Introduction to Spark

Paul Jackson
Paul.Jackson@ed.ac.uk

University of Edinburgh

Formal Verification
Autumn 2023

SPARK overview

- SPARK is a subset of Ada
- Ada is designed for high-integrity (safety/security/mission critical) applications

  Many features (e.g. syntax, strong typing) help with creating bug-free software
- SPARK subset chosen to further ease creation of high-integrity applications:
  - restricts use of language features more likely to introduce errors
  - supports formal verification of
    - information flow properties,
    - absence of run-time errors,
    - contracts (e.g. pre-conditions and post-conditions)

SPARK application examples

- iFACTS air-traffic management system
- Jet-engine control
- Avionics
- Railway signalling
- Cube-sat
- Diving life-support system
- Multi-level security workstation
- Medical devices

planetalkinglive.com

www.bart.gov

commons.wikimedia.org