SPARK: You simply can't write better code

Fabien Chouteau

Embedded Software Engineer at AdaCore

Twitter : @DesChips
GitHub : Fabien-Chouteau
Hackaday.io: Fabien.C

When failure is not an option

Failure is not an option

Functional Safety

Functional Safety

- Testing
- Code review
- Trust me I know what I'm doing

Programming is all about communication

With:

- The compiler
- The other tools (static analyzers, provers, etc.)
- Users of your API
- Your team
- Yourself in a couple weeks...

Contracts

```
type Stack is tagged private;

function Empty (S : Stack) return Boolean;
function Full (S : Stack) return Boolean;

procedure Push (S : in out Stack; Val : Integer)
  with Pre  => not S.Full,
       Post => not S.Empty;

procedure Pop (S : in out Stack; Val : out Integer)
  with Pre  => not S.Empty,
       Post => not S.Full;
```

Proving your code

iFACTS - Air Traffic Management System

IFACTS, introduced in 2011, predicts an aircraft's location up to 18 minutes into the future. NATS said the system has helped cut emissions and resulted in a 40% capacity increase for some airspace sectors.

EwoK - secure microkernel for USB

"Software classes of attacks (e.g. buffer overflows) are mitigated using EwoK [...] providing more confidence by using the Ada safe language along with SPARK for formal verification of critical parts."
github.com/wookey-project/ewok-kernel

LEARN.
ADACORE.COM