Software Quality

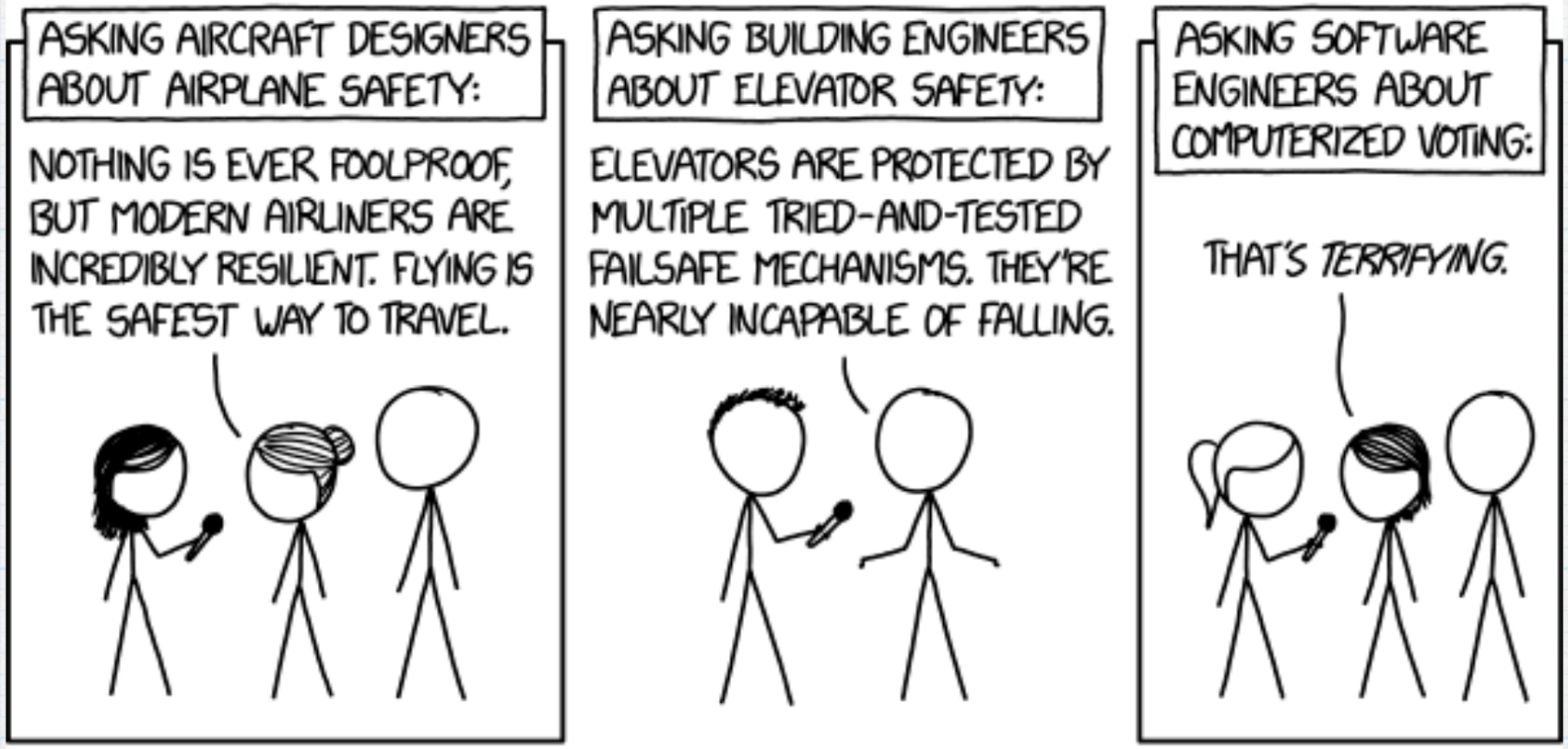
Spring 2020

About Me

* George Lesica
* Senior Software Engineer in Travis Wheeler's lab
* Previously at Workiva
* Occasional teacher, conference presenter
* Believer that software can (and should) be less awful
* https://www.lesica.com

Quality?


BUGS
BUGS EVERYWHERE



https://xkcd.com/2030/

So, now what?

That's... complicated.

* Software testing
* New languages and compilers
* Static analysis
* Improved processes

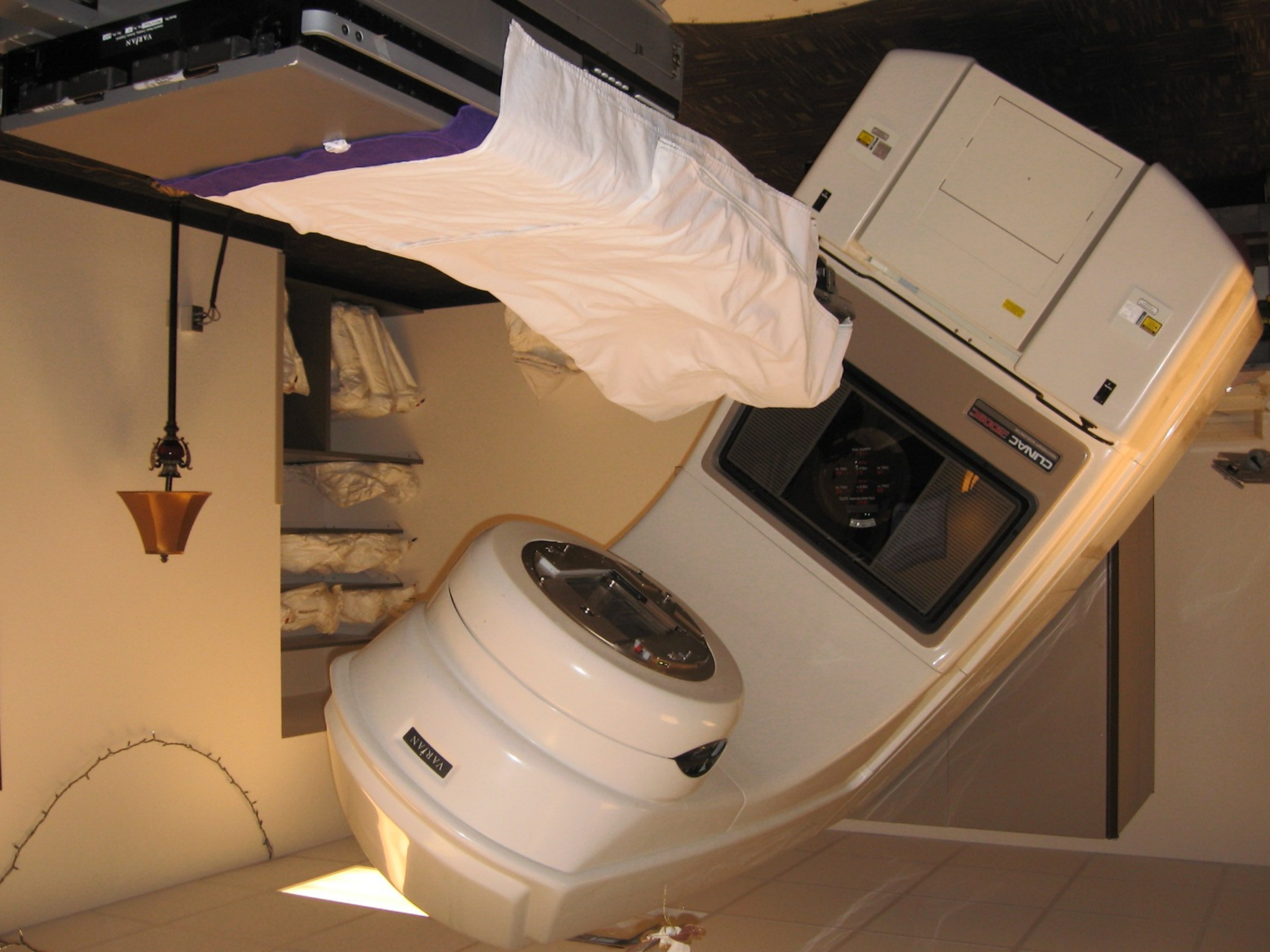
Software Testing

Manual Testing

* How we all tested our first "Hello, World" programs
* Run it, use it, see if it does the right thing
* Give it to someone else to run and use, ask them if it did the right thing
* If you're a AAA game studio, sell it to millions of people and see what happens

Automated Testing

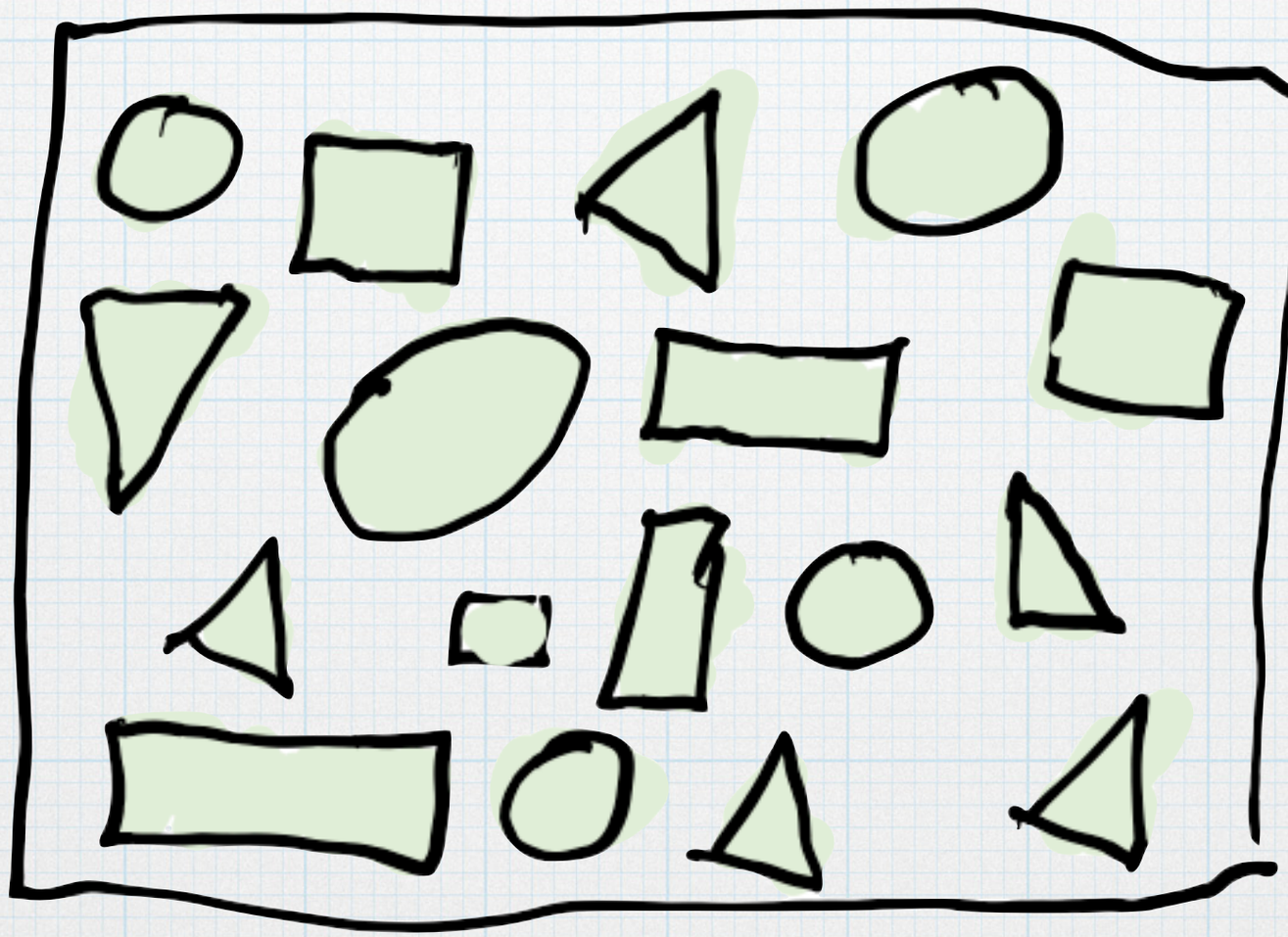
* A whole lot less boring
* Much, much faster (if you do it right)
* Repeatable and more reliable
* Incidentally, also quite a bit cheaper


VARIAN
VARIAN
CLINAC 2100CD

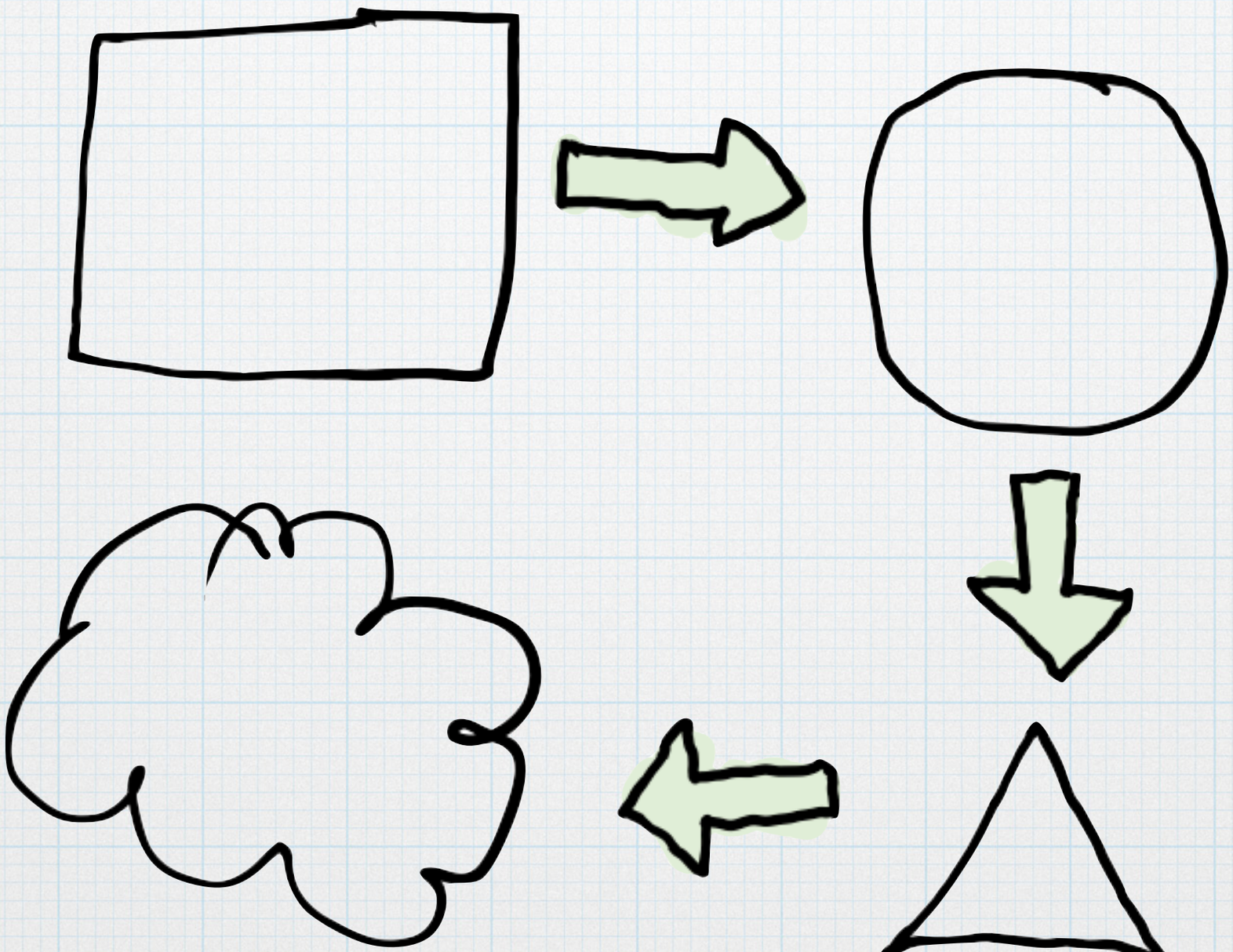
"A commission attributed the primary cause to general poor software design and development practices rather than single-out specific coding errors. In particular, the software was designed so that it was realistically impossible to test it in a clean automated way."

— Nancy Levenson

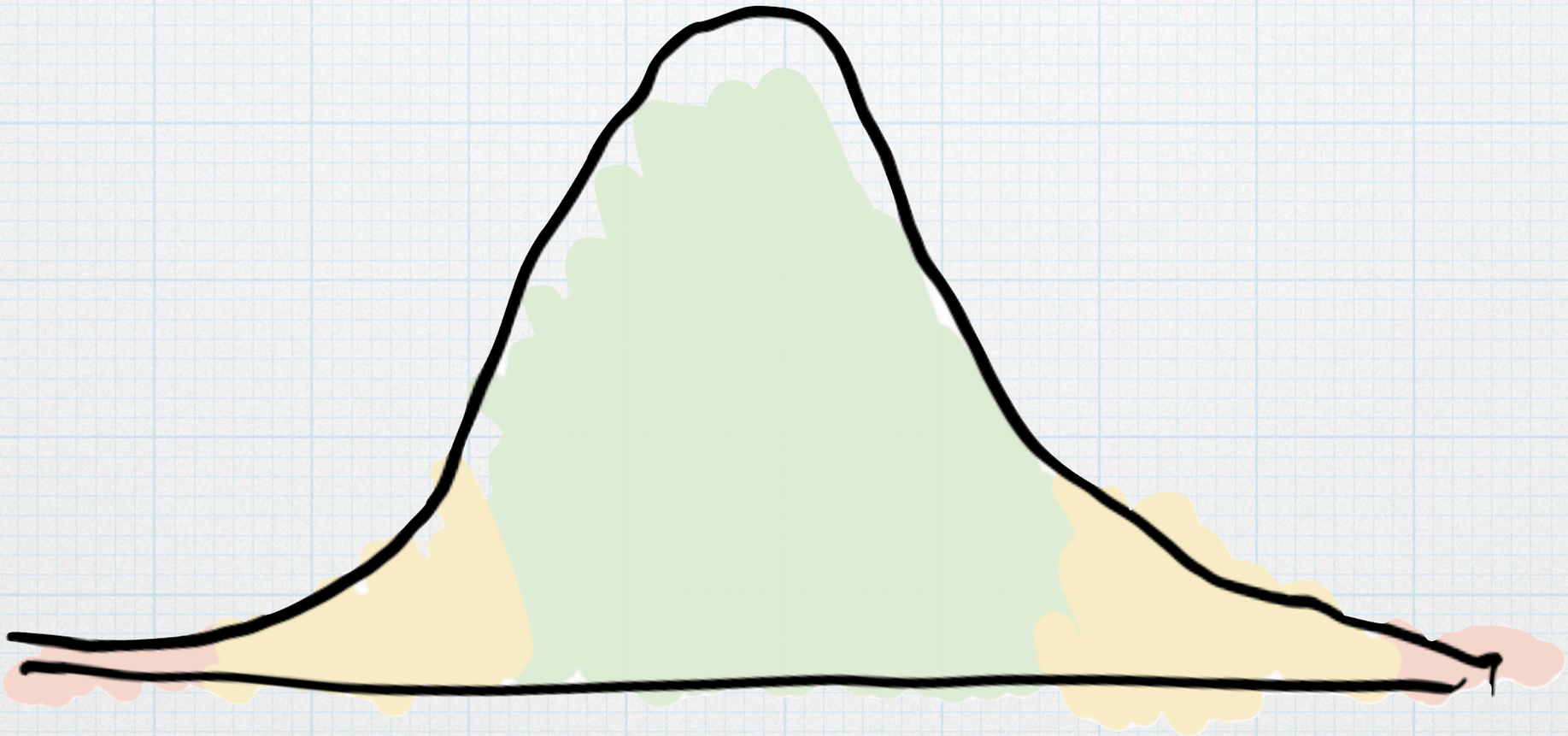
Unit Testing



Integration Testing

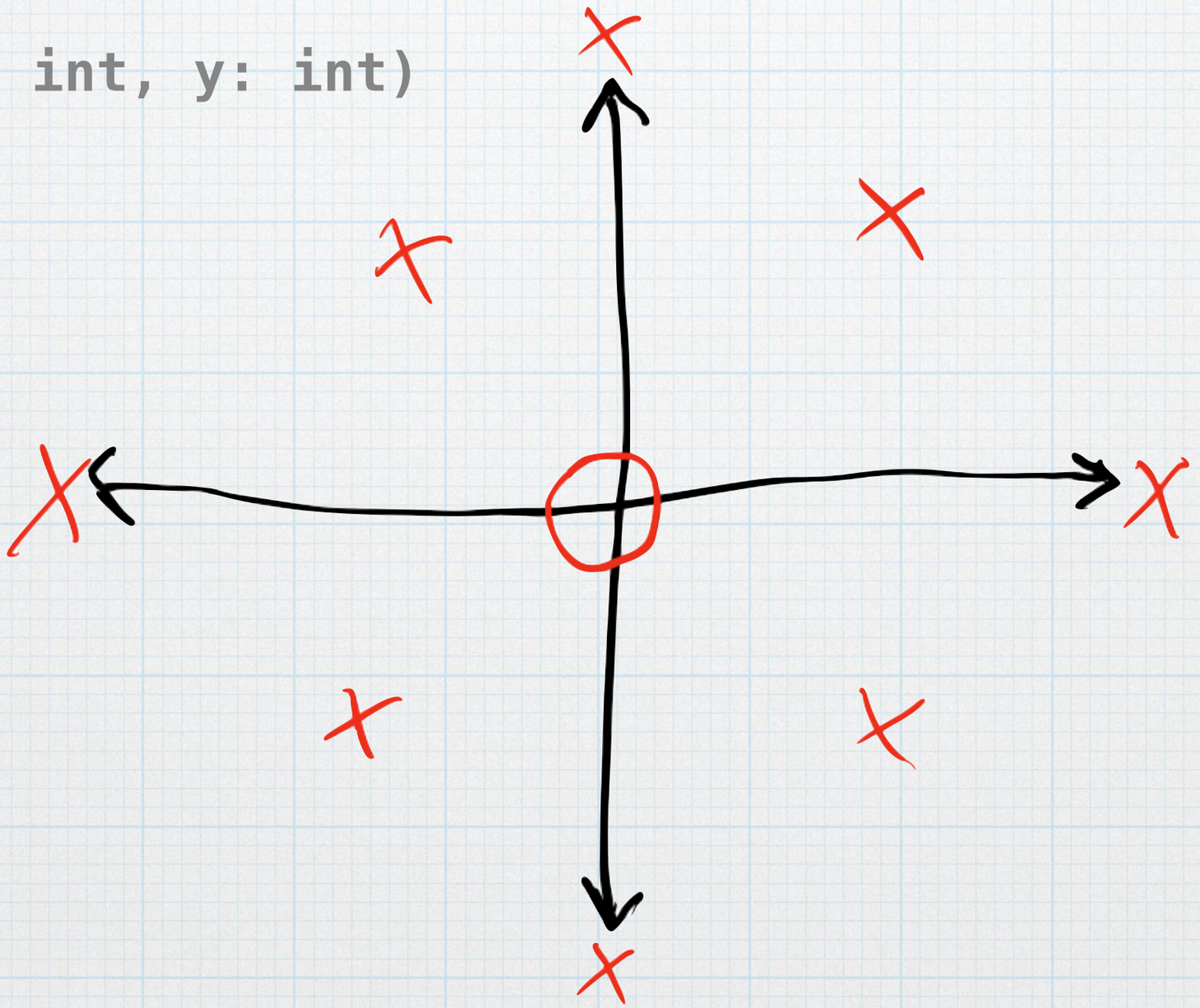


What To Test



Good Test Cases

```
def foo(x: int, y: int)
```



Slice Endpoint

```
@values = ("a", "b", "c", "d", "e");
$start = 1;
$end = 3;
print @values[$start .. $end];
```

```
values = ["a", "b", "c", "d", "e"]
start = 1
end = 3
print(values[start:end])
```

"Always, ALWAYS test zero. Seriously."

— Anonymous

New Languages and Compilers

Null Safety

```
class Main {
  private static void sayHello(String name) {
    if (name.startsWith("George")) {
      System.out.println("Hey, George! You're the best!");
      return;
    }

    System.out.println("Oh, hey there " + name + ".");
  }

  public static void main(String[] args) {
    sayHello("George");
    sayHello("Allison");
    sayHello(null);
  }
}
```

Rewrite in Kotlin

```
fun main() {
    sayHello("George")
    sayHello("Allison")
    sayHello(null)
}

fun sayHello(name: String) {
    if (name.startsWith("George")) {
        println("Hey, George! You're the best!")
        return
    }
    println("Oh, hey there ${name}.")
}
```

Memory Safety

```
#define P_CREATE 1
#define P_DELETE 1 << 1
#define P_ADMIN 1 << 2

typedef struct {
    char name[8];
    uint8_t role;
} t_user;

int main(int argc, char **argv) {
    t_user *user = malloc(sizeof(t_user));
    user->role = atoi(argv[2]);
    for (int i = 0; i < strlen(argv[1]); i++) {
        user->name[i] = argv[1][i];
    }
    if (user->role & P_ADMIN) {
        printf("ADMIN");
    } else {
        printf("NOT ADMIN");
    }
}
```

It Works!

```
$ ./unsafe "george" 0
P_CREATE : 1
P_DELETE : 2
P_ADMIN  : 4

id   : george
role : 0

NOT ADMIN
```

Pwned 😔

```
$ ./unsafe "george00$(echo -e "\0004")" 0
P_CREATE : 1
P_DELETE : 2
P_ADMIN  : 4

id   : george00
role : 4

ADMIN
```

Idris

```
app : Vect n a -> Vect m a -> Vect (n + m) a
app Nil       ys = ys
app (x :: xs) ys = x :: app xs ys
```


OT

Static Analysis

Guess That Value

==	0	false	''	null	undefined	" \t\r\n"	'0'	'false'
0	true	true	true	false	false	true	true	false
false	true	true	true	false	false	true	true	false
''	true	true	true	false	false	false	false	false
null	false	false	false	true	true	false	false	false
undefined	false	false	false	true	true	false	false	false
" \t\r\n"	true	true	false	false	false	true	false	false
'0'	true	true	false	false	false	false	true	false
'false'	false	false	false	false	false	false	false	true

https://martin-thoma.com/javascript-wtf/

https://github.com/denysdovhan/wtfjs

Domain Mismatch

* Sometimes an int isn't just an int
  * Strictly positive values
  * Units (inches, centimeters)
  * Even or odd numbers
* Enums instead of magic strings or ints

Improved Units

```
// This version will accept any float values
// but many of those values don't make sense.
let hypotenuse w h = sqrt (w * w + h * h)

// This version prevents mixing up English and
// metric length units, although it does the
// conversion implicitly which might be unwise.
type Length = In of float | CM of float

let hypotenuse_units w h =
  match (w, h) with
    | (In wi, In hi) -> In (hypotenuse wi hi)
    | (CM wc, CM hc) -> CM (hypotenuse wc hc)
    | (In wi, CM hc) -> CM (hypotenuse (wi * 2.54) hc)
    | (CM wc, In hi) -> CM (hypotenuse wc (hi / 2.54))


printfn "Dangerous: %f" (hypotenuse 4.0 5.0)
printfn "Safer    : %O" (hypotenuse_units (In 4.0) (In 5.0))
```

Improved Processes

"There are two levels of code inspection, or "eyeballing" the software looking for logic errors. One level of inspection is by the coders themselves and their peer reviewers. The second level is done by the outside verification team."

— "Computers in the Space Shuttle Avionics System"

https://www.history.nasa.gov/computers/Ch4-5.html

Goto Fail

```
if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
  goto fail;
  goto fail;
// …other checks…
fail:
  // …buffer frees (cleanups)…
  return err;
```

https://blog.codecentric.de/en/2014/02/curly-braces/

NO NEED TO DOUBLE CHECK THIS CHANGE LIST, IF SOME PROBLEMS REMAIN THE REVIEWER WILL CATCH THEM.

NO NEED TO LOOK AT THIS CHANGE LIST TOO CLOSELY, I'M SURE THE AUTHOR KNOWS WHAT HE'S DOING.

MANU

737 MAX Debacle

https://arstechnica.com/information-technology/2018/11/indonesia-737-crash-caused-by-safety-feature-change-pilots-werent-told-of/

https://www.seattletimes.com/business/boeing-aerospace/black-box-data-reveals-lion-air-pilots-struggle-against-boeings-737-max-flight-control-system/

Software download failed. Do you want to Retry?

OK

Apps

Media

Settings

https://www.makeuseof.com/tag/worst-programming-mistakes-in-history/

"If debugging is the process of removing bugs, then programming must be the process of putting them in."

— Edsger Dijkstra