SCOPE Lab mission:

How can we help developers build better software more easily?

- *more reliable*
- *faster*
- *more energy efficient*

- *automatic verification*
- *automatic debugging*
- *automatic synthesis*

Implementation Level

Verification Is the code correct? **(No.)**

```
Faulty reverse list method:
class List {
   Node head;

   void reverse() {
      Node near = head;
      Node mid = near.next;
      Node far = mid.next;
      near.next = far;

      while (far != null) {
         mid.next = near;
         near = mid;
         mid = far;
         far = far.next;
      }

      mid.next = near;
      head = mid;
   }
}
class Node {
   Node next;
   String data;
}
```

Which line(s) of code are incorrect? **Debug**

Synthesis How can we correct the faulty code?

```
near.next = ??;
@post-condition:
all n : Node | n.next = n.~next'
```

```
near.next = null;
```

Everyday we rely on complex software systems that may be faulty

Transportation | Financial | Entertainment | Social | Health | Exploration

Copy Pasta

Knight Capital Group suddenly forgot how to trade stock.

Between 9:30 a.m. and 10 a.m. EST on August 1, the company's trading algorithms decided to buy high and sell low on stocks. KCG ***lost $440 million in 30 minutes*** on trades.

Cause: a technician forgot to copy the new Retail Liquidity Program (RLP) code and ended up triggering a flag for left over, defective "Power Peg" trading code

Design Oversight

World Of Warcraft creates literal computer virus.

Wrold boss Hakkar hit players with a "Corrupted-Blood" virus that would kill off weaker characters. The virus was supposed to be contained to Hakkar's kingdom. **It wasn't.** Resulting in a **1,000+ "deaths"**

Cause: An oversight that allowed pets and minions to take the affliction out of its intended confines. By both accidental and purposeful intent, a pandemic ensued.

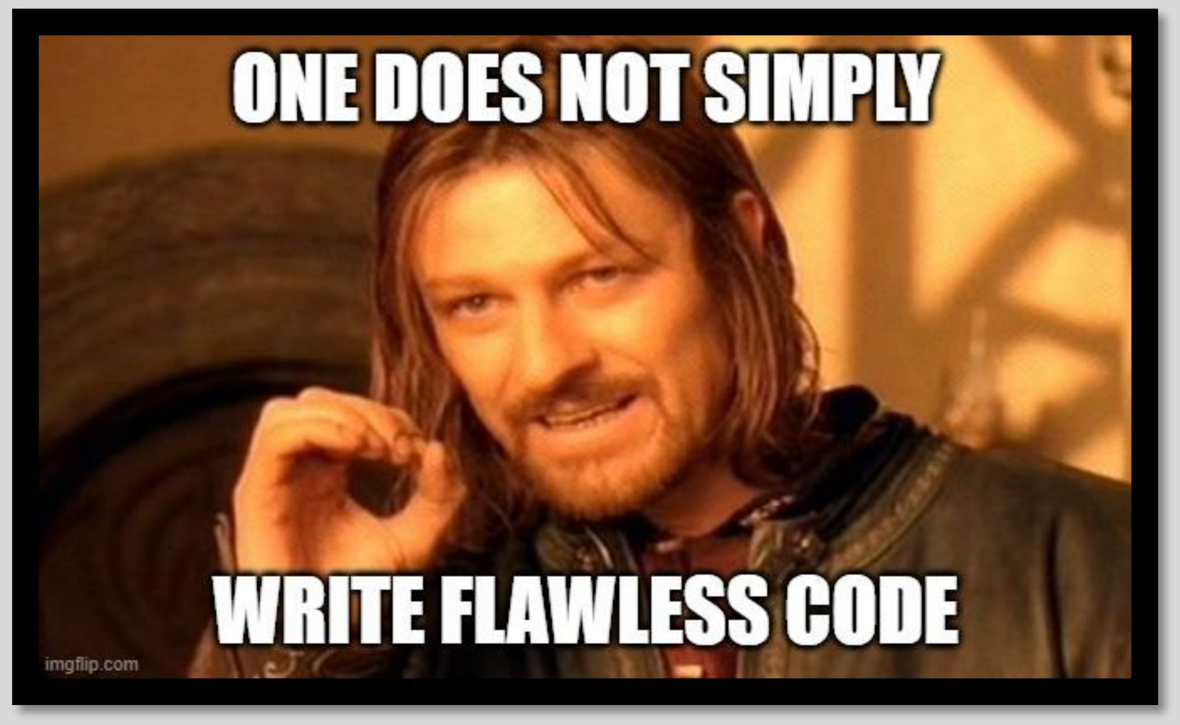
Too Large to Handle

Better user experience unless you die.

Toyota issued a recall on more than 9 million vehicles worldwide because of sudden and unintended acceleration, with people unable to use their brakes. This issue is linked to ***89 deaths and 57 injuries.***

Cause: Single bits in memory control each task, corruption due to HW or SW faults will suspend needed tasks or start unwanted ones. Known software bugs: buffer overflow, unsafe casting, and race conditions between tasks.

A universal truth:

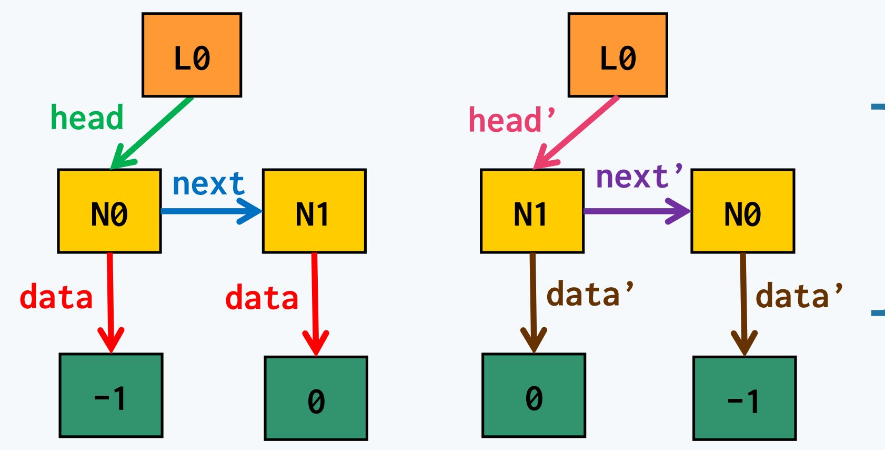


SCAN ME

Design Level

Verification What behavior should our system allow? Prevent?

```
Model of reverse list method:
one sig List { head: lone Node, head': lone Node }
sig Node { next: lone Node, data: one Int,
           next': lone Node, data': one Int }
fact WellFormedList{
   all n : List.head.*next | n !in n.^next
   List.head.*next = Node
   List.head.*next.data = List.head'.*next'.data'
   List.head.*next = List.head'.*next'
   all n : Node | n.data = n.data'
}
pred Reverse{
   all n : Node | n.next = n.~next'
}
run Reverse for 3 but 2 Int
```



These illustrations are the output of executing a model

How can we translate the Model's output into tests? **Debug**

Synthesis How can we generate code from the model?

Writing software models is ironically.... ***error prone***.

We verify, debug and synthesize models too.