Ada and SPARK 2014

Overview of the current status

IRVINE COMPILER

Presented by:
Joakim Strandberg
M.Sc. in Electrical Engineering, KTH
Mequinox AB

Definitions

Ada is an imperative programming language designed from the start to engineer safe, secure and reliable software.

SPARK is a formally verified Ada. Guarantees:

- No uninitialized variables before usage
- No infinite loops
- Dead-lock free code

Agenda

Introduction to Ada

- Defining new types, Bit-fiddling
- Tool support

Novelties in Ada 2012

- Iteration
- Use all type

SPARK 2014

- Example of SPARK code

Introduction to Ada

If your code looks like the following you are not doing it right:

```
procedure Initialize (This   : in out Car_Type;
                      Age    : Integer;
                      Length : Integer) is
begin
   This.Age    := Length;
   This.Length := Length;
end Initialize;
```

Introduction to Ada

Always define new types:

```
type Age_Type is new Integer range 0..3;

type Length_Type is new Integer;

procedure Initialize (This   : in out Car_Type;
                      Age    : Age_Type;
                      Length : Length_Type) is
begin
   This.Age    := Age;
   This.Length := Length;
end Initialize;
```

Introduction to Ada

Complete control over bit-representation:

```
type Age_Type is new Integer range 0..3;

type Length_Type is new Integer;

 type Car_Type is
    record
       Age    : Age_Type;
       Length : Length_Type;
    end record;

 for Car_Type use
    record
       Age    at 0 range 0..1;
       Length at 0 range 2..40;
    end record;
```

Introduction to Ada

The practise of always defining new types and specifying ranges of all types is important due to it promotes software safety, see next slide.

Mac OS X Mavericks Security Update Sep. 2014

12 out of 19 security issues:

Impact: A malicious application may be able to execute arbitrary code with system privileges

Description: This issue was addressed through improved bounds checking.

http://support.apple.com/kb/HT6443

Introduction to Ada - Tool support

Demo of the following:

- GPS
  - The importance of using the Outline view
  - Placing multiple cursors and editing simultaneously in several places

Notable compiler vendors

AdaCore	GNAT Compiler	Ada 2012
ptc	ObjectAda (Windows) ApexAda (Linux)	Ada 2005
Irvine Compiler	Irvine Compiler	Ada 2005
RR Software	Janus Ada Compiler	Ada 95

Introducing Ada in organizations

Tip: Emphasize the importance of code snippets a.k.a. aliases

Novelties in Ada 2012: Iteration

Iteration in Ada 2005 and before:

```
for X_Id_Index in 1..Last_Index (Xcb.X_Ids) loop
   declare
      X_Id : X_Proto_XML.X_Id.Ptr renames Element (Xcb.X_Ids, X_Id_Index);
   begin
      ...
   end;
end loop;
```

The same iteration, but in Ada 2012:

```
for X_Id of Xcb.X_Ids loop
   ...
end loop;
```

Ada 2005 and before

Java code:

```
Car car = new Car();

car.age();
```

Ada code:

```
Car : Vehicles.Car_Type;

Vehicles.Age (Car);
```

Ada 2012 and Use all type

Java code:

```
Car car = new Car();

car.age();
```

Ada code:

```
use all type Vehicles.Car_Type;

…

Car : Vehicles.Car_Type;

Age (Car);
```

Improved multi-core support in Ada 2012

- Synchronized containers:
- Possible to query how many cores the CPU has
- Subpools concept, for more information see: https://github.com/joakim-strandberg/xcb_library_thin_ada_binding and https://github.com/joakim-strandberg/vulkan

Ada 2012 - Summary

Many improvements to simplify notation and make the language less verbose

The language has become even more flexible (i.e. in out parameters allowed in function definitions)

SPARK 2014 - Formally verified Ada

The SPARK tools transform the Ada code into Why3 modelling language

The Why3 modelling code can then be analyzed by three automated theorem provers: Alt-Ergo, CVC4 and Z3

SPARK is a mature technology and a pleasure to work with. For an example of Safety critical script in SPARK see:

https://github.com/joakim-strandberg/aida_2012

Make with Ada competition

Programming competition between the 15:th of May to 15:th of September 2017

If you are teacher at the University, inform your students!

http://makewithada.org/

Thank you for your time!