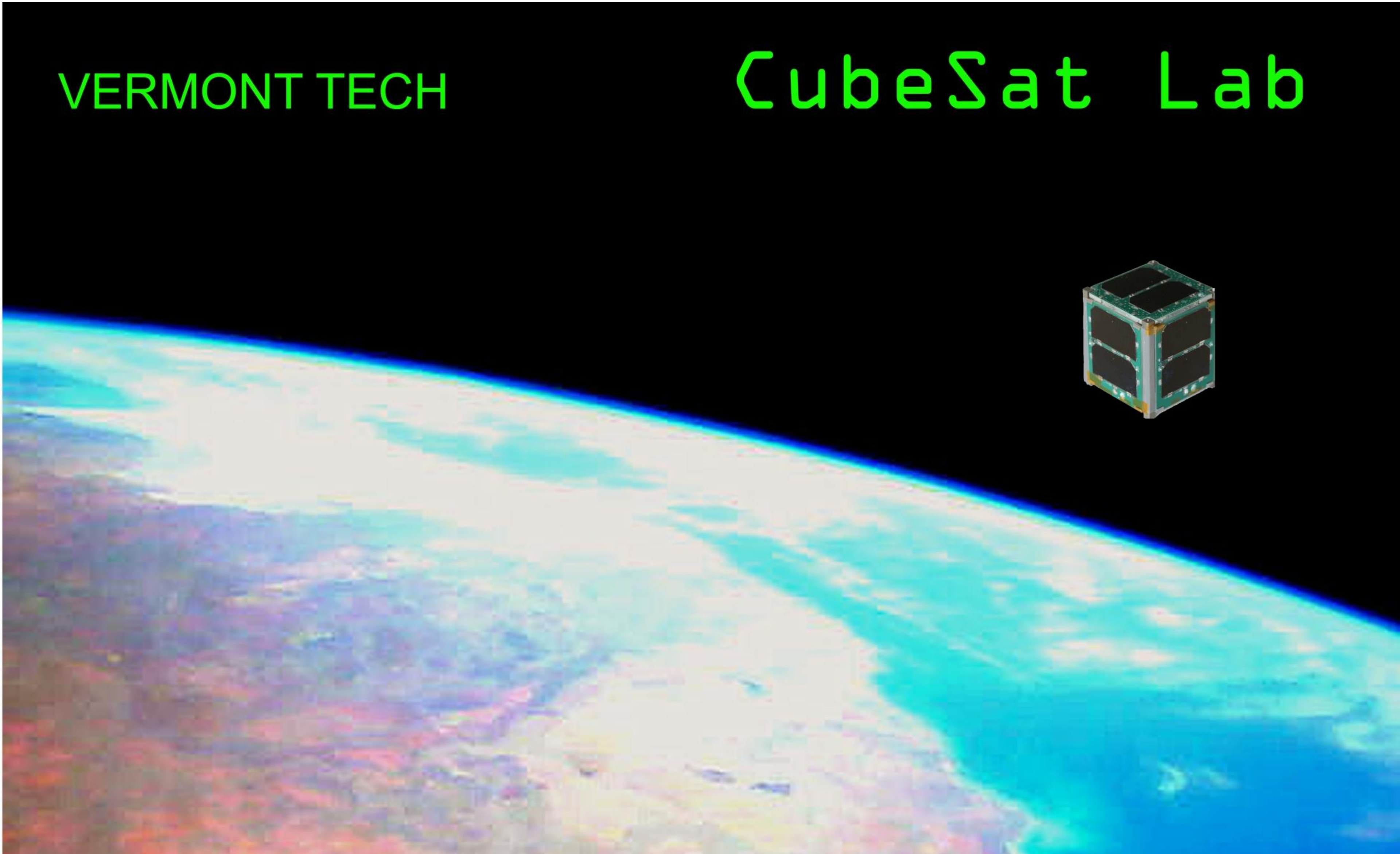
The Use of SPARK in a Complex Spacecraft

CubeSat Developer's Workshop - Copyright 2017 Carl Brandon & Peter Chapin

Dr. Carl Brandon & Dr. Peter Chapin carl.brandon@vtc.edu peter.chapin@vtc.edu
Vermont Technical College +1-802-356-2822 (Brandon), +1-802-522-6763 (Chapin)



Why We Use SPARK/Ada

ELaNa IV lessons for CubeSat software:

- NASA’s 2010 CubeSat Launch Initiative (ELaNa)
- Our project was in the first group selected for launch
- Our single-unit CubeSat was launched as part of NASA’s ELaNa IV on an Air Force ORS-3 Minotaur 1 flight November 19, 2013 to a 500 km altitude, 40.5^o inclination orbit and remained in orbit until reentry over the central Pacific Ocean, November 21, 2016. **Eight others were never heard from, two had partial contact for less than a week, and one worked for 4 months.**
- The Vermont Lunar CubeSat tested components of a Lunar navigation system in Low Earth Orbit

Vermont Lunar CubeSat

It worked until our reentry on November 21, 2015:

- We completed 11,071 orbits.

- We travelled about 293,000,000 miles, equivalent to over 3/4 the distance to Jupiter.

- Our single-unit CubeSat was launched as part of NASA's ELaNa IV on an Air Force ORS-3 Minotaur 1 flight November 19, 2013 to a 500 km altitude, 40.5º inclination orbit and remained in orbit until November 21, 2016. **It is the only one of the 12 ELaNa IV university CubeSats that operated until reentry, the last one quit 19 months earlier.**

- We communicated with it the day before reentry

- We are the only successful university satellite on the east coast

- **Follow our project at cubesatlab.org**

Vermont Lunar CubeSat SPARK 2005 software

- 5991 lines of code
- 4095 lines of comments (2843 are SPARK annotations)
- a total of 10,086 lines (not including blank lines)
- The Examiner generated 4542 verification conditions
- all but 102 were proved automatically (98%)
- we attempted to prove the program free of runtime errors
- which allowed us to suppress all checks
- The C portion consisted of 2239 lines (including blank lines)
- Additional provers in SPARK 2014 would improve this

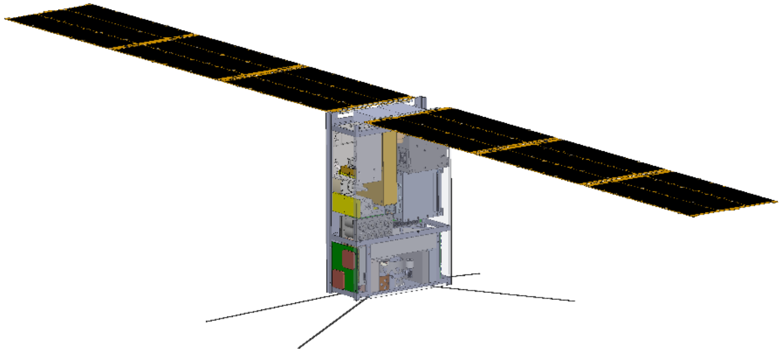
Our new SPARK 2014 CubedOS CubeSat software:

- General purpose CubeSat software system
- Written in SPARK/Ada & proven free from runtime errors
- Will be developed from our Lunar IceCube flight software
- Can integrate existing Ada or C runtime libraries
- Uses a Low Level Abstraction Layer (LLAL)
- LLAL allows running on bare hardware, or OS such as Linux or VxWorks, easily modified for new hardware
- Provides inter module communication
- All modules are completely independent

Some errors that verification condition proofs prevent with SPARK/Ada:

- array index out of range
- type range violation (see Ariane 5 below)
- division by zero
- numerical overflow (see Boeing 787 below)

VxWorks Operating System



Although Vermont Lunar CubeSat did not have an operating system, Lunar IceCube has much more complex software, requiring an operating system. We are using VxWorks because of its very high reliability. It is used for most airliner avionics and many other aerospace applications i.e. the Mars Science Laboratory rover, where extreme safety and security and important.

Three software failures that would have been prevented with SPARK/Ada:

- Mars Science Laboratory Sol-200 Memory Anomaly
- Ariane 5 initial flight failure
- Boeing 787 generator control computer shutdown
- Boeing 787 avionics reset

Mars Science Laboratory

Sol-200 Memory Anomaly

- Six months after landing on Mars, uncorrectable errors in the NAND flash memory led to an inability of the Mars Science Laboratory (MSL) prime computer to turn off for its normal recharge session.

- This potentially fatal error was apparently due to two pieces of its C software having pointers which pointed to the same memory. Curiosity has about 3.5 MLOC written in C. (One would expect about 35,000 errors.)

- SPARK/Ada would have prevented this almost fatal error in a 2.5 billion dollar spacecraft.

Ariane 5 initial flight failure:

Good

Bad, 37 seconds later

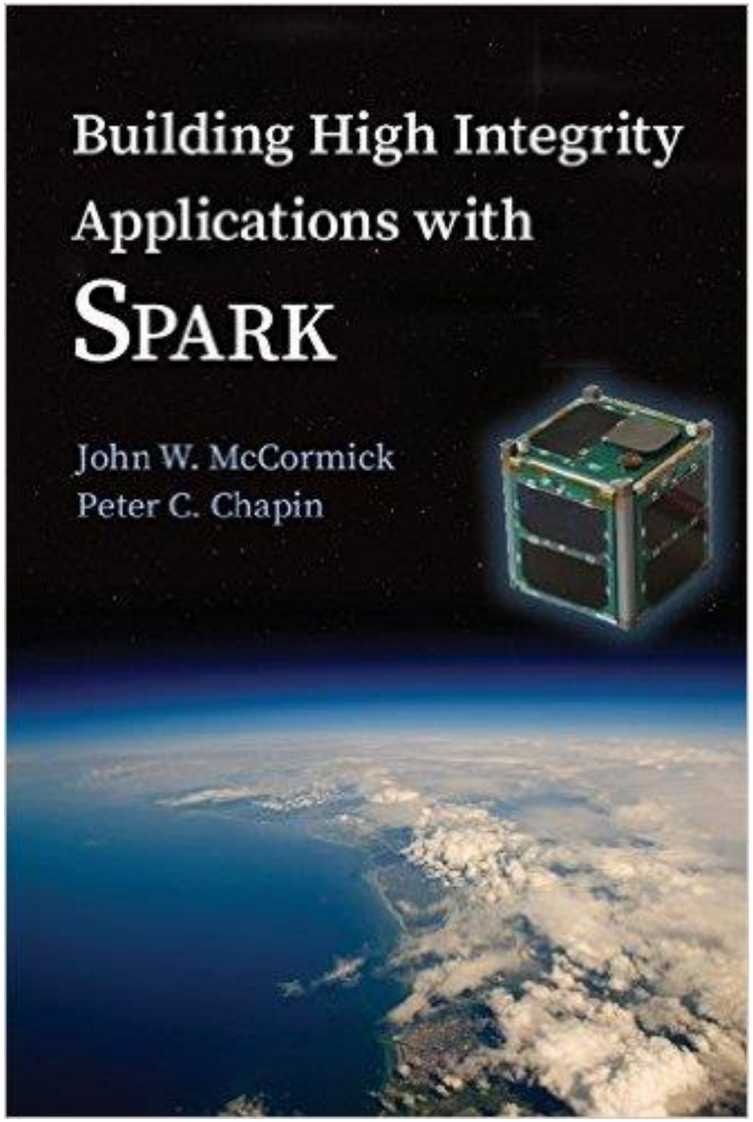
Ariane 5 initial flight failure:

- Software reused from Ariane 4, written in Ada
- The greater horizontal acceleration caused a data conversion from a 64-bit floating point number to a 16-bit signed integer value to overflow and cause a hardware exception.
- “Efficiency” considerations had omitted range checks for this particular variable, though conversions of other variables in the code were protected.
- The exception halted the reference platforms, resulting in the destruction of the flight.
- Financial loss over $500,000,000.
- SPARK/Ada would have prevented this failure

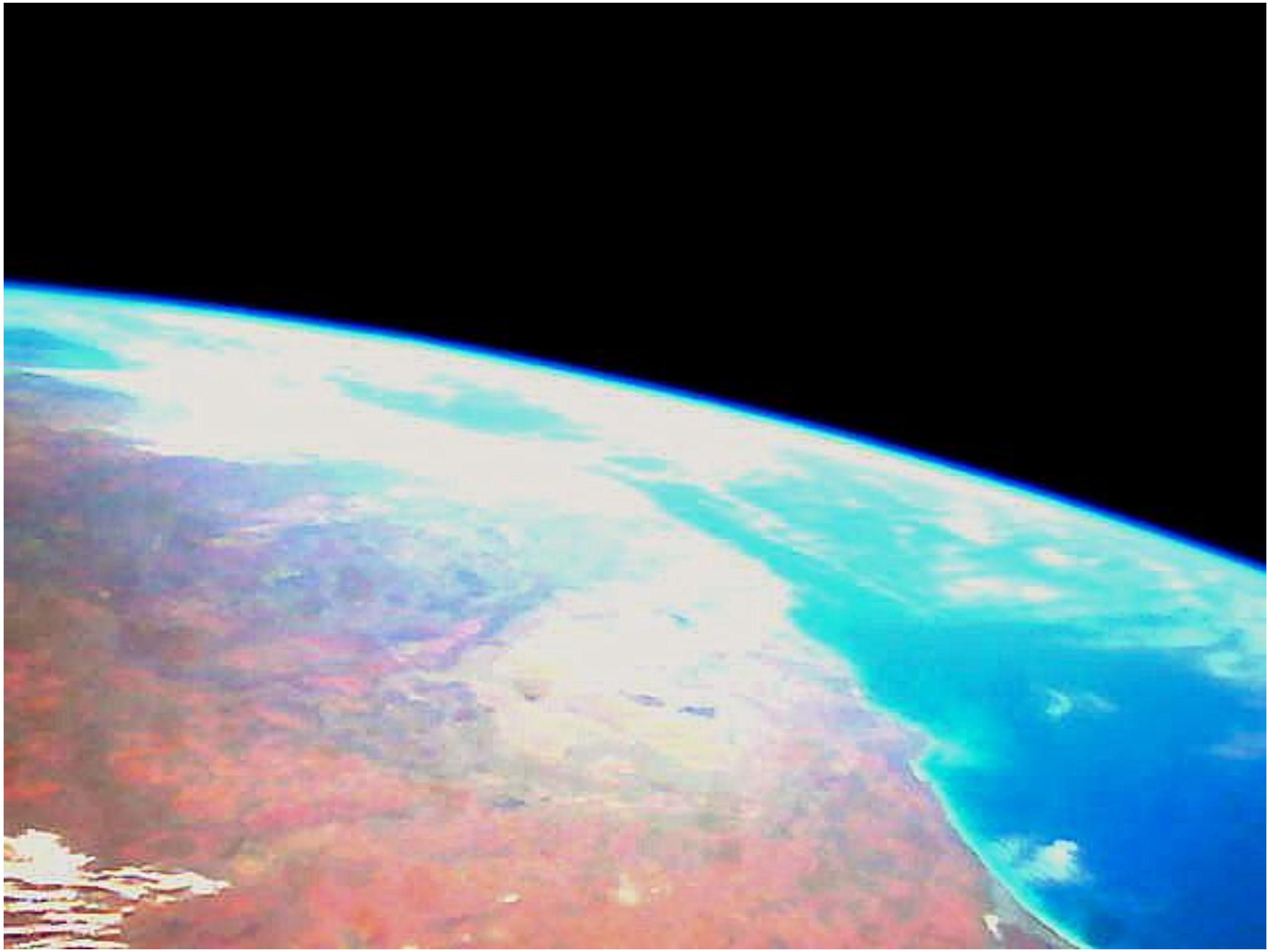
Boeing 787 generator control computer:

- There are two generators for each of two engines, each with its own control computer programmed in Ada
- The computer keeps count of power on time in **centiseconds** in a 32 bit register
- Just after 8 months elapses, the register overflows
- Each computer goes into “**safe**” mode shutting down its generator resulting in a complete power failure, causing loss of control of the aircraft
- The FAA Airworthiness Directive says to shut off the power before 8 months as the solution
- There is now a second 787 reset problem
- SPARK/Ada would have prevented this

A SPARK 2014 book is now available:

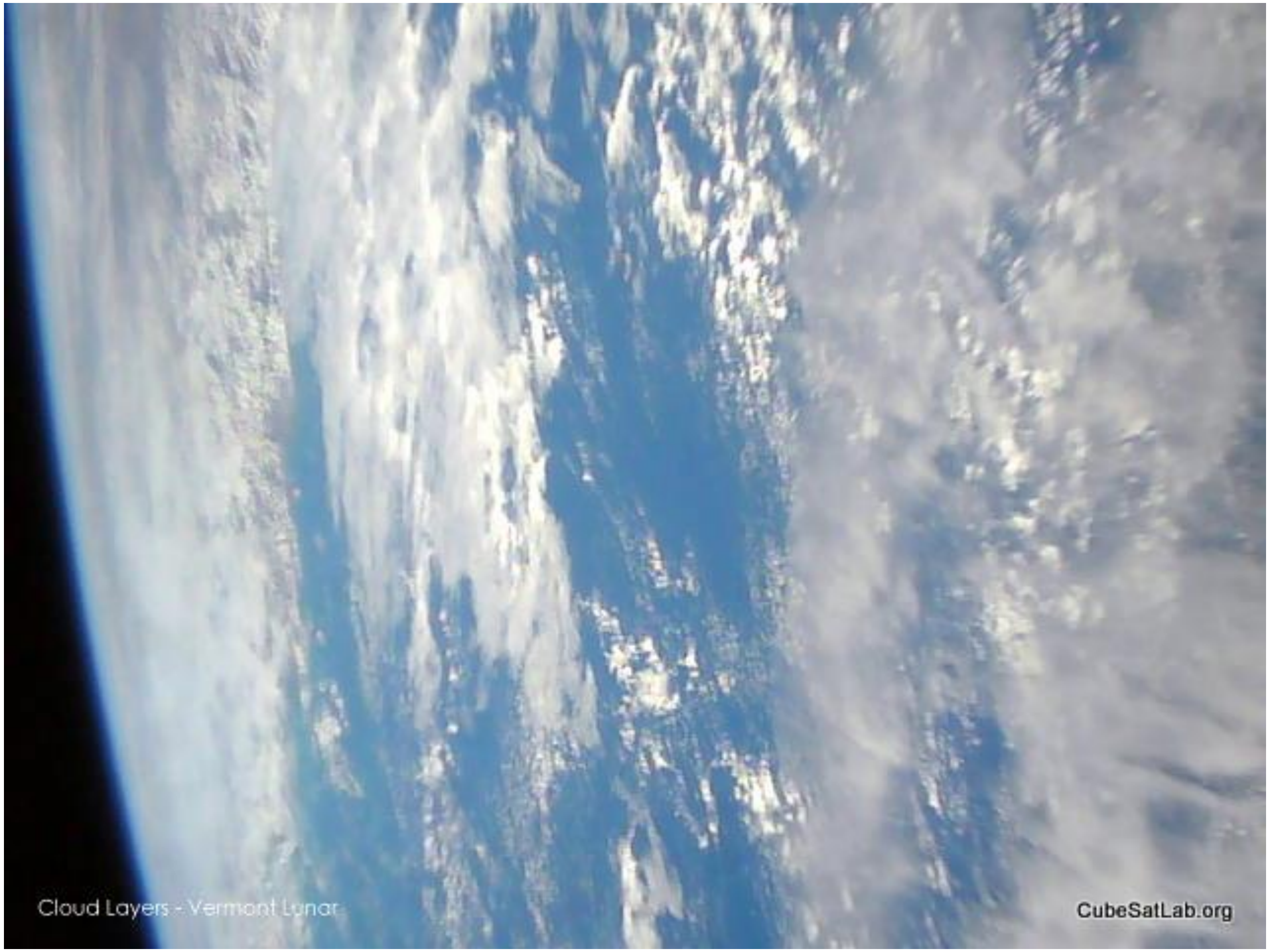


Vermont Lunar CubeSat



Our first picture of Earth, The North coast of Western Australia

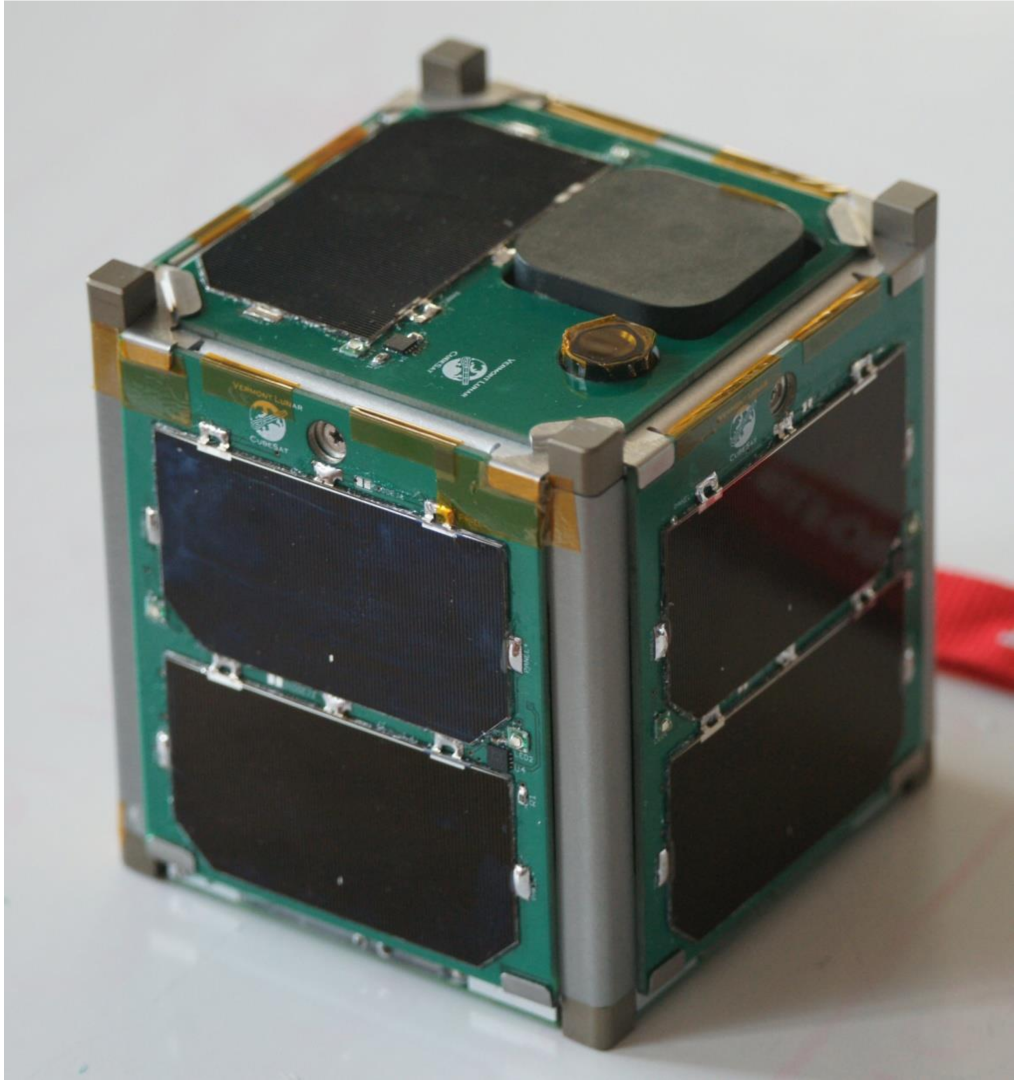
Vermont Lunar CubeSat



Clouds over the ocean, June 2015.

Vermont Lunar CubeSat

VERMONT TECH

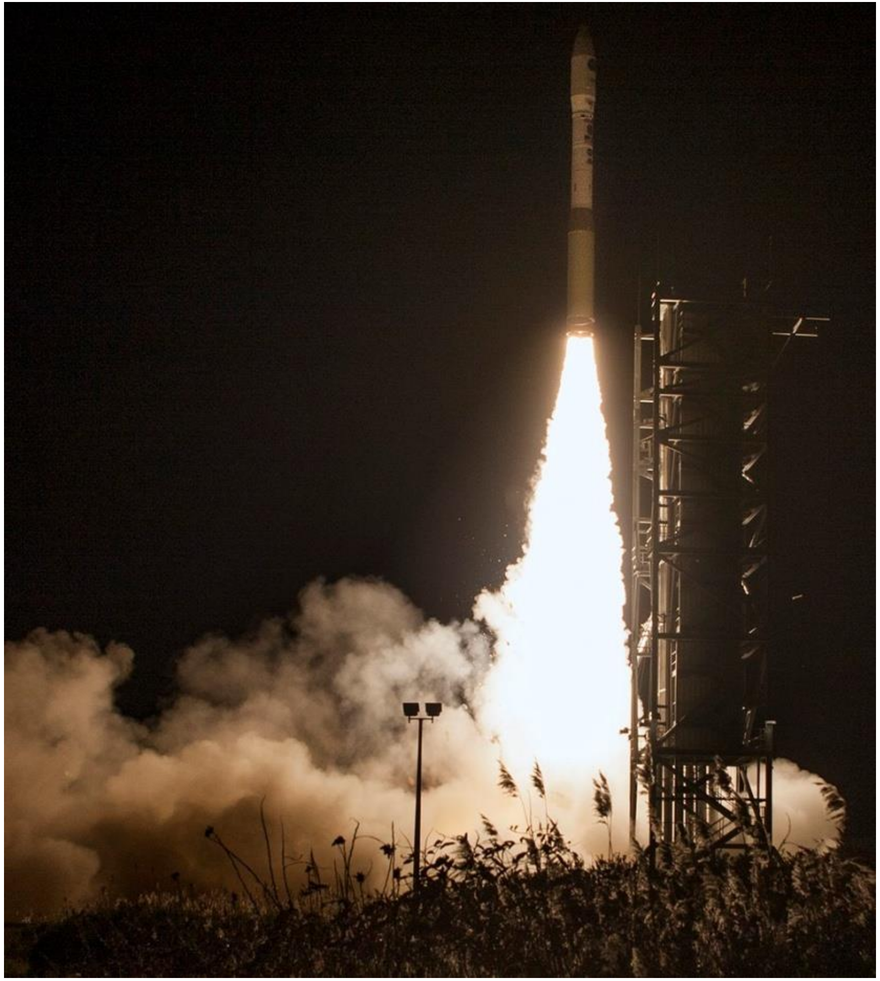


Vermont Lunar CubeSat (10 cm cube, 1 kg)

Software Development Comments for our first CubeSat

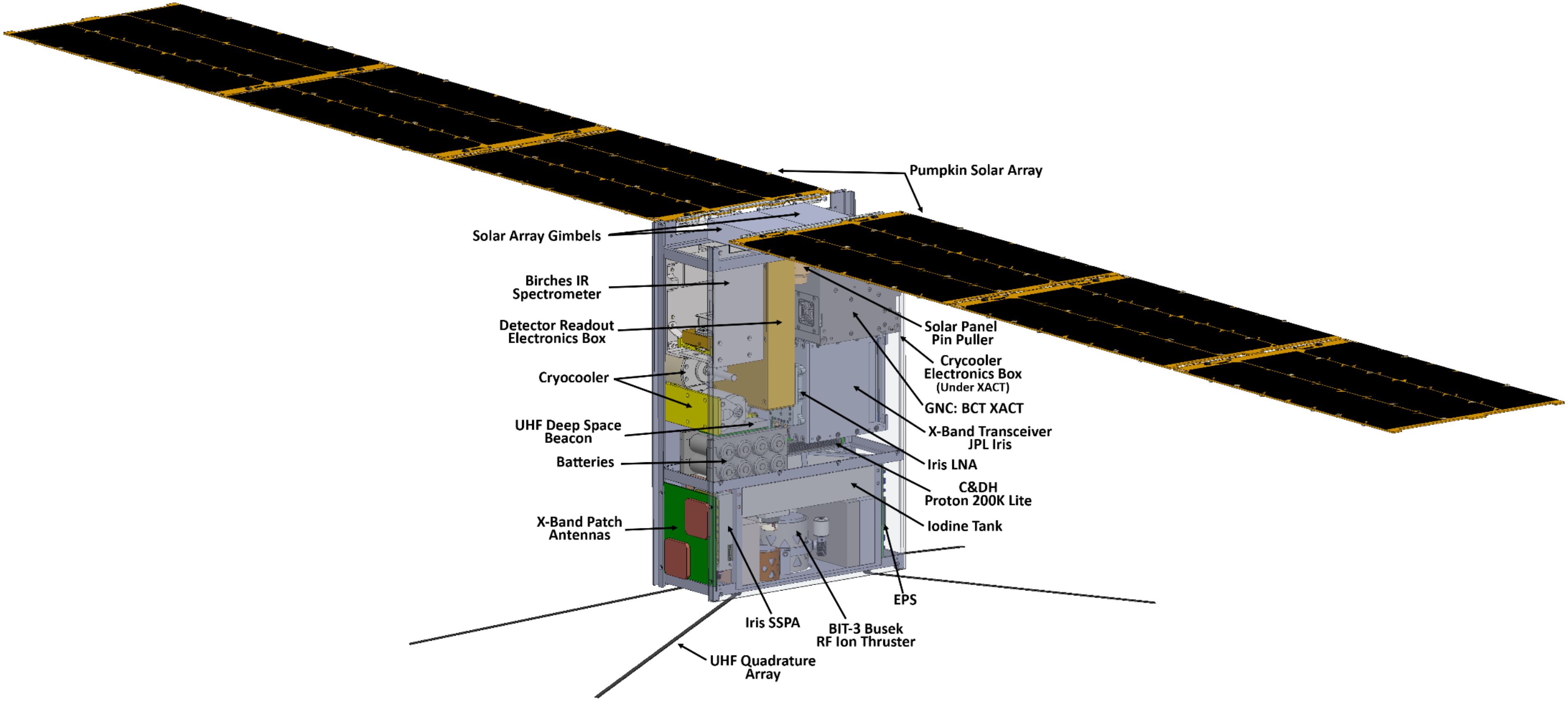
- SPARK caught errors as we refactored the software as we developed greater understanding of the hardware
- SPARK helped the discipline of the software during turnover as some students graduated and were replaced
- Although we did not have a formal development process, without SPARK we probably would not have completed the project with the limited personnel resources and tight time constraint
- Although the CubeSat is limited to 1.3kg, the paperwork is unlimited 😉

ELaNa IV Launch Minotaur 1 – Wallops Island November 19, 2013, 8:15 PM

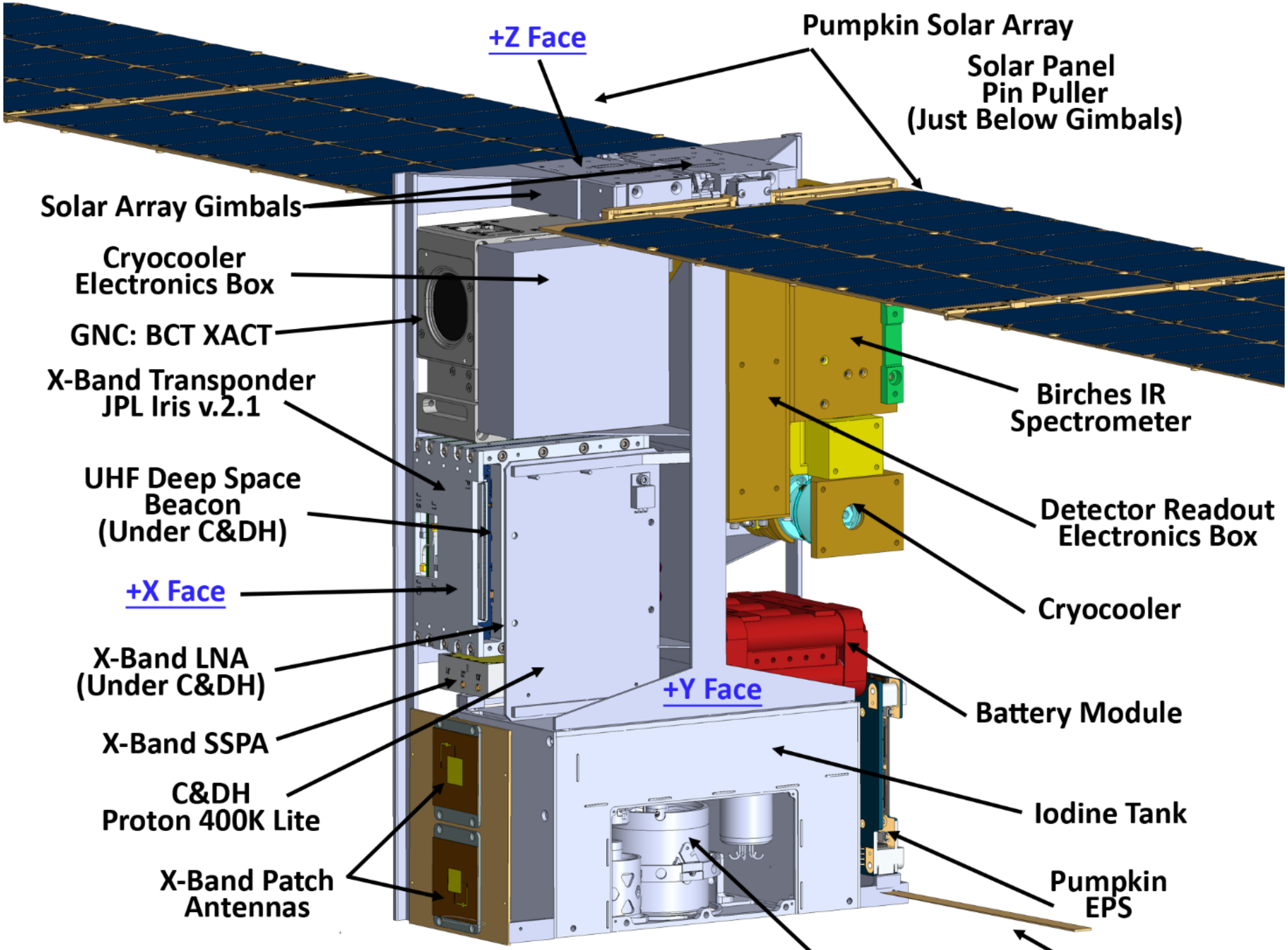


First two stages are Minuteman II, third and fourth stages are Pegasus second and third stages

Lunar IceCube (10cm x 20cm x 30cm)



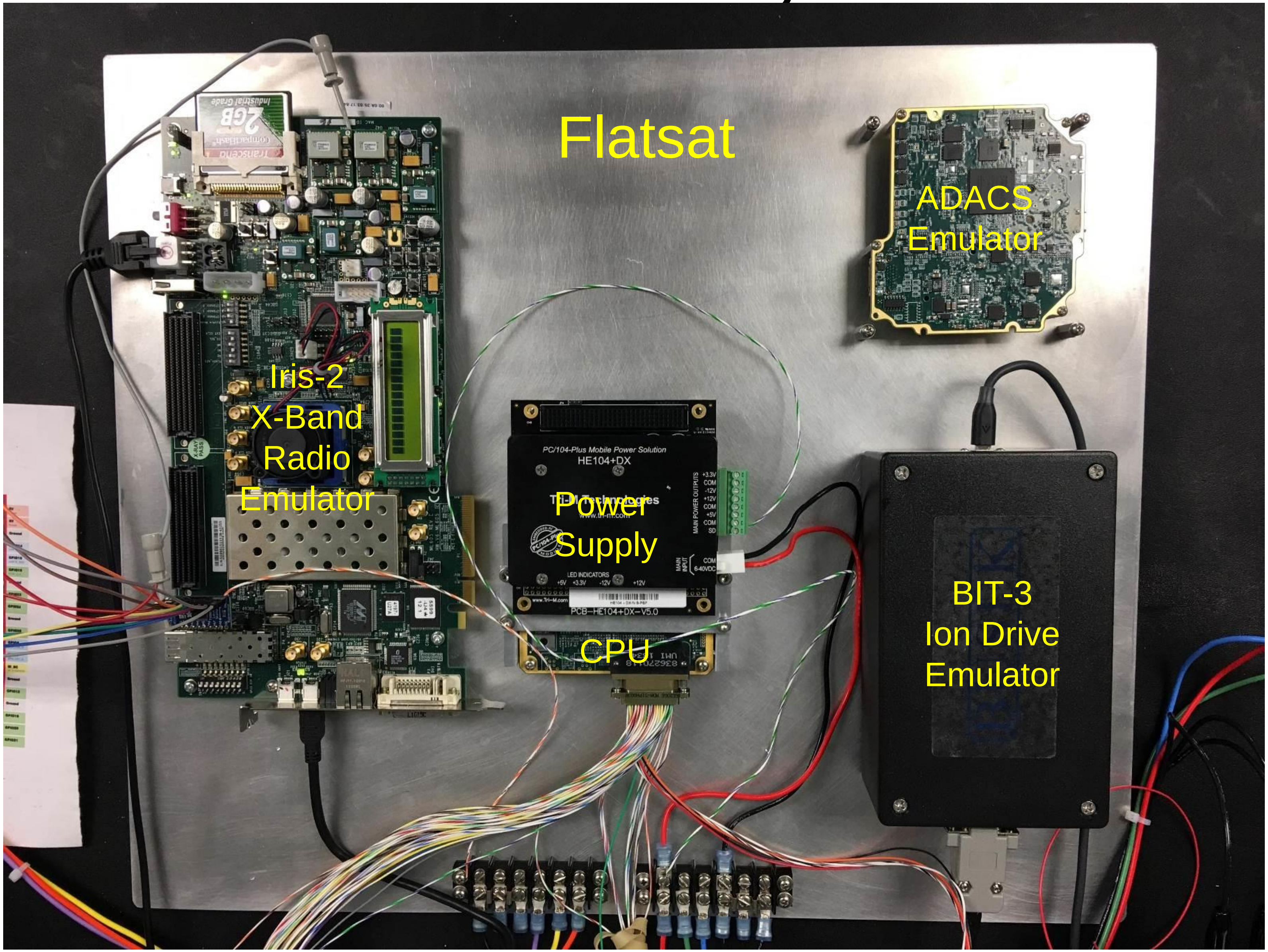
Lunar IceCube 6U CubeSat, Morehead State University, PI., Goddard (BIRCHES IR Spectrometer), JPL (Iris 2 data & nav radio) & Vermont Tech (Flight software). Busek ion drive with 1.5 kg Iodine propellant, Pumpkin photovoltaic array (120 W).


+Z Face
Pumpkin Solar Array
Solar Panel Pin Puller (Just Below Gimbals)
Solar Array Gimbals
Cryocooler Electronics Box
GNC: BCT XACT
X-Band Transponder JPL Iris v.2.1
UHF Deep Space Beacon (Under C&DH)
+X Face
X-Band LNA (Under C&DH)
X-Band SSPA
C&DH Proton 400K Lite
X-Band Patch Antennas
Birches IR Spectrometer
Detector Readout Electronics Box
Cryocooler
Battery Module
+Y Face
Iodine Tank
Pumpkin EPS
UHF Dipole Antenna
Busek BIT-3 Busek RF Ion Thruster

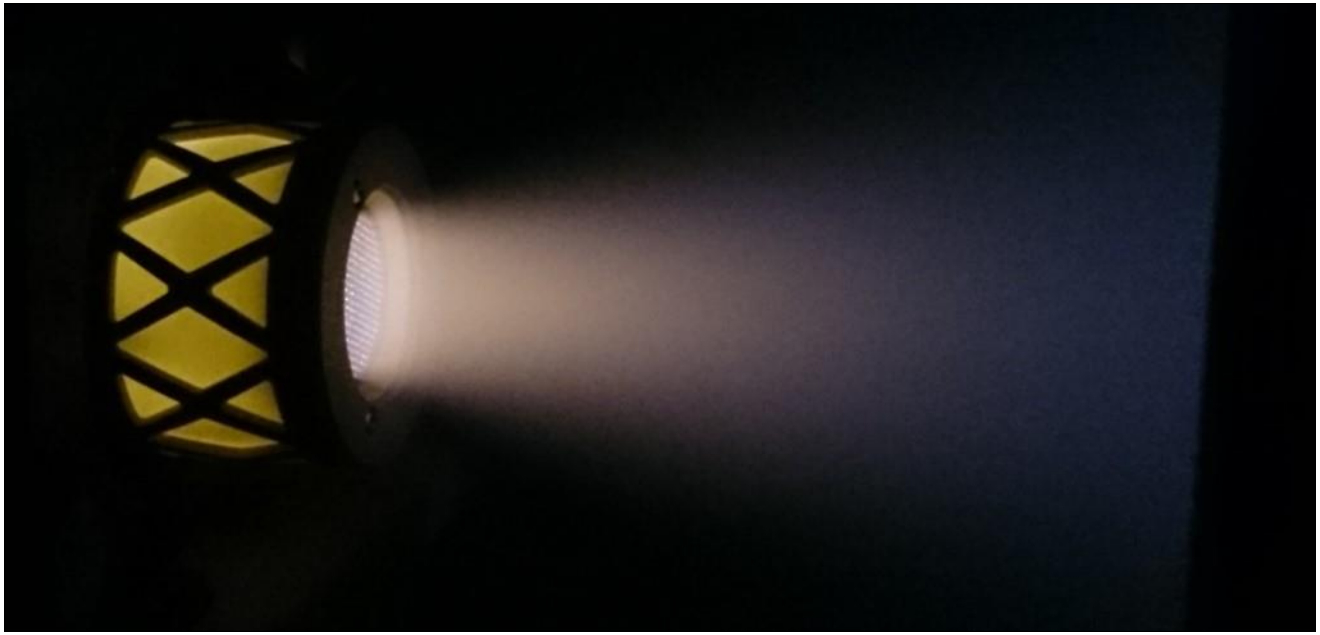
Hardware Controlled by Our Software

- A photovoltaic (PV) panel orientation drive for aiming the panels
- Broadband Infrared Compact High Resolution Exploration Spectrometer (BIRCHES), Goddard Space Flight Center
- Blue Canyon XACT attitude determination and control system (ADACS): star tracker camera, CPU, and 3 momentum wheels
- Iris-2 X-band data & nav radio by NASA's Jet Propulsion Lab
- Busek BIT-3 iodine propellant ion drive (first use in space), controlling thrust and gimbals
- Spiral Thrusting (developed at JPL) for 3-axis momentum wheel desaturating
- Flight software will run on a Space Micro Proton-400 dual core PowerPC, radiation hardened CPU board

Hardware Controlled by Our Software

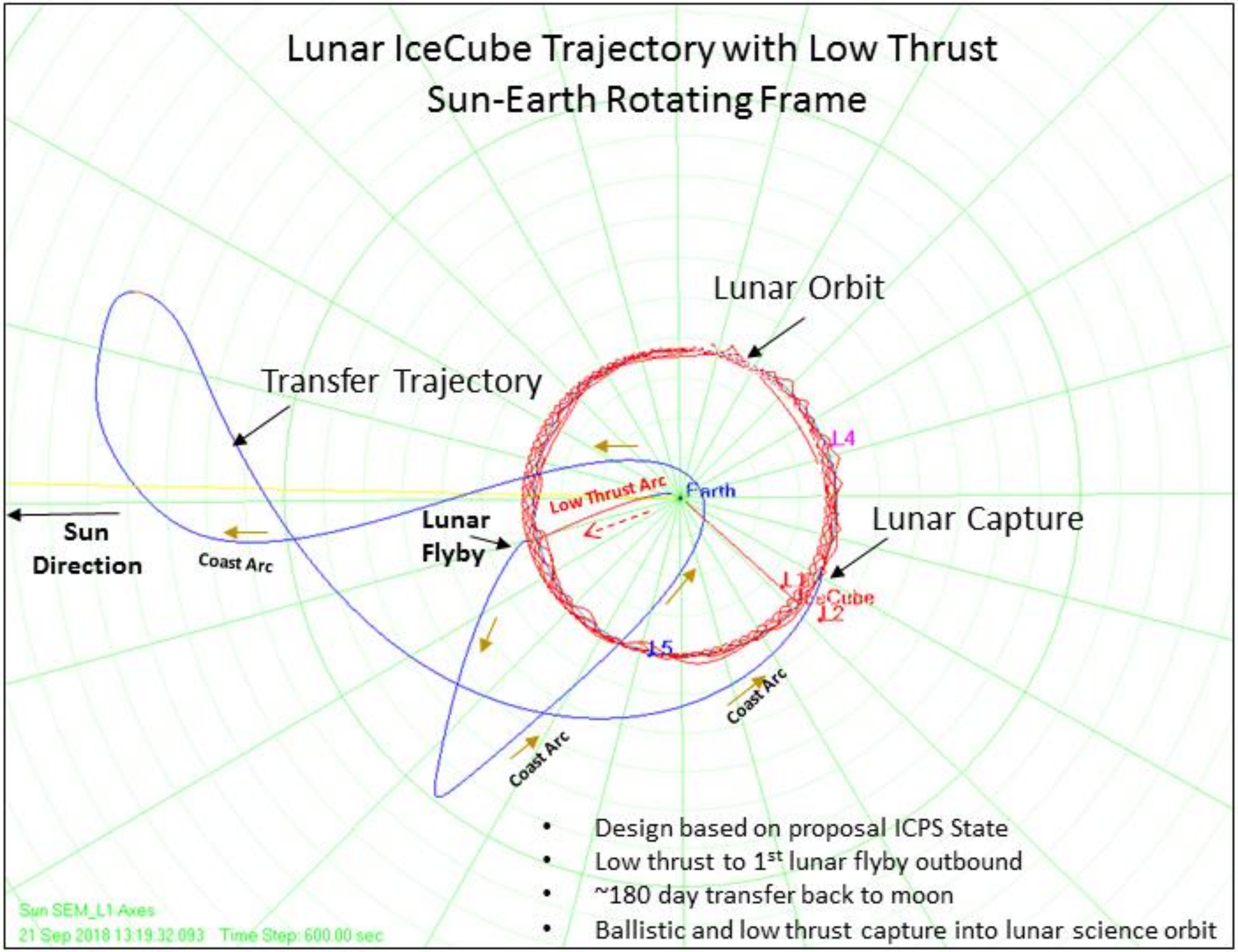


Busek Ion Thruster



BIT-3 Iodine Propellant

75W 1.15 mN, 2.5 cm beam width



Lunar IceCube Trajectory with Low Thrust
Sun-Earth Rotating Frame

- Design based on proposal ICPS State
- Low thrust to 1st lunar flyby outbound
- ~180 day transfer back to moon
- Ballistic and low thrust capture into lunar science orbit

Brandon & Chapin- CDW 2017

Software Environment

- VxWorks 6.8 on PowerPC
- SPARK 2014 with Ravenscar runtime

Developers

- VTC: 2 faculty, 4 students (2 MS, 2 BS)
- Morehead State University: 1 faculty, 1 student (others TBD)

Verification Goals

- No flow errors
- Show freedom from runtime error
- Other correctness properties as time allows

Testing

- Unit tests with AUnit on x86
- Some additional test programs on x86
- Flatsat (development system)
- On flight platform

Continuous Integration

- Jenkins-CI (https://jenkins.io/)
- Daily builds
- Unit tests
- SPARK examination + proof

Software Architecture

Core scheduler

- Accepts “script” of timestamped commands from the ground
- Plays the script by executing commands at appropriate times
- Gathers/accepts telemetry from “modules” associated with each subsystem
- Transmits telemetry (and science data) to the ground
- Minimal autonomous behavior except during deployment

Deployment Tasks

- Stabilize the spacecraft (with help from the XACT unit)
- Deploy and orient solar panels
- Establish communication with Earth via the DSN

Protocols

- CCSDS Space Link protocol for communications over the DSN
- A variation of the Space Link protocol also used for internal communication
- CCSDS File Delivery Protocol (CFDP) for file transfer. We are building a SPARK implementation.

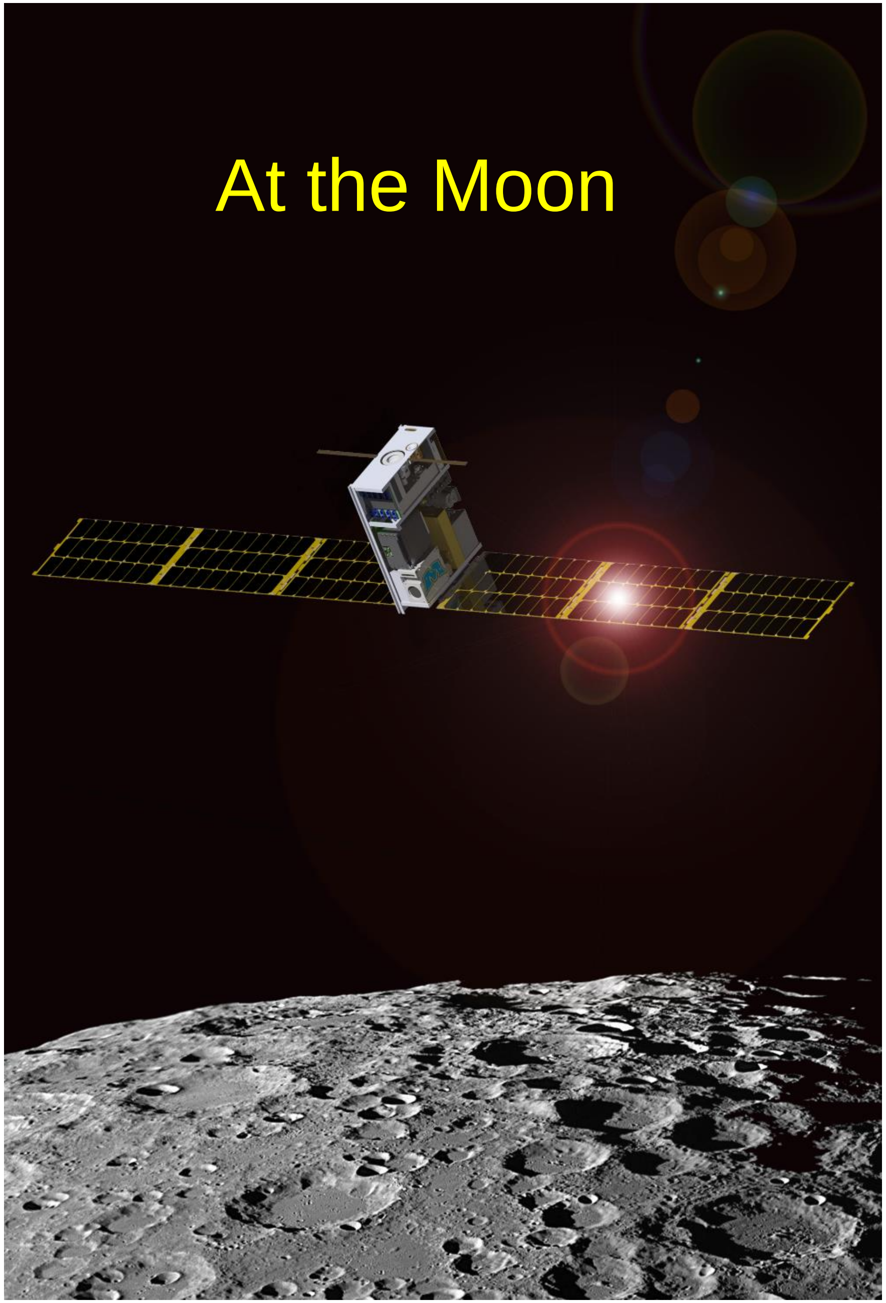
Why not NASA’s cFE?

- What is cFE (Core Flight Executive)
- cFE is written in C. Not verified
- We hope to generalize our work (CubedOS) and eventually offer it as a competing SPARK platform for spacecraft software

VERMONT TECH

Lunar IceCube Launch Vehicle

NASA’s Space Launch System 2018



At the Moon

One of Our Ground Stations

The 70m Dish at Goldstone, California

21m Dish at Morehead State University

Acknowledgements

- NASA Vermont Space Grant Consortium

  NATIONAL SPACE GRANT COLLEGE AND FELLOWSHIP PROGRAM VSGC NASA VERMONT

- Vermont Technical College

  VERMONT TECH

- AdaCore, Inc. (GNAT Pro, SPARK Pro)

  AdaCore The GNAT Pro Company

- Morehead State University

  MOREHEAD STATE UNIVERSITY

- Applied Graphics, Inc. (STK)
- Busek (BIT-3 Iodine ion drive)

  BUSEK

- Pumpkin, Inc.

  PUMPKIN SPACE SYSTEMS

- NASA Jet Propulsion Lab

  NASA Jet Propulsion Laboratory California Institute of Technology

- NASA Goddard Space Flight Center

  NASA Goddard SPACE FLIGHT CENTER

The Use of SPARK in a Complex Spacecraft

CubeSat Developer's Workshop - Copyright 2017 Carl Brandon & Peter Chapin

Dr. Carl Brandon & Dr. Peter Chapin   carl.brandon@vtc.edu peter.chapin@vtc.edu
Vermont Technical College   +1-802-356-2822 (Brandon), +1-802-522-6763 (Chapin)