Using Spark/Ada for the use of automated correctness verification

Brian E. Lavender

CSC 201

Nov 7, 2023

List of Frames

A little bit about me.

- MS in Computer Science Fall 2010.
- Taught lower division comp sci at Sac State and American River College.
- Work for State of CA, primarily Java.
- Intrigued by program correctness. Axiomatic semantics and formal methods.
- Private Pilot. Future: Computers, Carbon Fiber, and Jet-A/Diesel.

Ada selected for C-130J Software

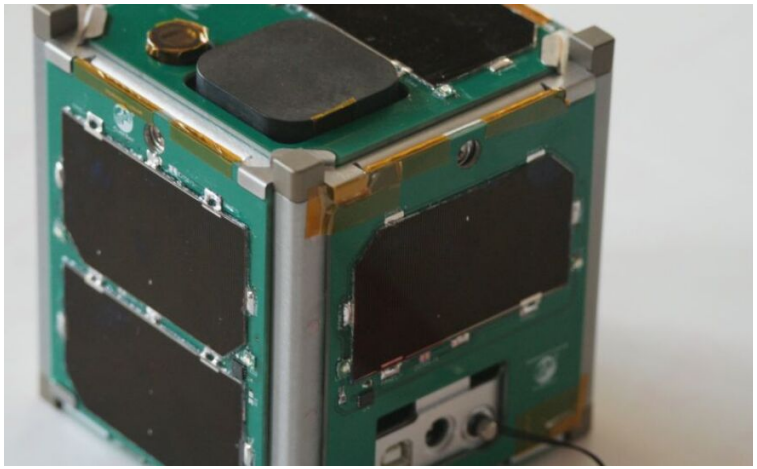
The specific product is GNAT Pro High-Integrity Edition for a PowerPC target running VxWorks 653, the time- and memory-partitioned real-time operating system from Wind River Systems.

Lockheed Martin Selects GNAT Pro for C-130J Software

C 130J loop

C130J You Tube Video

CubedOS



A SPARK Message Passing Framework for CubeSat Flight Software

Simple Ada program

Guessing game to illustrate simple ada program

- getAns.ads spec file
- getAns.adb implementation
- AddQuick2.adb is our main
- imports at top
- subtype
- variable declarations
- loop

Ada background

Originally designed by a team led by French computer scientist Jean Ichbiah of CII Honeywell Bull under contract to the United States Department of Defense (DoD) from 1977 to 1983. Named after Ada Lovelace.

No language grows up in a vacuum.

- ALGOL 68
- Pascal
- C++ (Ada 95)
- Smalltalk (Ada 95)
- Modula-2 (Ada 95)
- Java (Ada 2005)
- Eiffel (Ada 2012)

Safe and Secure Book

Ada emphasizes the following features and are detailed in the book Safe and Secure Software, An Invitation to Ada

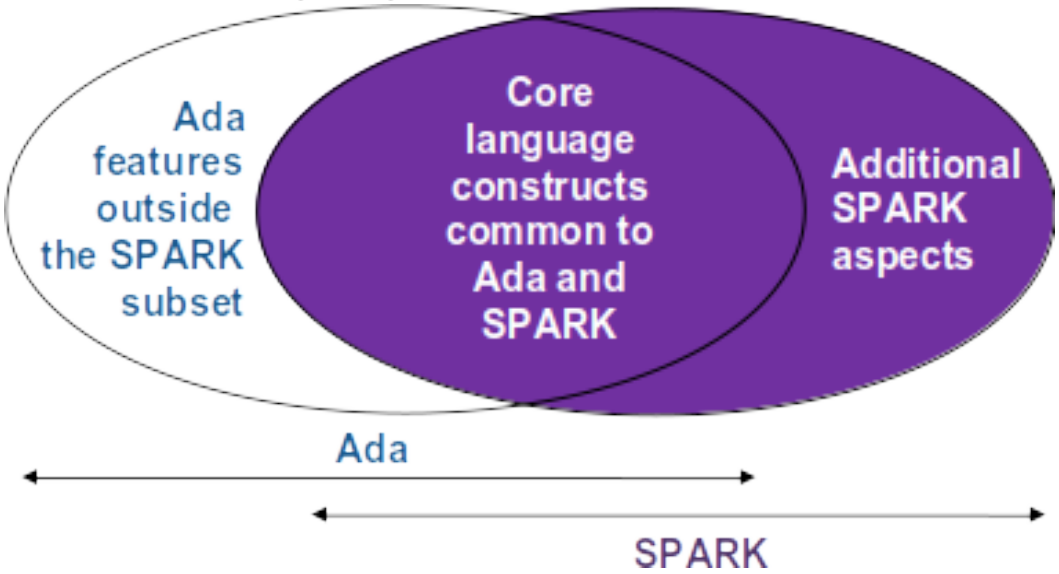
- Safe Syntax
- Safe Typing
- Safe Pointers
- Safe Architecture
- Safe Object-Oriented Programming
- Safe Object Construction
- Safe Memory Management
- Safe Startup
- Safe Communication
- Safe Concurrency
- **Certified Safe with SPARK**

Old School Security is Popular Once Again

If we look at the programming libraries developed in the early 1960s, particularly in mathematical areas and perhaps written in Algol 60 (a language favored for the publication of such material in respected journals such as the Communications of the ACM and the Computer Journal), we find that the manuals tell us what parameters are required, what constraints apply on their range and so on.
Barnes, Safe and Secure Software, An Invitation to Ada, 2014, p128.

What is Spark?

SPARK language is based on a subset of the Ada language.



Spark 2014 Features

Static Verification of programs

- Flow analysis is the fastest form of analysis. It checks initializations of variables and looks at data dependencies between inputs and outputs of subprograms. It can also find unused assignments and unmodified variables.
- proof checks for the absence of runtime errors as well as the conformance of the program with its specifications.

Constructs used to do the static analysis

- structure separating interface from implementation
- correctness by construction
- contracts (pre / post conditions)

Spark Programming Requirements

Spark requires that you adhere to certain requirements .

- Expressions and function calls free from side effects
- Aliasing of names is not permitted
- goto statement prohibited
- Use of controlled types prohibited
- SPARK manual on restrictions.

Spark Mode

SPARK_Mode(On)

Some examples

Let's review some actual code

1. Simple
2. Euclidian Division
3. Ring Buffer
4. Saturation. Contract Case
5. Factorial

Ada/SPARK Crate Of The Year Award Competition!

Ada/SPARK Crate Of The Year Award! competition results. Possibly upcoming competition?