

C Program Specification and Verification with ACSL and Frama-C/WP

VerifyThis Tutorial

Virgile Prevosto
virgile.prevosto@cea.fr

CEA Tech List

2019-04-06



- ▶ short general introduction to Frama-C and ACSL
- ▶ examples of writing ACSL specifications
- ▶ verification of implementations with the WP plugin of Frama-C
- ▶ All material available on [Frama-C github](#):

<https://frama.link/TODO>




- ▶ **Examples** contains plain (unannotated) C code
- ▶ **Solutions** contains the corresponding annotations...
- ▶ ... that should be provable by Frama-C 18.0, Alt-Ergo and Coq

It's 2019! Why bother with proving C programs?

- ▶ Lot of legacy code
- ▶ Embedded world (aka IoT) still uses it in many places
- ▶ And in some cases they care about safety and (cyber)security

A few recent use cases

- ▶ **S2OPC** OPC (communication protocol for industrial systems), result of INGOPCS French project
- ▶ **Bureau Veritas Cybersecurity Guidelines**
- ▶ **Vessedia H2020 project**  including verification of parts of **Contiki OS**

- ▶ A Framework for modular analysis of C code.
- ▶ <http://frama-c.com/>
- ▶ Developed at CEA Tech List and Inria
- ▶ Released under LGPL license (v18.0 Argon in November 2018)
- ▶ Kernel based on CIL (Necula et al. – Berkeley).
- ▶ ACSL annotation language.
- ▶ Extensible platform
 - ▶ Collaboration of analyses over same code
 - ▶ Inter plug-in communication through ACSL formulas.
 - ▶ Adding specialized plug-in is easy

