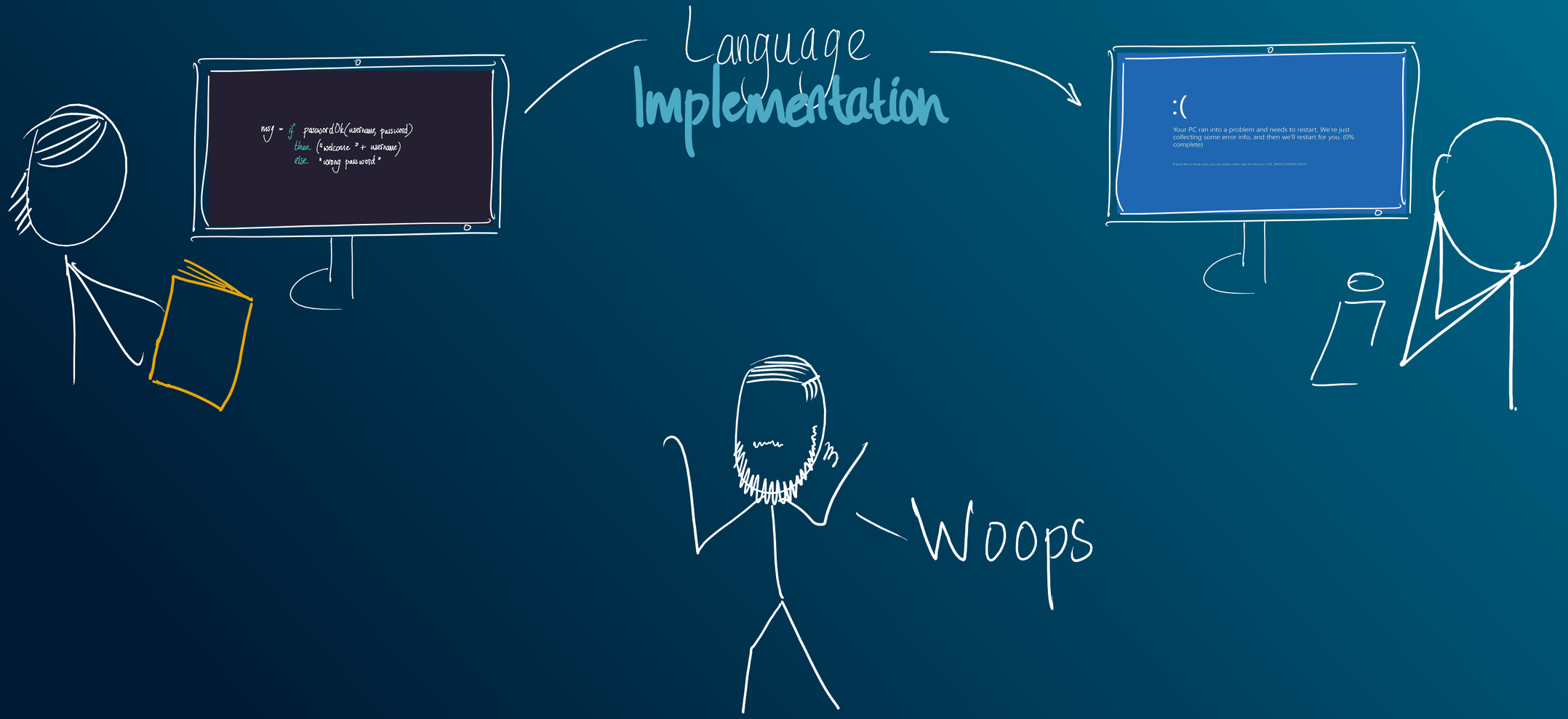


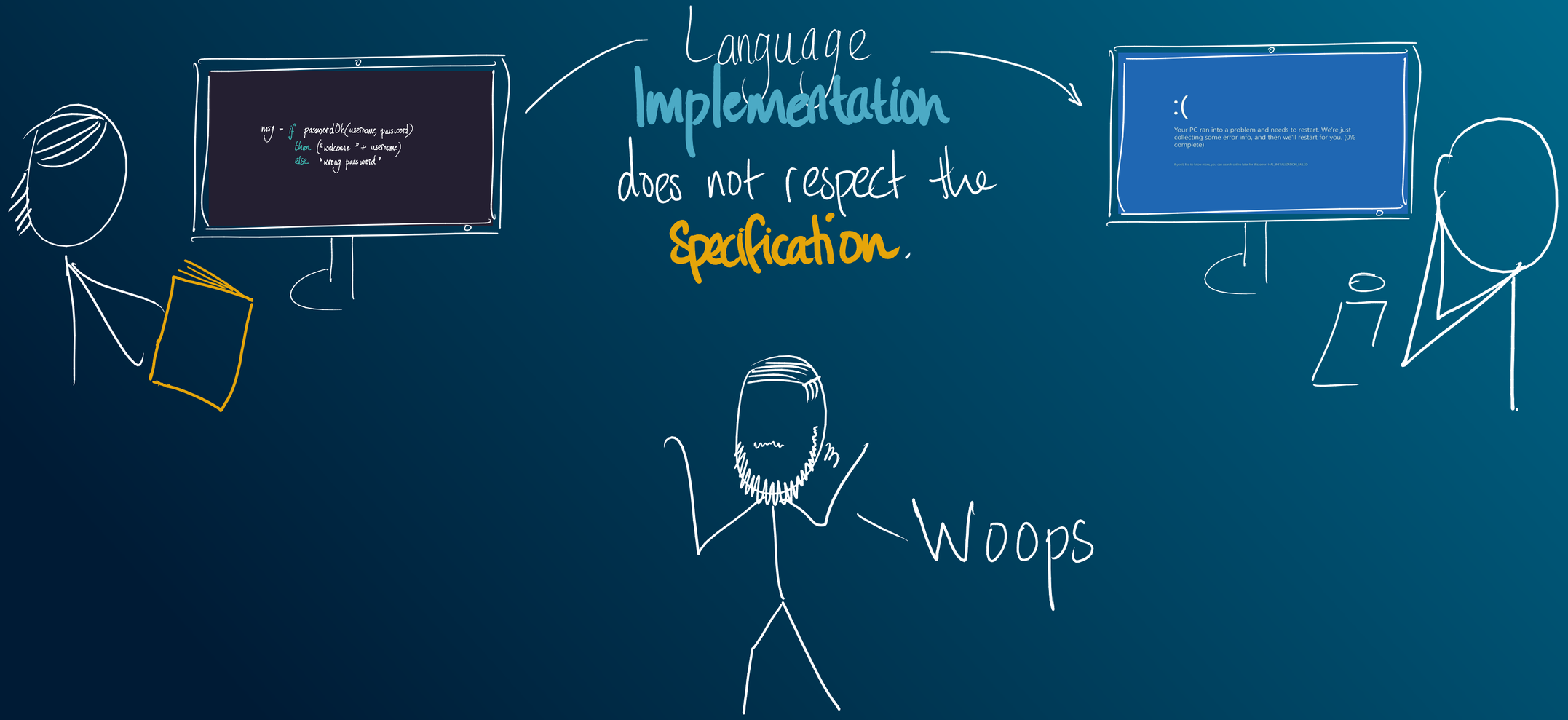
No?

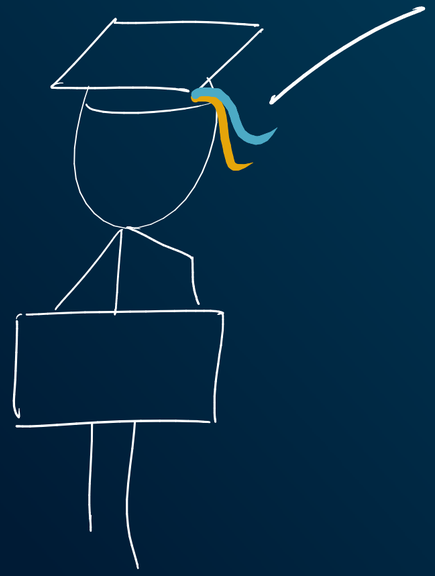


Have you turned it off and on again?

...yes!


msg = if passwordOk(username, password)
then ("welcome " + username)
else "wrong password"
Language
Implementation
:(
Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you. (0% complete)
Woops


msg = if passwordOk(username, password)
then ("welcome " + username)
else "wrong password"
Language
Implementation
does not respect the
Specification.
:(
Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you. (0% complete)
If you'd like to know more, you can search online later for this error: YAG_INTERLOCKING_DEED
Woops

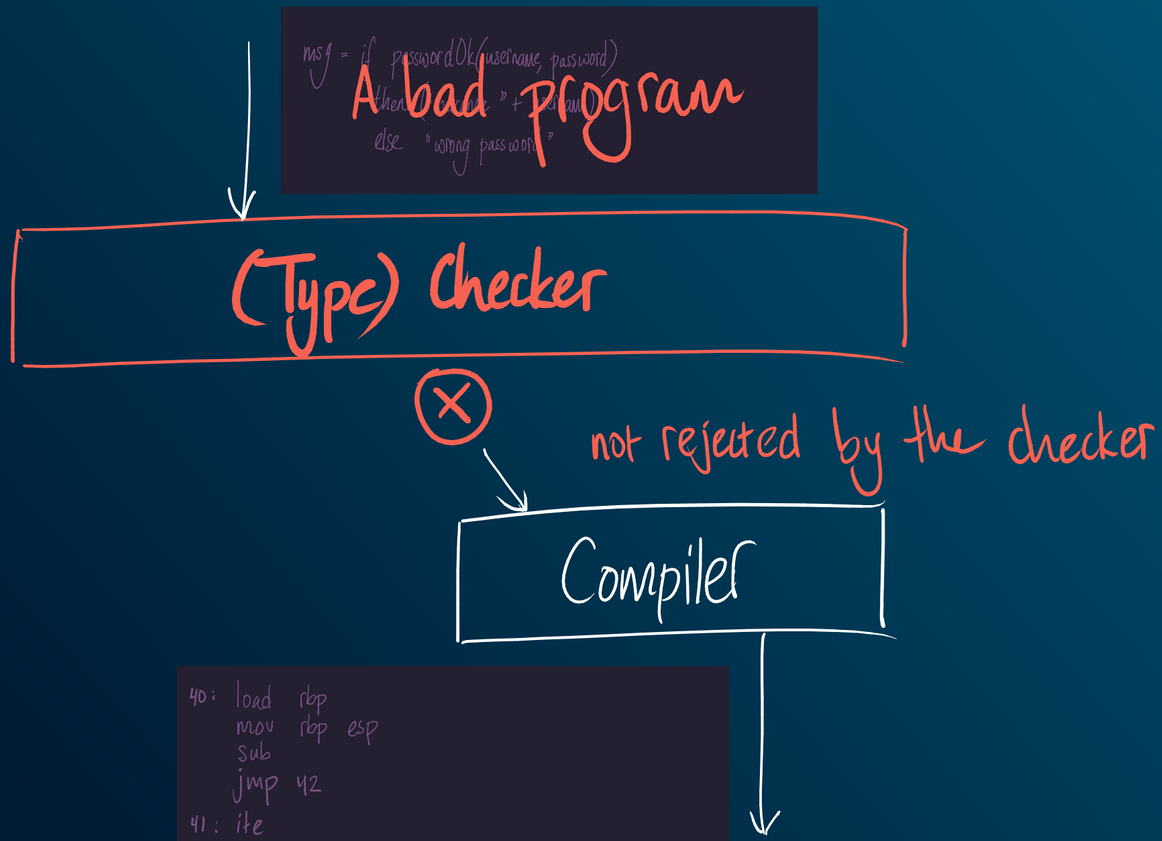


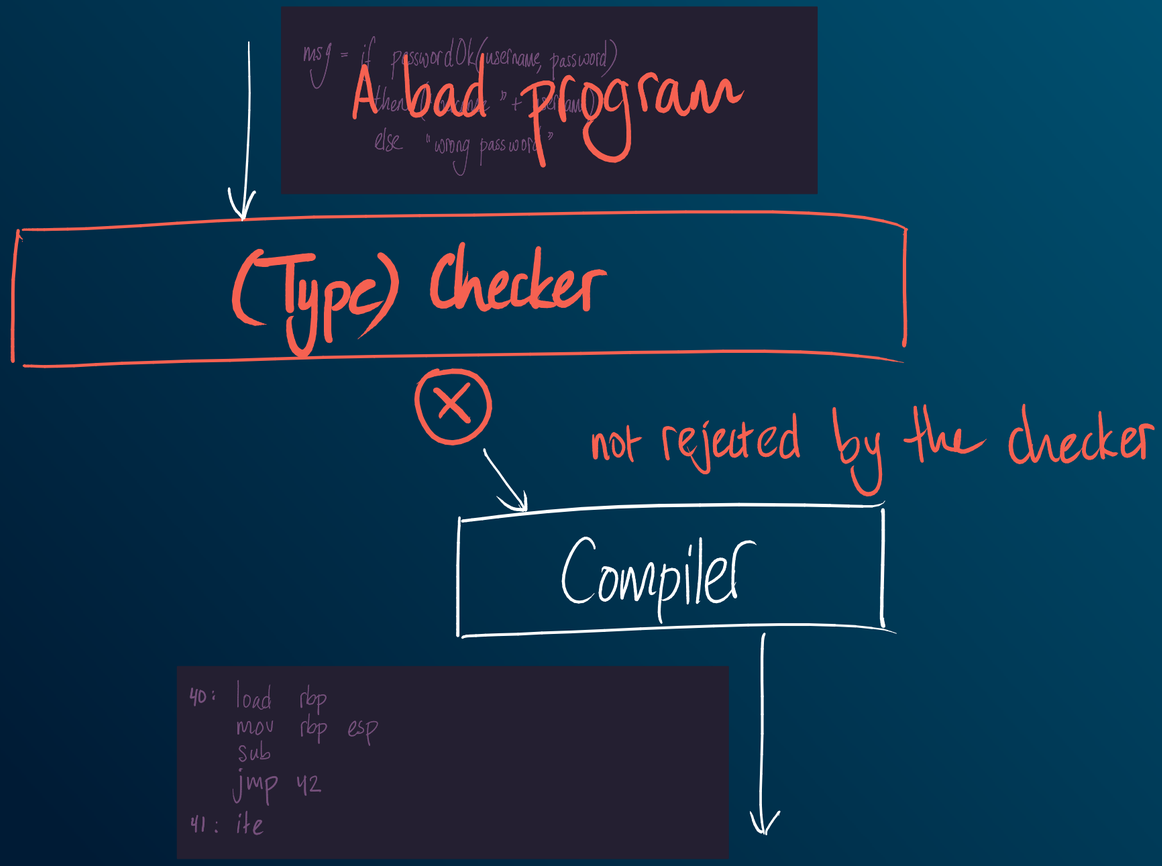
My dissertation is about

Methods for developing Implementations

correct with respect to the Specification.

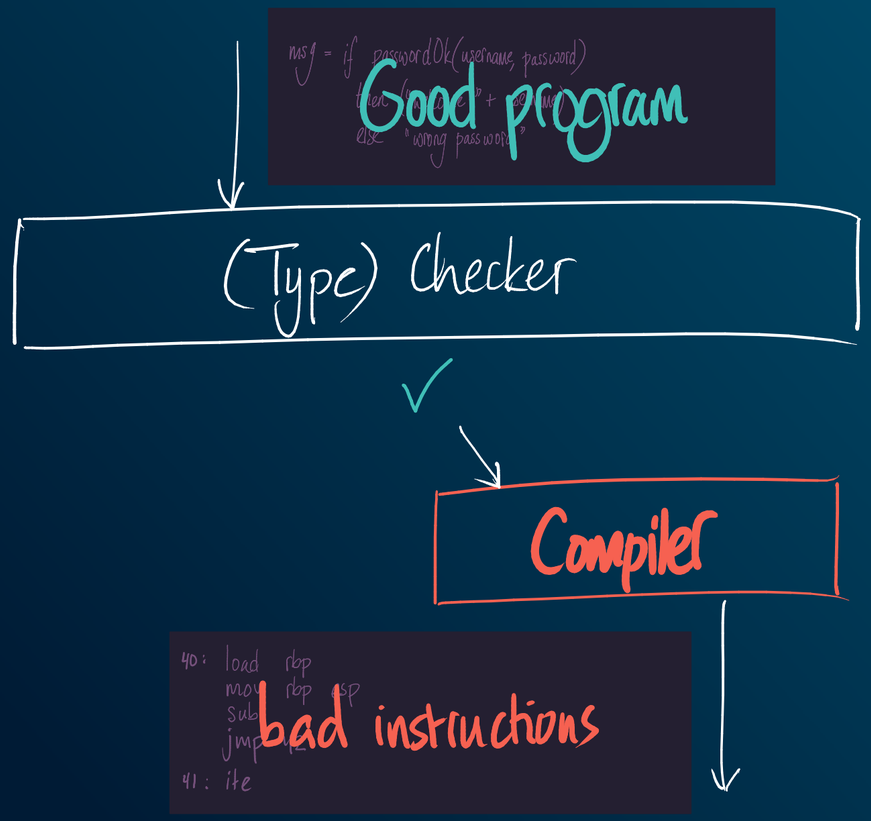
How can Language Implementations go wrong?

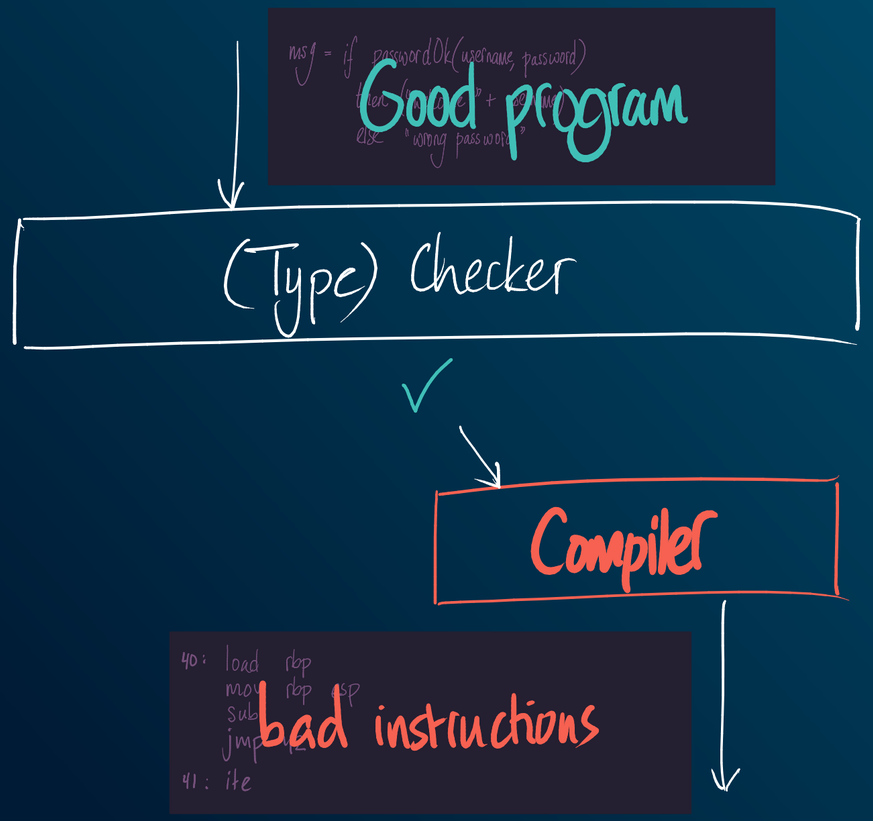

msg = if passwordOk(username, password)
A bad program
else "wrong password"
(Type) Checker
not rejected by the checker
Compiler
40: load rbp
mov rbp esp
sub
jmp 42
41: ite



Part II
of the thesis

Correct Language Frontends


msg = if passwordOk(username, password)
Good program
(Type) Checker
Compiler
40: load rbp
mov rbp rsp
sub
jmp
41: ite
bad instructions

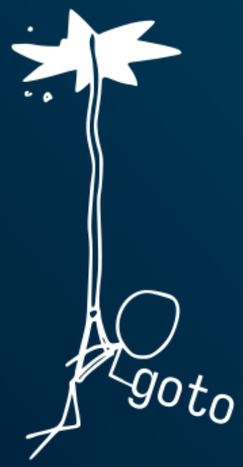


Part I
of the thesis
(my favorite part)

Correct Language Backends

TU Delft

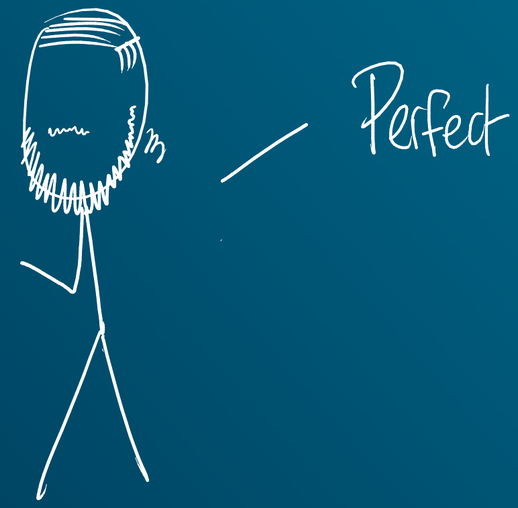
CORRECT BY CONSTRUCTION LANGUAGE IMPLEMENTATIONS



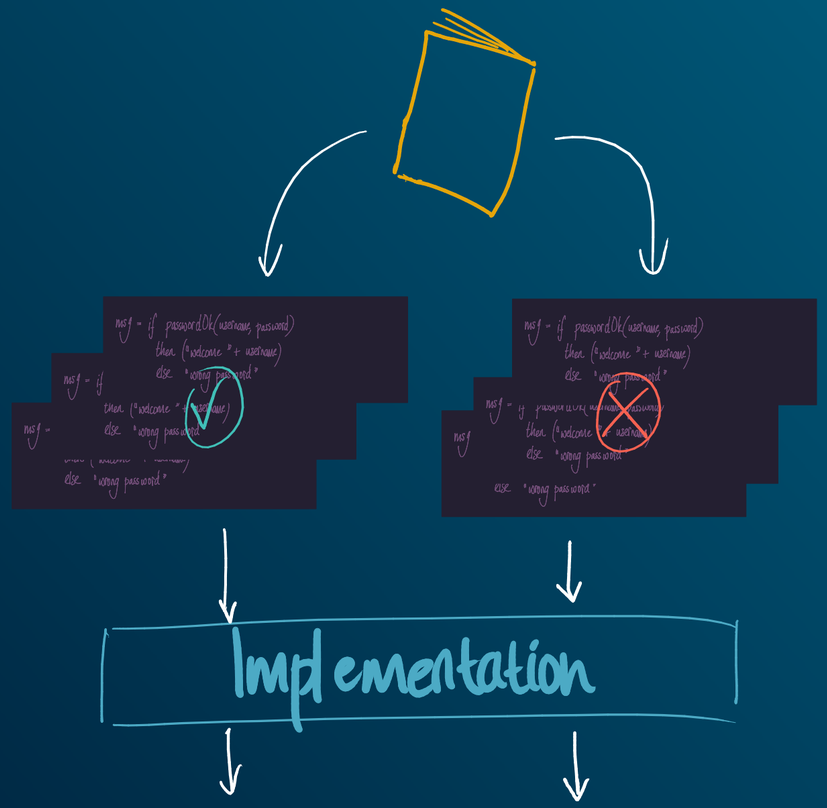
... by construction?

Certainly!

How do we verify that Implementations go right?

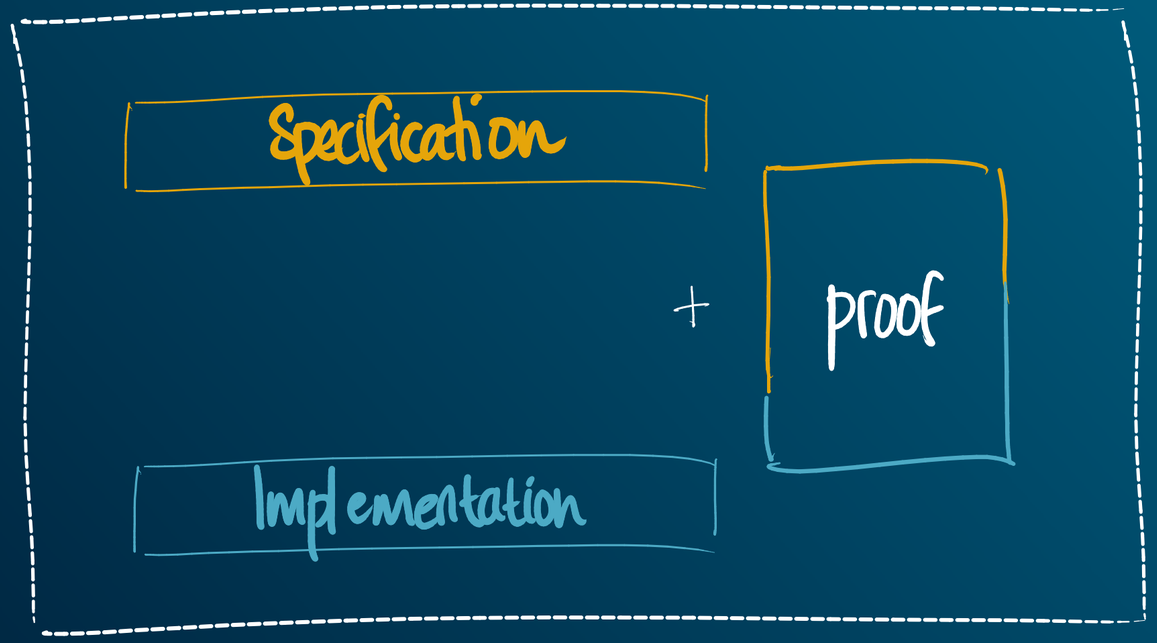


Verification by Testing



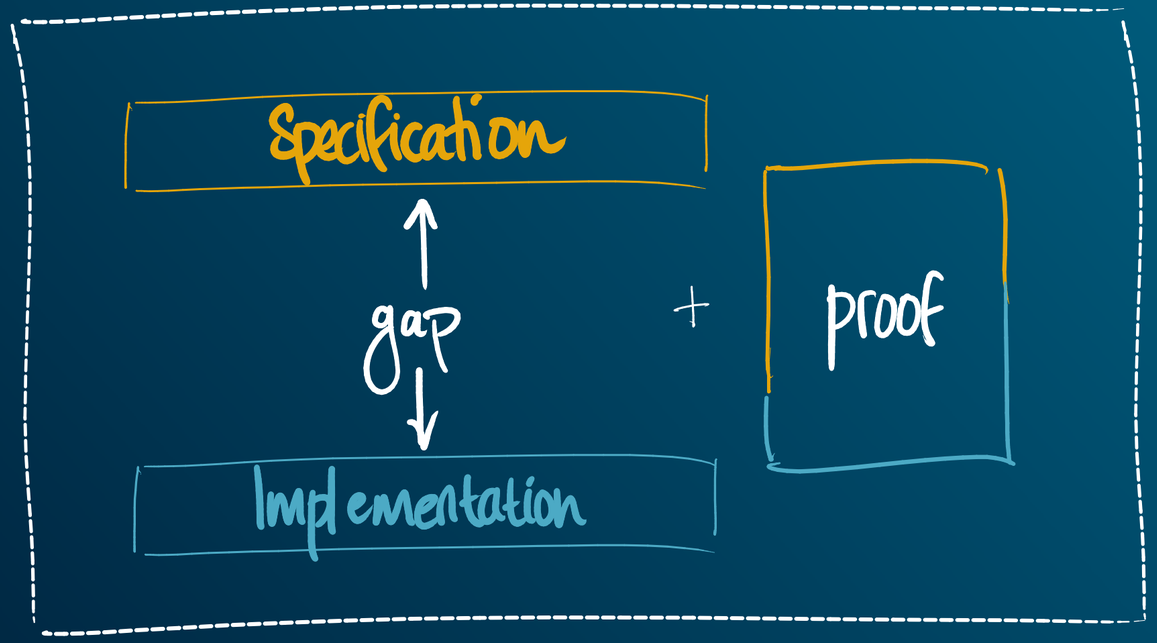
Compare result with reference

Formal Verification



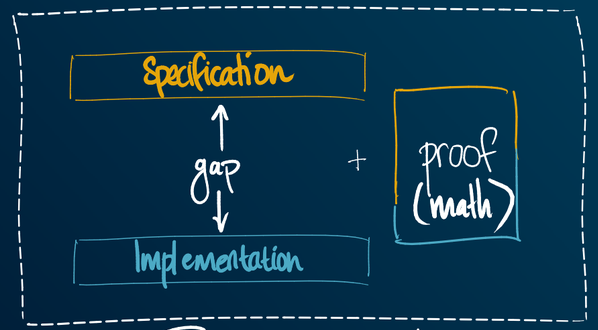
Proof Assistant

Formal Verification

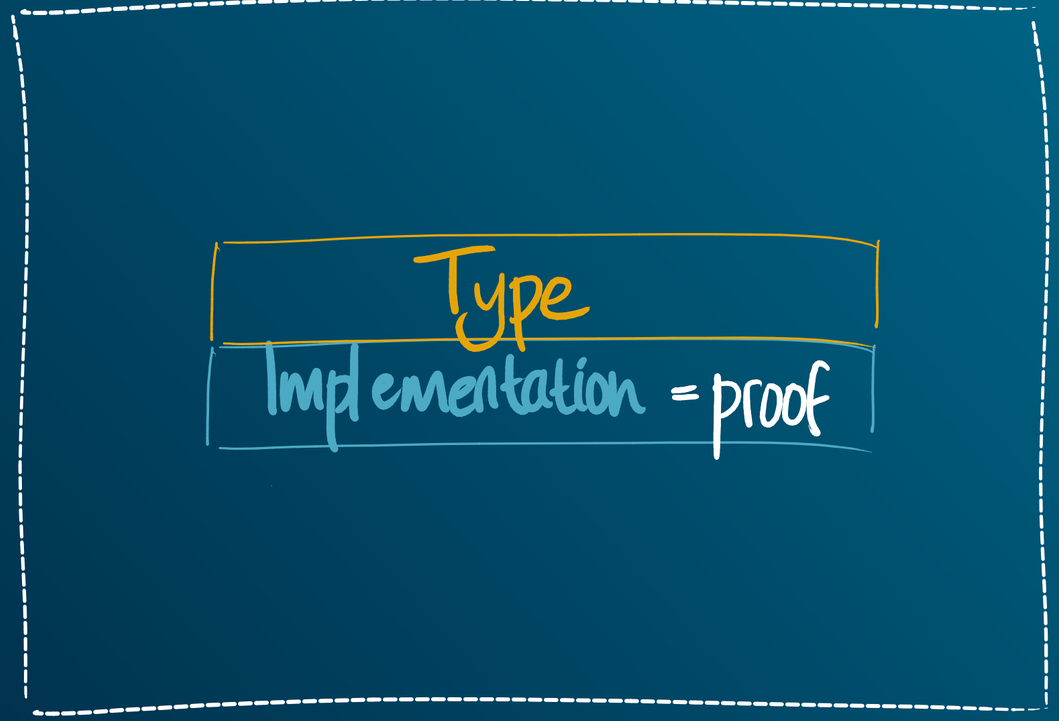


Proof Assistant

Correct by Construction Programming

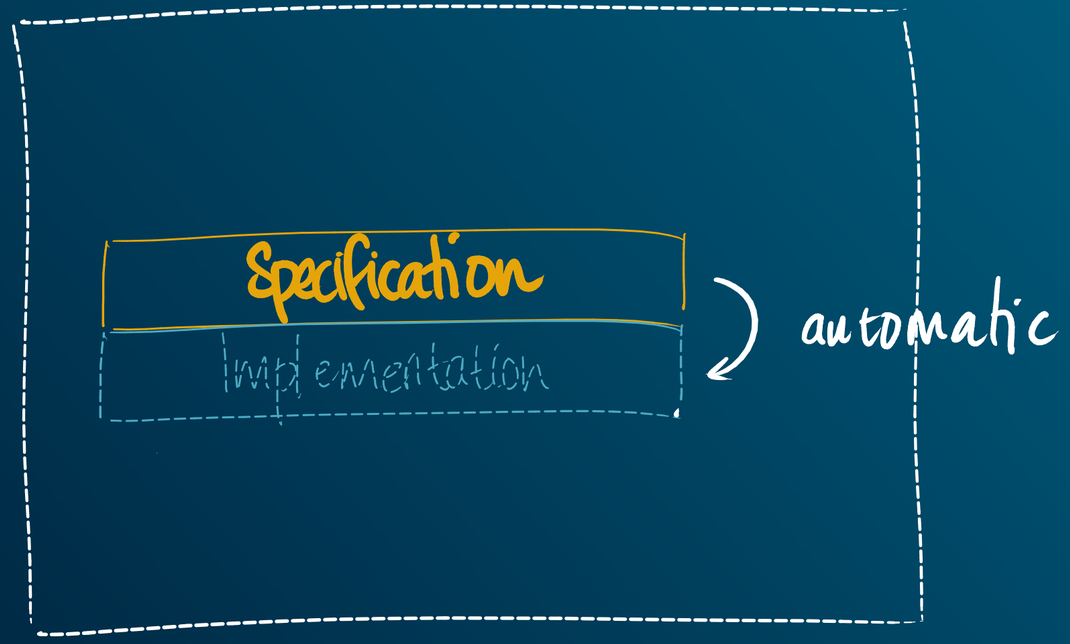


Proof Assistant

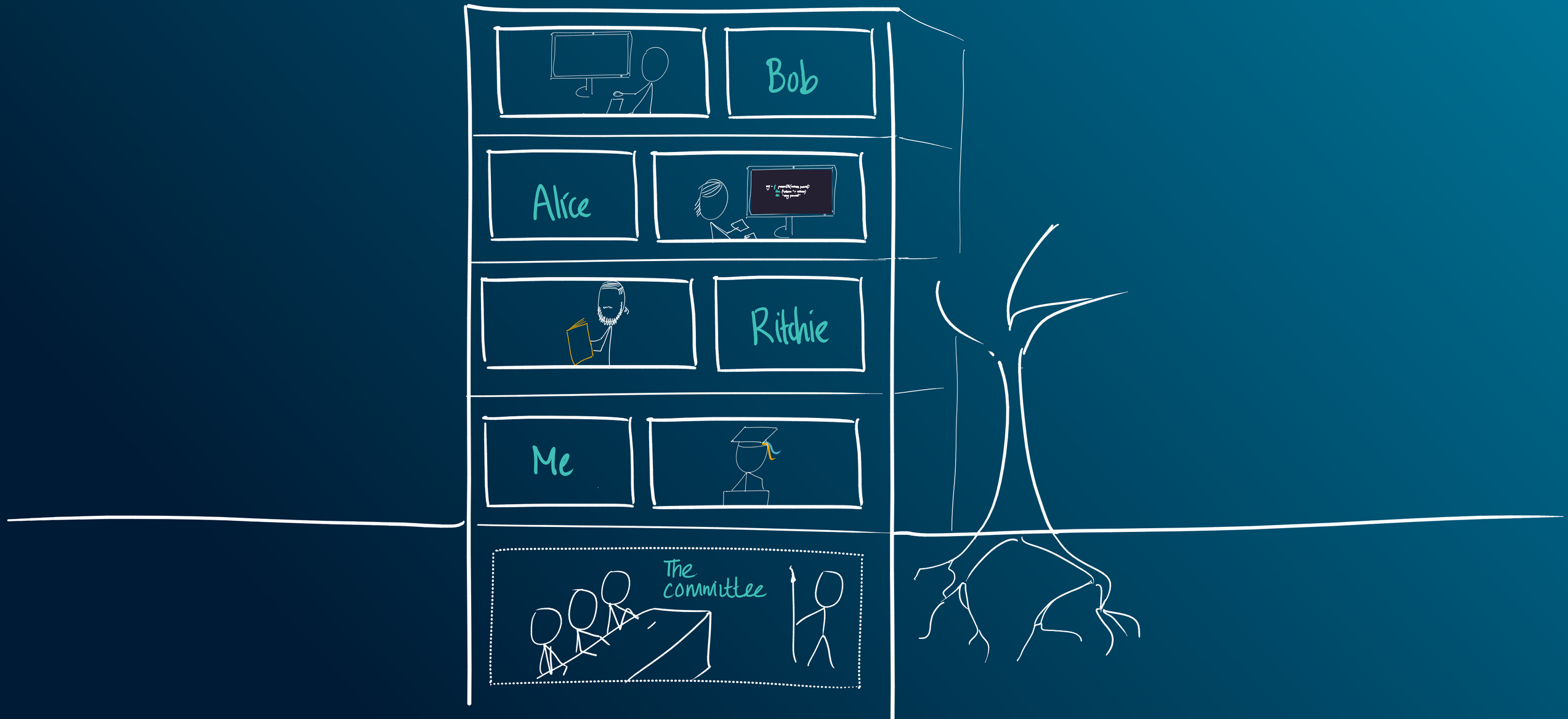


Functional Programming language

Generating correct implementations



Statix


Bob
Alice
Ritchie
Me
The committee

TU Delft

CORRECT BY CONSTRUCTION LANGUAGE IMPLEMENTATIONS