Can we Verify C with Whiley?

David J. Pearce

School of Engineering and Computer Science
Victoria University of Wellington

@WhileyDave
http://whiley.org
http://github.com/Whiley

Verification: An Idea

"It is clear to **"Formal Methodists"** *like ourselves, for some of whom formal methods can be something of a "religion", that introducing greater rigor into software development will improve the software development process, and result in software that is* **better structured**, **more maintainable**, *and with* **fewer errors***"*

–Bowen and Hinchey

"It is clear to all the best minds in the field that a **more mathematical approach** *is needed for software to progress much."*

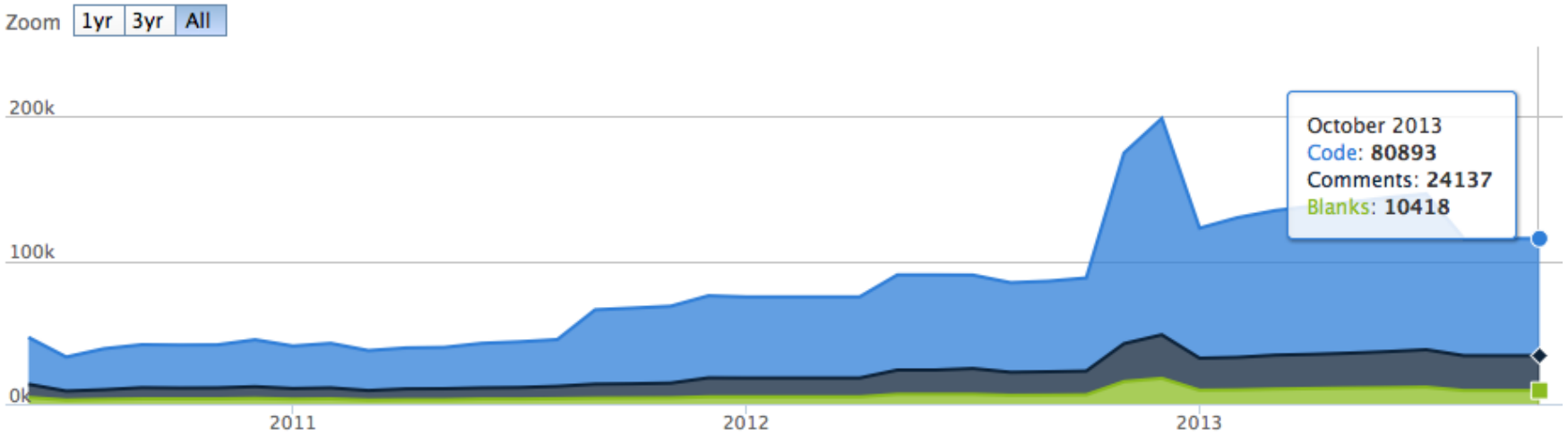
–Meyer

Verification: A Challenge

"A **verifying compiler** *uses automated mathematical and logical reasoning methods to check the correctness of the programs that it compiles"*

–Hoare'03

History of Whiley

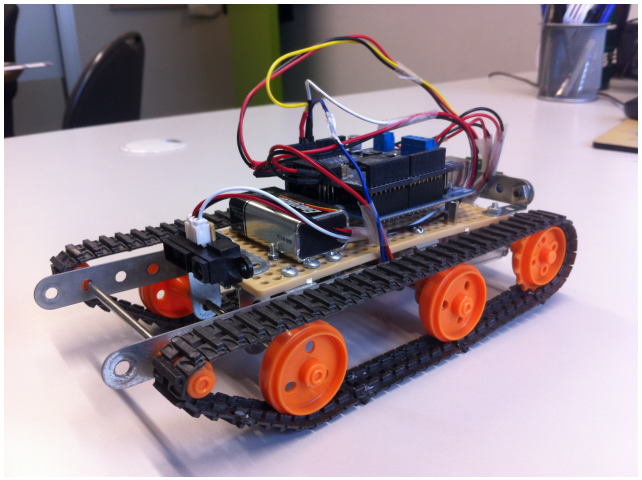


- 2009 — **Initial** version of Whiley released (GPL Licence)
- 2010 — **GitHub** repository and **`http://whiley.org`** go live
- 2010 — **Version 0.3.0** released (BSD Licence)
- 2013 — **Version** 0.3.20 (approx 81KLOC)
- 2014 — Used for **Teaching** SWEN224 ($\approx$ 110 students)
- 2015 — **Version** 0.3.36 released
- 2015 — Used for **Teaching** SWEN224 ($\approx$ 130 students)

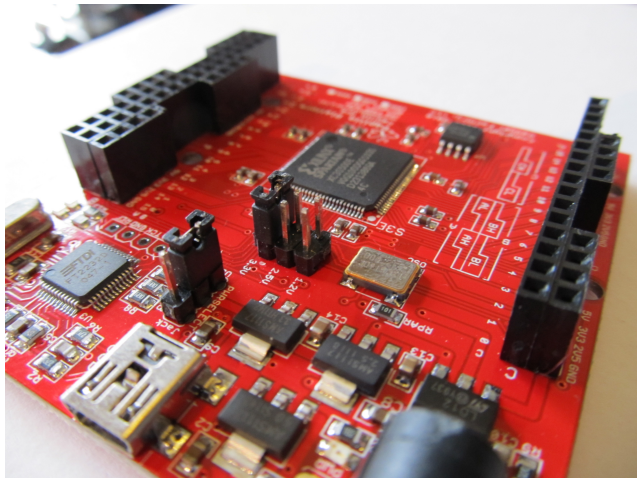
Demo

Embedded Systems ... ?

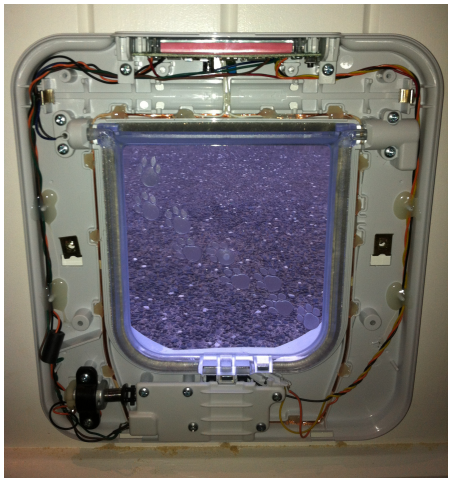
The BitCraze **CrazyFly** Nano-QuadCopter



An **Arduino** Tracked Robot



The Papilio **FPGA** Board



A microchip-based **Cat Flap**

http://whiley.org

@WhileyDave
http://github.com/DavePearce/Whiley