Use of SPARK in a Resource Constrained Embedded System

Chad Loseby
Peter C. Chapin
Carl Brandon

Vermont Technical College

Outline

- Overall Problem
- Ice Buoy Requirements
- Our Solution Using SPARK/Ada
- Lessons Learned
- Future Work

Sea Ice Dynamics

- Desire to understand the dynamics of Arctic sea ice
  - Jun Yu (University of Vermont) has been developing mathematical models.
  - Used satellite obtained data of ice movement, deformation, and thickness.
  - Needs ground truth information.
    - Wind
    - Temperature
- VTC's role?

General Requirements

- Must tolerate spring conditions in arctic
  - Temperatures down to -20 C
  - Wind, rain, ice (not much snow)
  - Animals
- Must operate for ~3 months
- Will not be retrieved
  - Must transmit data to base via satellite link

Data Requirements

- Each sample contains...
  - GPS location
  - Wind speed
  - Relative wind direction
  - Temperature
  - 3-axis magnetometer reading
    - Together with location allows absolute orientation to be computed.
- Each data item separately time stamped

Software Requirements

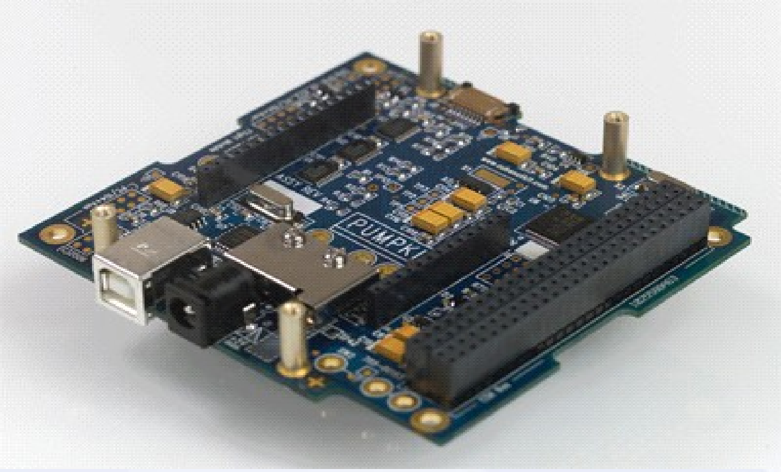
- Sampling Frequency
  - Very slow... once every 30 minutes
    - Software performance not an issue
    - No significant real-time requirements
- Accuracy
  - Spacial resolution: 100s of feet
  - Temporal resolution: minutes
  - Data accuracy: 10-20%

Reliability

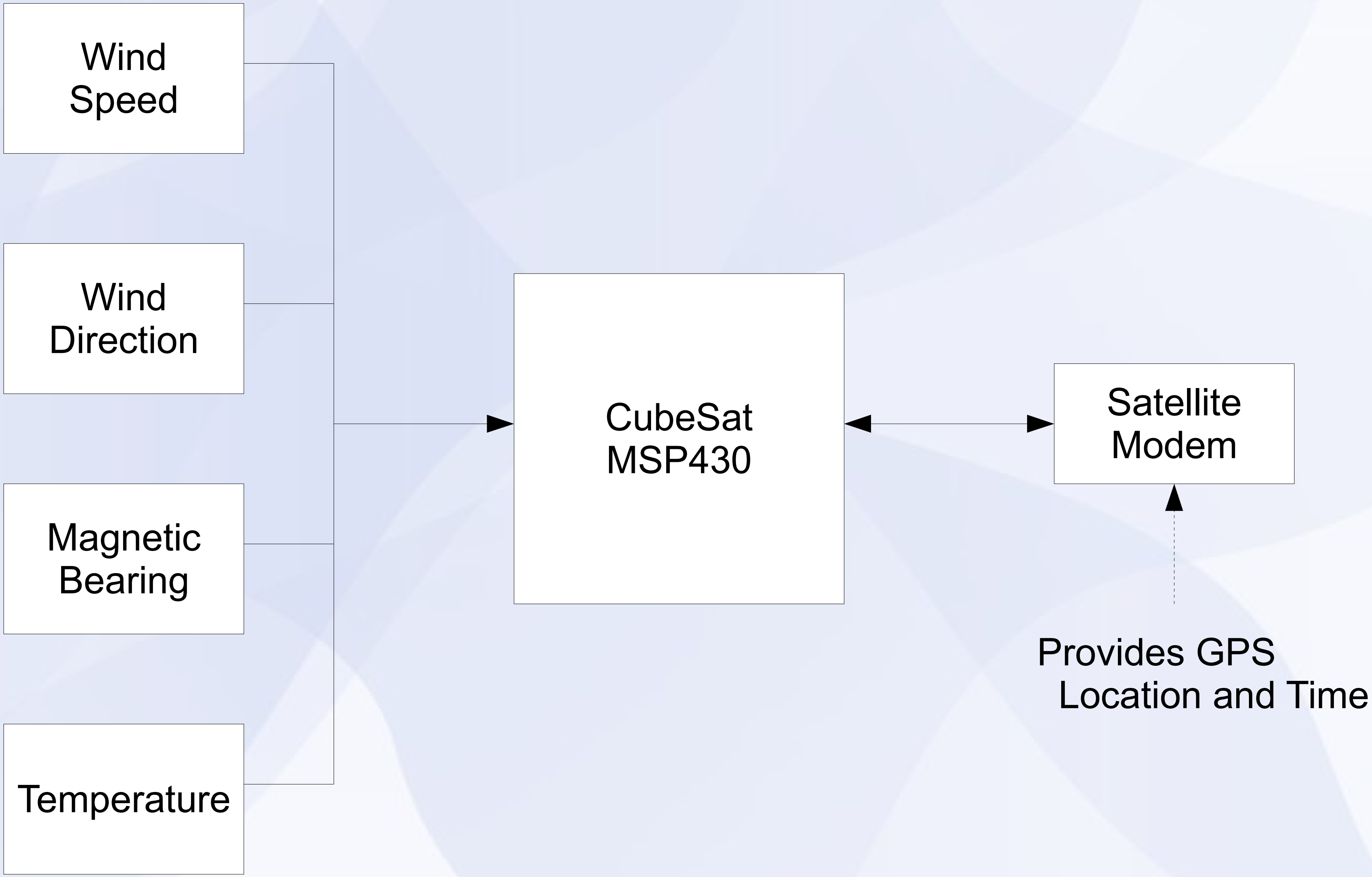
- Significant requirements
  - No access once deployed
  - No ability to upload fixes
  - Device entirely autonomous
  - Must recover from intermitient hardware failure
- Keep it simple
  - No on board processing of data

CubeSat Platform

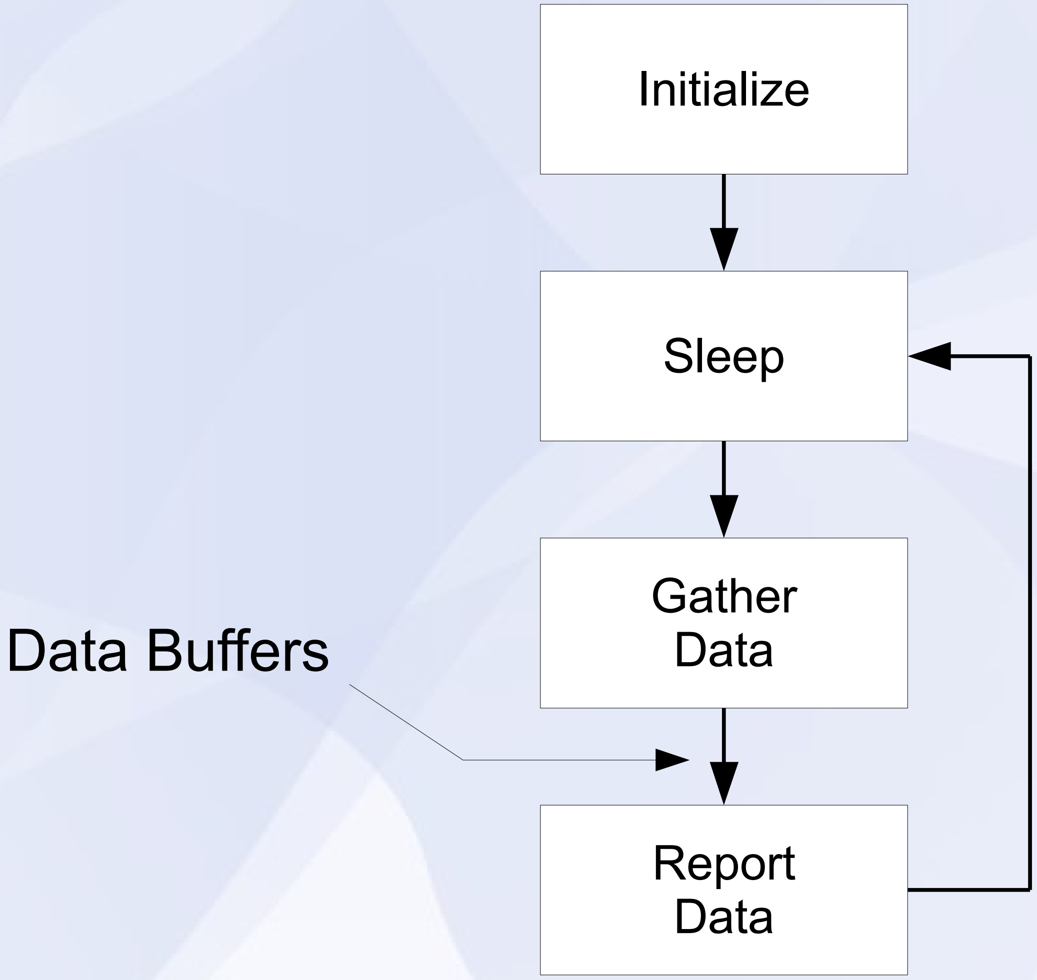
- MSP430 based
  - Very low power
  - Adequate performance
  - Highly constrained
    - 60 KiB ROM
    - 2 KiB RAM
- Used for future projects



Block Diagram



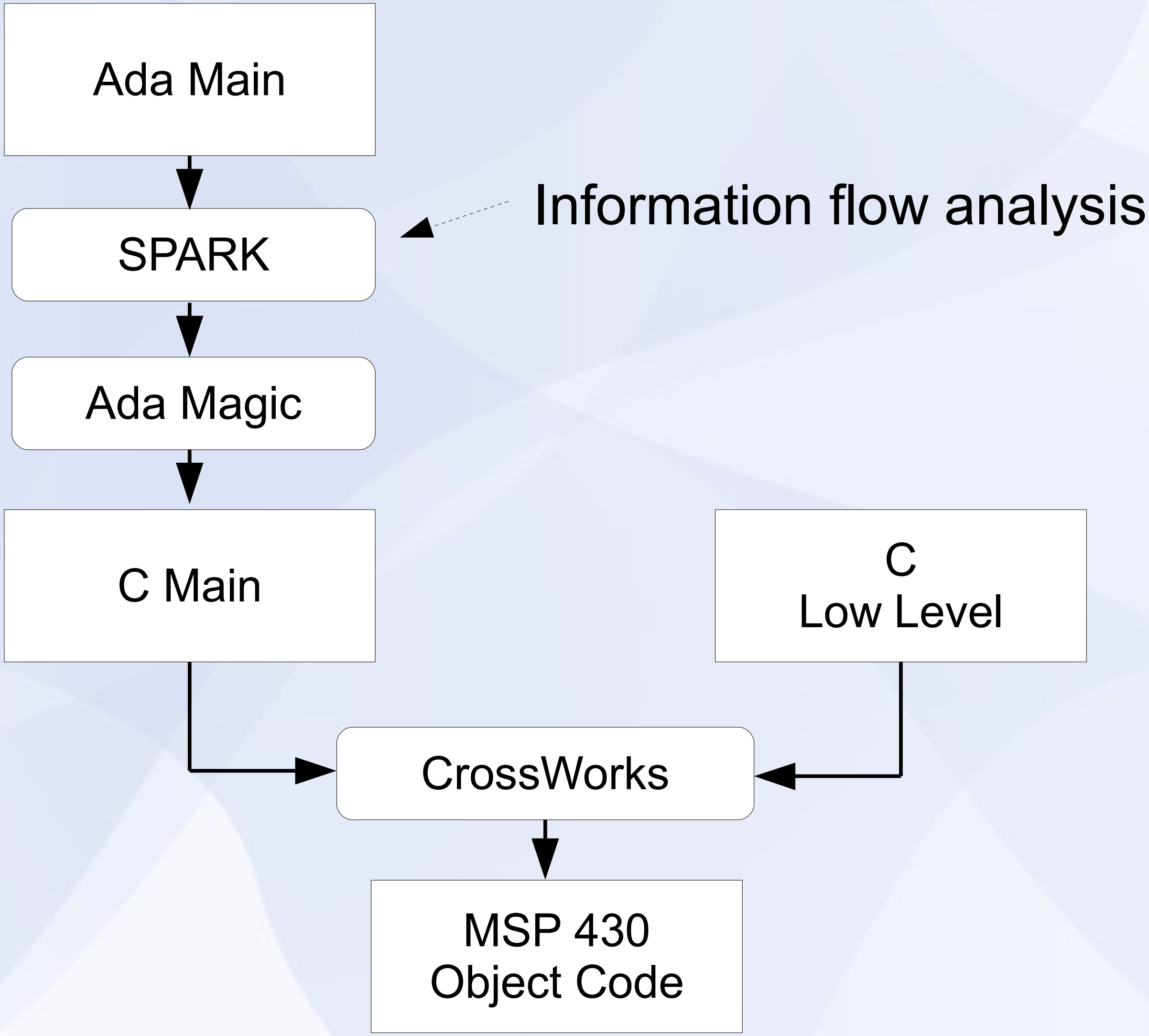
Software Structure



Software

- SPARK/Ada
  - Problem...
    - No Ada compiler for CubeSat platform
  - Solution...
    - Compile Ada to C, then use C compiler

Tool Chain


Ada Main
SPARK
Information flow analysis
Ada Magic
C Main
C
Low Level
CrossWorks
MSP 430
Object Code

SPARK Provides

- More reliable software
- A way to simplify the run time system
  - Exception support not needed
    - Program_Error can't occur
    - Constraint_Error can be avoided
  - Dynamic memory allocation not needed
  - Lack of dynamic memory also makes evaluating memory consumption easier
- *We didn't use any run time system!*

C as Assembly Language

- Need C for low level access
  - Ada Magic compiler does not know the platform.
- Minimize the amount of C
  - C is error prone
  - C is not visible to SPARK
- We kept our C functions one or two lines.

Timer Interface

- ```
  package Timer
  --# own Hardware;
  is
    procedure Initialize;
    --# global out Hardware;
    --# derives Hardware from ;
    pragma Import(C, Initialize);

    procedure Sleep;
    --# global in out Hardware;
    --# derives Hardware from Hardware
    pragma Import(C, Sleep);

  end Timer;
  ```
  ```

Hand Written C

- Platform specific code written in C
  - … Interacts with target C compiler
  - … Uses names compatible with Ada Magic generated code
- ```
  #include <msp430x14x.h>
  #include <standard.h>

  void Timer_Sleep(void)
  {
    _BIS_SR(LPM3_bits);
  }
  ```
  ```

Other Hardware

- A similar technique was used for
  - Interfacing to A/D converters
  - Interfacing to USARTs
  - Interfacing to debugging LEDs
- Interrupt service routines in C
  - But we only used one (for the timer)
    - Used to wake up the system.
  - USART I/O was done with polling!

Results

- It is possible to compile Ada onto a very small device using C as an intermediate language.
- *SPARK helps by enabling massive run time simplifications.*
- It is possible to build such a system in an educational setting.

Future Work

- Finish prototype
  - Still need to complete enclosure
  - Still need to complete software
    - Data formatting
    - Verify freedom from run time errors
    - Evaluate memory consumption
    - Prove buffers can be drained
  - Plan to do live tests this winter in Vermont
- Deploy in March 2011?

QUESTIONS?

(Thanks to AdaCore, Praxis, Rowley Associates, SofCheck)