SPARK/Ada Software for CubeSats

FOR ULTRA-RELIABLE SOFTWARE

Dr. Carl S. Brandon, Professor & Director, CubeSat Lab
Peter C. Chapin, Software Director, CubeSat Lab
Vermont Technical College, Randolph Center, VT 05061
carl.brandon@vtc.edu peter.chapin@vtc.edu

VERMONT TECH

Why Use Ada?

- If the software fails, we would also lose the satellite cost of $30,000-$50,000 and launch cost of $80,000-$100,000 and several years' effort
- Ada offers a greatly improved probability of error-free software when compared with C, which is used in most CubeSat projects
- The development and debugging time would be less, which is helpful with our smaller resource base
- Students get learn and use the best software engineering features in Ada in a real-world embedded system

Ada and SPARK

- Allows for a further increase in software reliability
- Allows for various conditions to be checked by static analysis
- Although small by SPARK standards, our Arctic Sea Ice Buoy and CubeSat have only one chance to get the software right
- A rare opportunity for our students to work on a real-world, very high-integrity system using the best tools available
- The elimination of the run-time system for the Arctic Sea Ice Buoy
- High-integrity realtime programming using the RavenSPARK subset of the Ada Ravenscar Tasking Profile for the CubeSat

AdaMagic

- There is no Ada compiler for the Texas Instruments MSP430 series of processors that we are using
- The AdaMagic compiler front end which produces ANSI C as the intermediate language allows us to do the projects in SPARK/Ada
- The C output from AdaMagic is then run through the Rowley Crossworks cross compiler to produce object code for the MSP430
- This same procedure, for a different purpose, was discussed by Praxis at the Ada Europe 2004 conference in "High Integrity Ada in a UML and C World"

Other SPARK/ADA information

- Our project is discussed in detail in "Use of Ada in a Student CubeSat Project," *Ada User Journal*, Vol. 29, No. 3, Sept. 2008, and at Ada Europe 2009, Venice, Italy, June 2009, SIGAda 2010, St. Petersburg, FL, November 2009, the CubeSat Developers Workshop at Cal Poly, San Luis Obispo, CA, April 2010 and will be presented at the Fifth International Conference on Design Principles and Practices, Rome, Italy, February 2011
- In a 10,000-line program, Tokeneer, written in SPARK/Ada for the National Security Administration, after two years of testing, NSA found only one error
- The complete Tokeneer project can be found at: http://www.adacore.com/home/products/gnatpro/tokeneer
- In a large mixed language avionics project, Ada had 10% of the C error rate, while SPARK/Ada had only 1% of the C error rate

Arctic Sea Ice Buoys

- Buoys will share hardware and software with our CubeSat
- Measures: Wind speed, direction, temperature and GPS position
- Data uploaded to Iridium Satellites, via Short Burst Data Modem Service
- Ultra low power Texas Instrument MSP430 CPU on Lithium thionyl chloride batteries
- Working on the simpler software for the buoys will give us experience before tackling the much more complicated CubeSat software
- Sample SPARK/Ada code from the Sea Ice Buoy:

```
procedure ADC_Read
    (Temperature_Value    : out Data_Types.Temperature_Type;
     Wind_Direction_Value : out Data_Types.Wind_Direction_Type)
  --# global in out ADC.ADC_Hardware;
  --# derives ADC.ADC_Hardware      from ADC.ADC_Hardware &
  --#         Temperature_Value     from ADC.ADC_Hardware &
  --#         Wind_Direction_Value  from ADC.ADC_Hardware;
  is
     TempVal    : ADCValue;
     WindDirVal : ADCValue;
  begin
     ADC.Read(TempVal, WindDirVal);
     Temperature_Value := Data_Types.Temperature_Type(TempVal);
     Wind_Direction_Value :=  Data_Types.Wind_Direction_Type(WindDirVal);
  end ADC_Read;
```