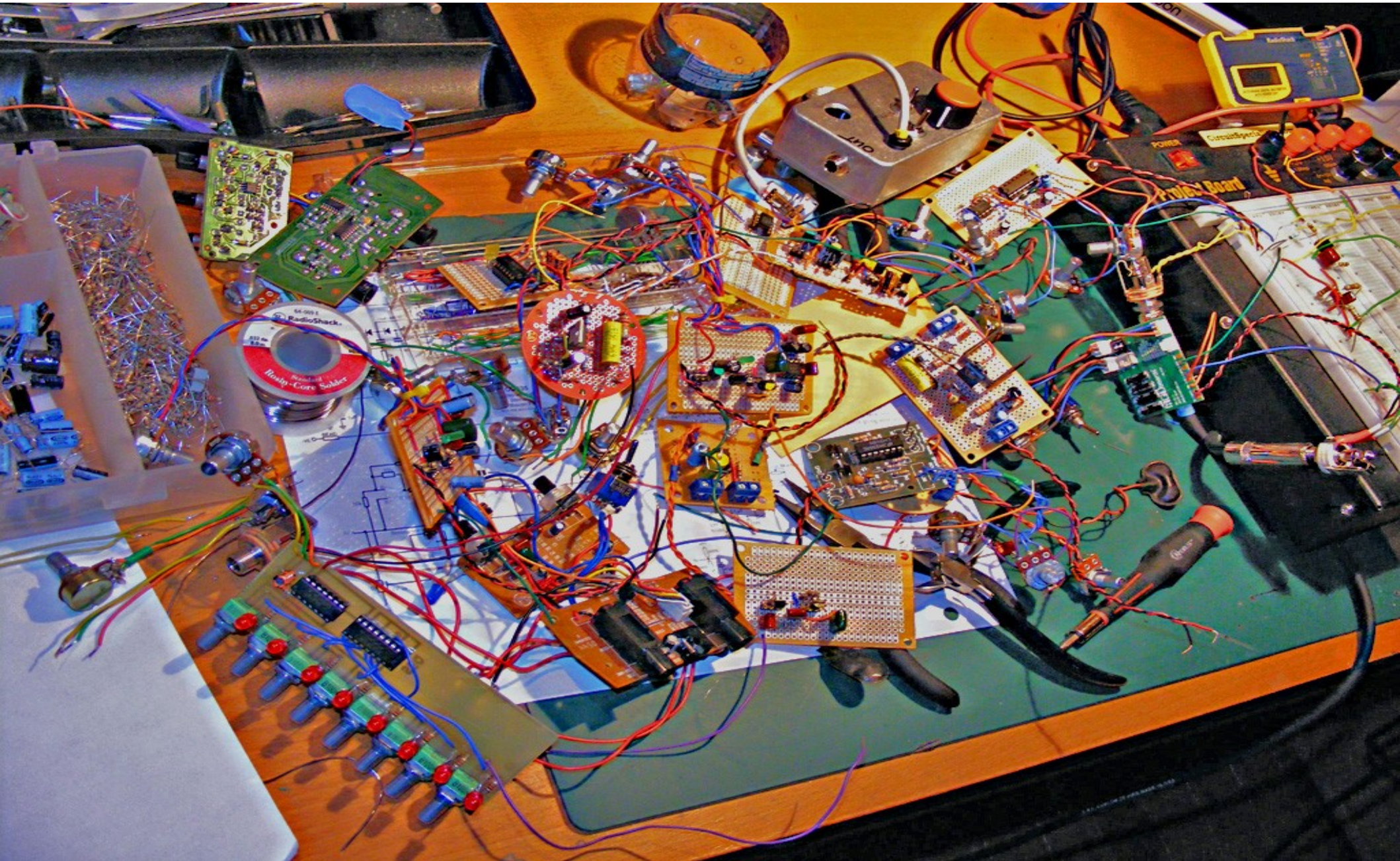
# Formal verification of an “ever changing” protocol

**Vieri del Bianco**
Joe Kiniry
Dragan Stosic

# A tricky problem



# Wishes...

FAST DEVELOPMENT

PRECISE (FORMAL)

RUNNING SYSTEM without the board

ADAPT TO SPEC CHANGES

STABLE API

...good luck

# The solution: multiple hats

## Formal

## Bad weather

# The solution: multiple hats

| Formal | Bad weather |
| --- | --- |
| Stylish | Unshaped |
| Elegant | Ruggish |
| Think how to wear it | Put it on |
| Beautiful | Beautiful... “inside” |
| Can be ruined by bad weather | Completely water proof |

# Seriously

| Formal facts | Agile facts |
| --- | --- |
| Stable API JML specified | Changing and stable: dependency inversion |
| RAC with JML2 tools | TDD |
| Simulators | Contract based tests |
| 10000+ generated tests | Continuous build |

# Seriously

Formal-Agile facts

Suites tested with RAC

Suites (hacks) without RAC

and...

Specs tested with unit tests

Unstable behaviors only on specs

# The point is... it works

Simulators are running

Rapid development

Formal specs of the stable API

And when the first prototype board came:

worked out of the box!

(well... almost)