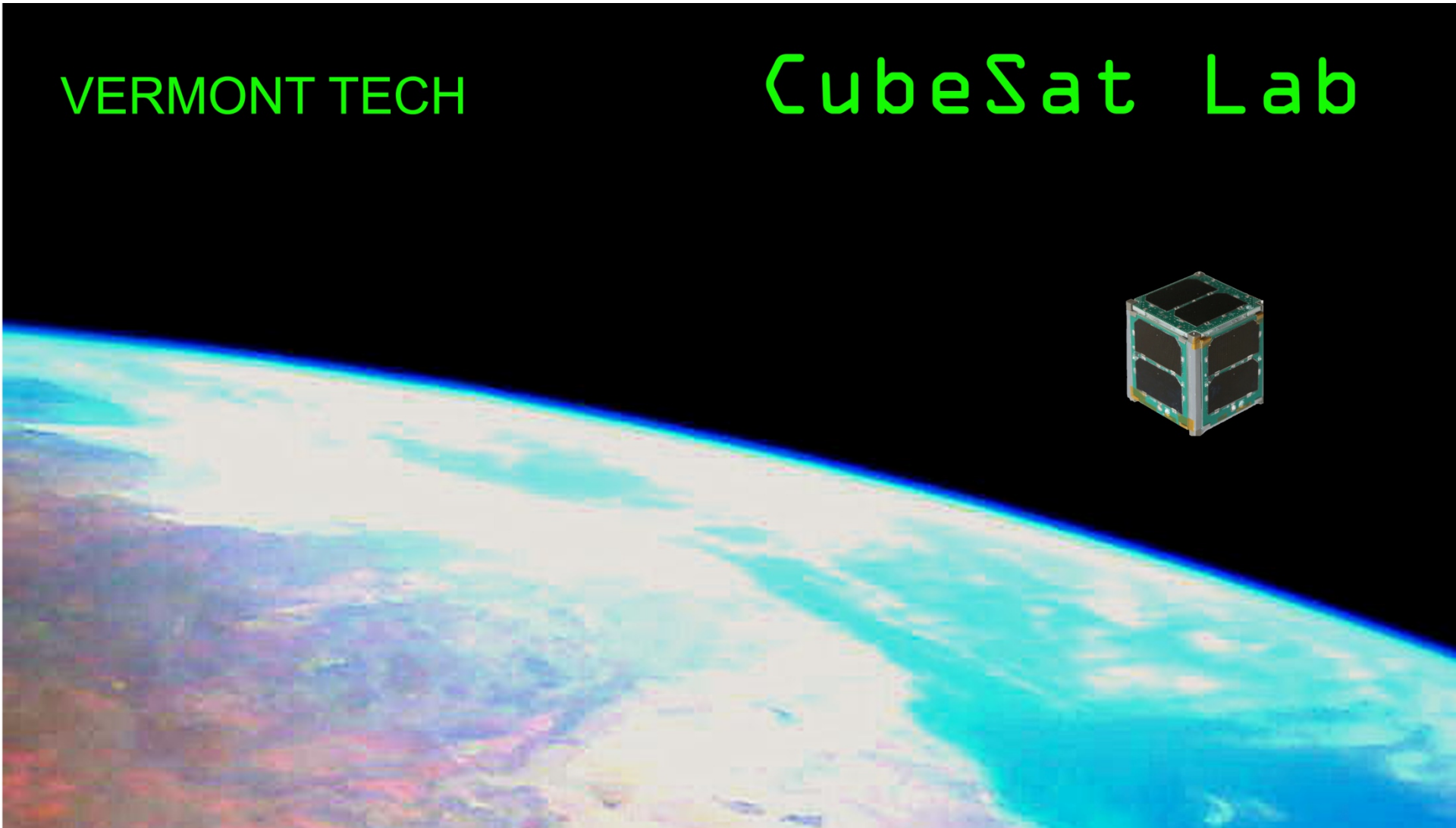
High Integrity Software for Spacecraft

Dr. Carl Brandon & Dr. Peter Chapin
Vermont Technical College
Randolph Center, VT 05061 USA

carl.brandon@vtc.edu
+1-802-356-2822 (Voice)
http://www.cubesatlab.org



NASA ELaNa IV Launch

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 will remain in orbit until about July, 2016. **It is the only one of the 12 ELaNa IV university CubeSats still operating.**
- The Vermont Lunar CubeSat is testing components of a Lunar navigation system in Low Earth Orbit
- **Follow our project at cubesatlab.org**

ELaNa IV Results

- 12 University & 2 NASA CubeSats launched
- Only 4 university CubeSats were heard from at all, 8 were DOA
- One may have lasted part of a week
- One lasted four months
- One fried the batteries the first day (software error)
- Ours, as many Vermonters do, took a 2 ½ month winter vacation

ELaNa IV Results May 8, 2014

Last updated	5/7/2014	by Carl Brandon					
Position	**Payload Name**	**Beacon Heard?**	**Commanding and Telemetry**	**Ground System Status**	**Overall Status**	**Identified by JSpOC?**	**Notes**
1.1-A	Prometheus 1.1					Yes	Prometheus is all green.
1.1-B	Prometheus 1.2					Yes	
1.2-A	Prometheus 2.1					Yes	
1.2-B	Prometheus 2.2					Yes	
1.3	Horus					No	No updates.
1.4	ORSES					Yes	No uplink/downlink established since 25Nov13.
1.5	ORS Tech 1					Yes	No change for ORS Tech 1 – Full communications (uplink and downlink) . Object 39387.
1.6	ORS Tech 2					Yes	No change for ORS Tech 2 – Full communications (uplink and downlink) . Object 39396.
1.7-A	Prometheus 3.1					Yes	Prometheus is all green.
1.7-B	Prometheus 3.2					Yes	
1.8-A	Prometheus 4.1					Yes	
1.8-B	Prometheus 4.2					Yes	
2.1	SENSE SV 1					Yes	1 of 2 solar panels deployed, currently experiencing a low-power anomaly. No contact with SV for 7 days in January, working through fishbone anaylsis.
2.2	H2					No	No change since last report
2.3-A	Vermont Lunar					Yes	Working
2.3-B	TJ3Sat					No	No change since last report
2.3-C	Black Knight 1					No	No change for Black Knight 1. We have MIT Lincoln Labs testing our ground station radio and LNA right now. Anticipate renewed contact efforts in two weeks.
2.4	Firefly					Yes	Firefly continues to be GREEN (spacecraft). Ground station is YELLOW (cold weather issues, next expected contact Thursday). We are commissioning the spacecraft, preparing to enter science mode in February.
2.5-A	KYSat II					Yes	No changes from last week, using 39384 to track. Still no reliable uplink haven't been able to use 21 meter dish at Morehead State University due to snow and ice in the area. Ground stations and spacecraft are currently green.
2.5-B	NPS-SCAT					Maybe	Still no contact with NPS-SCAT since last contact reported. No other updates but we are currently using the new 39389 object allocation in our attempts.
2.5-C	CAPE 2					Yes	Only works in sunlight. Batteries dead.
2.6-a	DragonSat-1					No	No satellite contact; good ground station.
2.6-B	PhoneSat					Yes	Tracked and working.
2.6-C	SPA-1 Trailblazer					No	Trailblazer still not heard from. We are now continuing to look at those two TLEs and are hopeful. Satellite Red, Ground Station Green.
2.7-A	COPPER					No	No changes to COPPER.
2.7-B	SwampSat					No	There is no update from SwampSat. We have been using the information from JSpOC to track, however, we are unable to communicate with SwampSat. Also, our ground station is fully functional.
2.7-C	ChargerSat					No	No change in SV status. We are currently repairing wind damage on our antenna mount, and as such, have not been able to utilize the information provided by JSpOC.
2.8	SENSE SV 2					Yes	Averaging 5 contacts per day. Yellow, 0 of 2 solar panels deployed, shedding loads to regain positive power balance. Beginning payload checkout as power balance allows.

Reliability issues from ELaNa IV

Software reliability issues:

- Design reviews
- Language selection (SPARK/Ada)
- Static analysis tools (SPARK 2005)
- Repository (Assembla)
- ISIS (Holland, not Syria) antenna electrical model testing

Software reliability issues:

- Most CubeSats have used C
- Ada, alone has 10% of the C error rate
- SPARK/Ada with the SPARK toolset has 1% of the C error rate
- Students became productive with SPARK in a couple of weeks

SPARK/Ada is used in:

Commercial aviation:

- Rolls-Royce Trent jet engines
- ARINC ACAMS system

Military aviation:

- EuroFighter Typhoon
- Harrier GR9
- AerMacchi M346
- Lockheed Martin C130J

Air-traffic management: (UK NATS iFACTS system)

Rail: (numerous signaling applications)

Medical: (LifeFlow ventricular assist device)

Our current SPARK 2005 CubeSat 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 allow 100%

Our new SPARK 2014 CubedOS CubeSat software:

- General purpose CubeSat software system
- Written in SPARK/Ada & proven free from runtime errors
- Currently in development for use in 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

Our new SPARK 2014 CubedOS CubeSat software:

• An asynchronous message passing system with mailboxes. This, together with the underlying Ada runtime system constitutes the "kernel" of CubedOS.
•A runtime library of useful packages, all verified with SPARK.
•A real time clock module.
•A file system interface.
•A radio communications interface.
•Modules providing support for CCSDS (Consultative Committee for Space Data Systems) protocols.
• A general driver model that allows components to communicate with drivers fairly generically

CubedOS provides several advantages over "home grown" frameworks:

- The message passing architecture is highly concurrent and allows many overlapping activities to be programmed in a natural way.
- For example, our implementation of the CCSDS File Delivery Protocol (CFDP) used in the Deep Space Network takes advantage of this.
- The architecture provides a lot of runtime flexibility; programs can adapt their communication patterns at runtime.
- The architecture is consistent with the restrictions of Ada's Ravenscar profile (for safe concurrency).

CubedOS also brings several disadvantages over more customized solutions:

- Because CubedOS messages are just octet sequences, there is runtime overhead associated with encoding and decoding them.
- CubedOS sacrifices some static type safety; decoded messages must be validated at runtime with type errors being handled during the validation process. This is particularly worrisome in light of CubedOS's goal of providing robust assurances of correctness.
- It is unclear at this time how analyzable CubedOS will be with the SPARK tools. We await access to SPARK 2014 tools that can process tasking constructs.

CubedOS:

- CubedOS is an ongoing effort and should be considered experimental at this time.
- However, we hope to refine the architecture and implement enough non-trivial services to make CubedOS useful to other groups.
- Our long term goal is to distribute CubedOS to others working on CubeSat software or, for that matter, other similar embedded systems.

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)

Some examples of SPARK annotations (which are Ada comments):

```
--# global in out Counter;
--# derives Counter from Counter, Table, Value &
--#         Found, Index from Table, Value;
--# pre  Counter < Integer'Last;
--# post Found -> (Table(Index) = Value and
                   Counter = Counter~ + 1);
```

-- precedes an Ada comment
--# indicates a SPARK annotation
~ indicates the initial value

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

- Ariane 5 initial flight failure
- Boeing 787 generator control computer shutdown

Ariane 5 initial flight failure:

Good

Bad, 37 seconds later

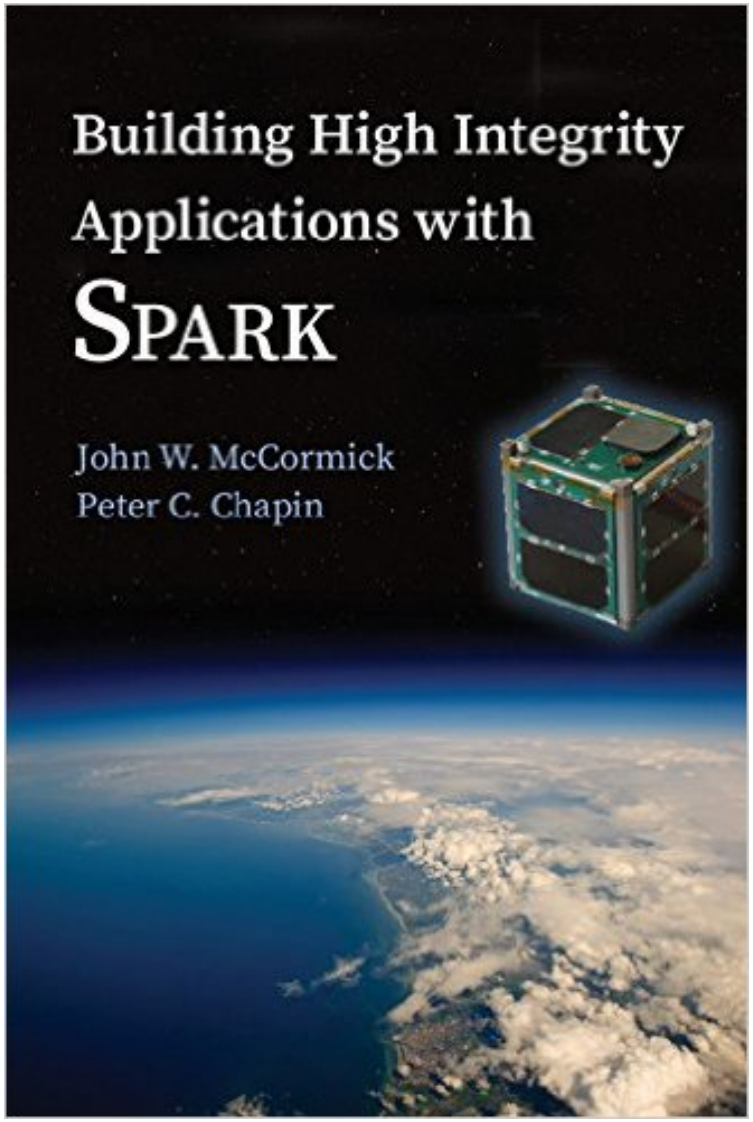
Ariane 5 initial flight failure:

- 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 close to $500,000,000.
- SPARK/Ada would have prevented this failure

Boeing 787 generator control computer:

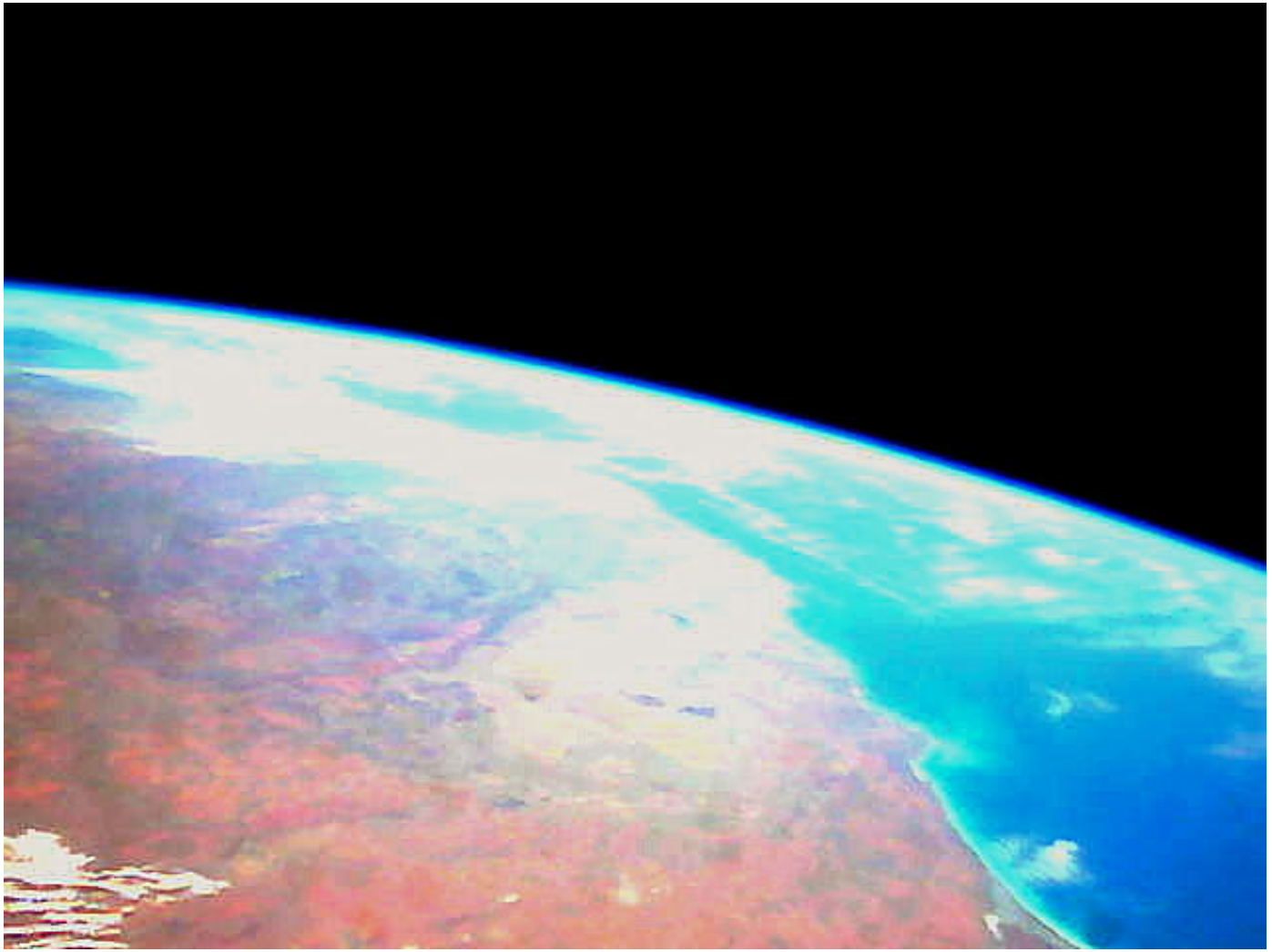
- There are two generators for each of two engines, each with its own control computer programmed in Ada
- The computer keeps count of power on time in centiseconds in a 32 bit register
- Just after 8 months elapses, the register overflows
- Each computer goes into “safe” mode shutting down its generator 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
- SPARK/Ada would have prevented this

A SPARK 2014 book is now available:

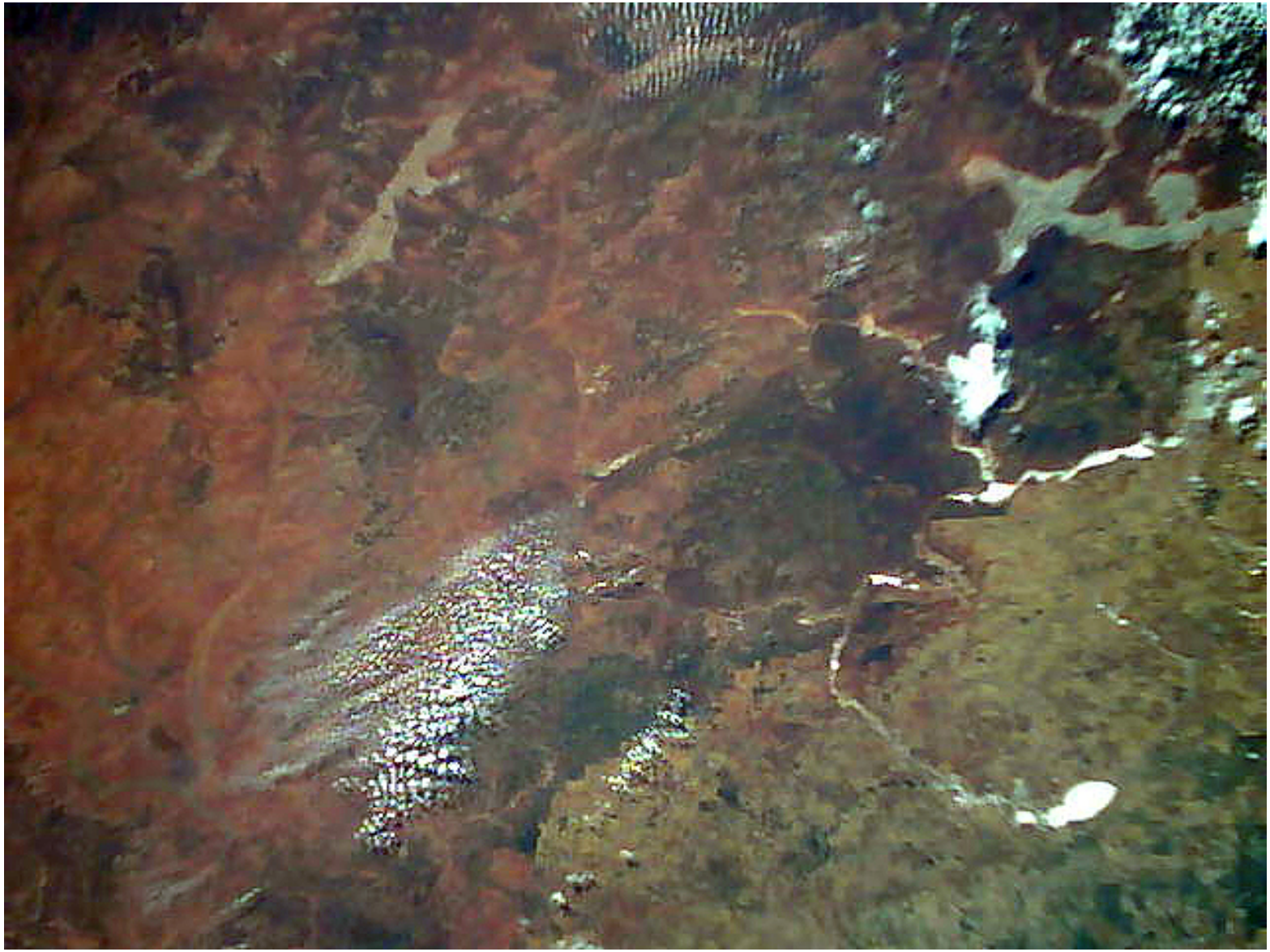


Vermont Lunar CubeSat

VERMONT TECH

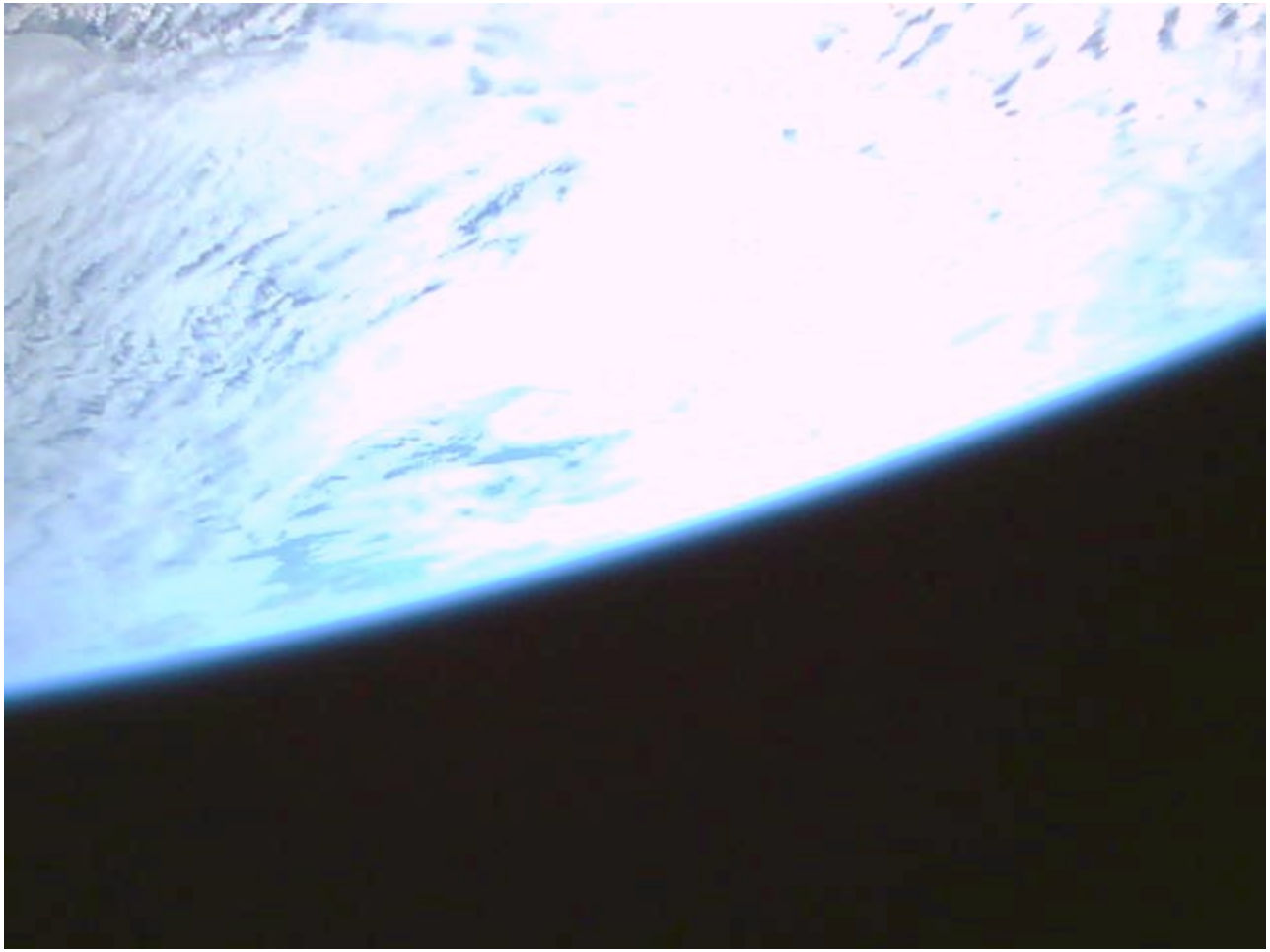


Our first picture of Earth, February 2014
The North coast of Western Australia near Port Hedland



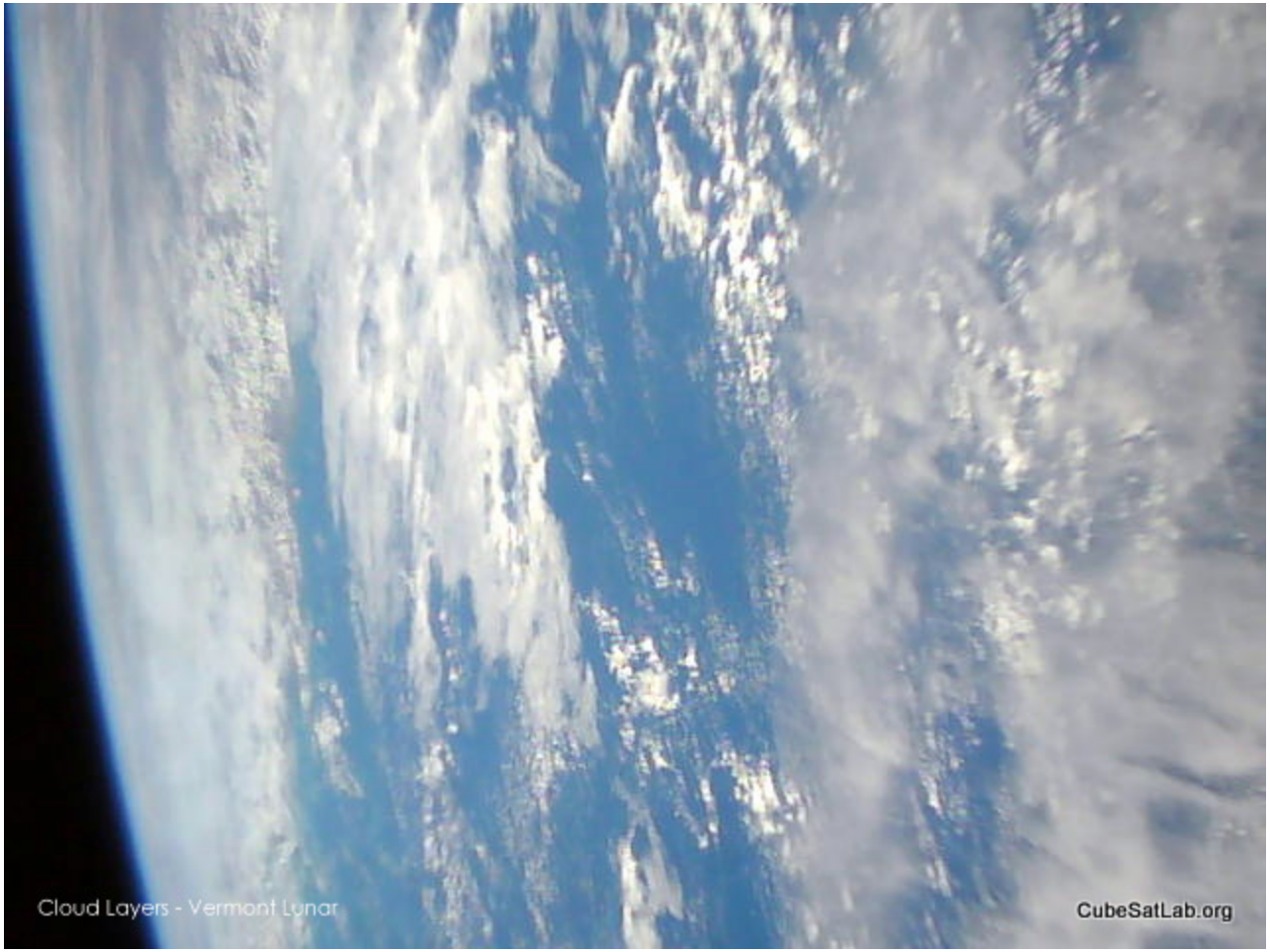
Western Australia north of Perth

Vermont Lunar CubeSat



More clouds.

Vermont Lunar CubeSat



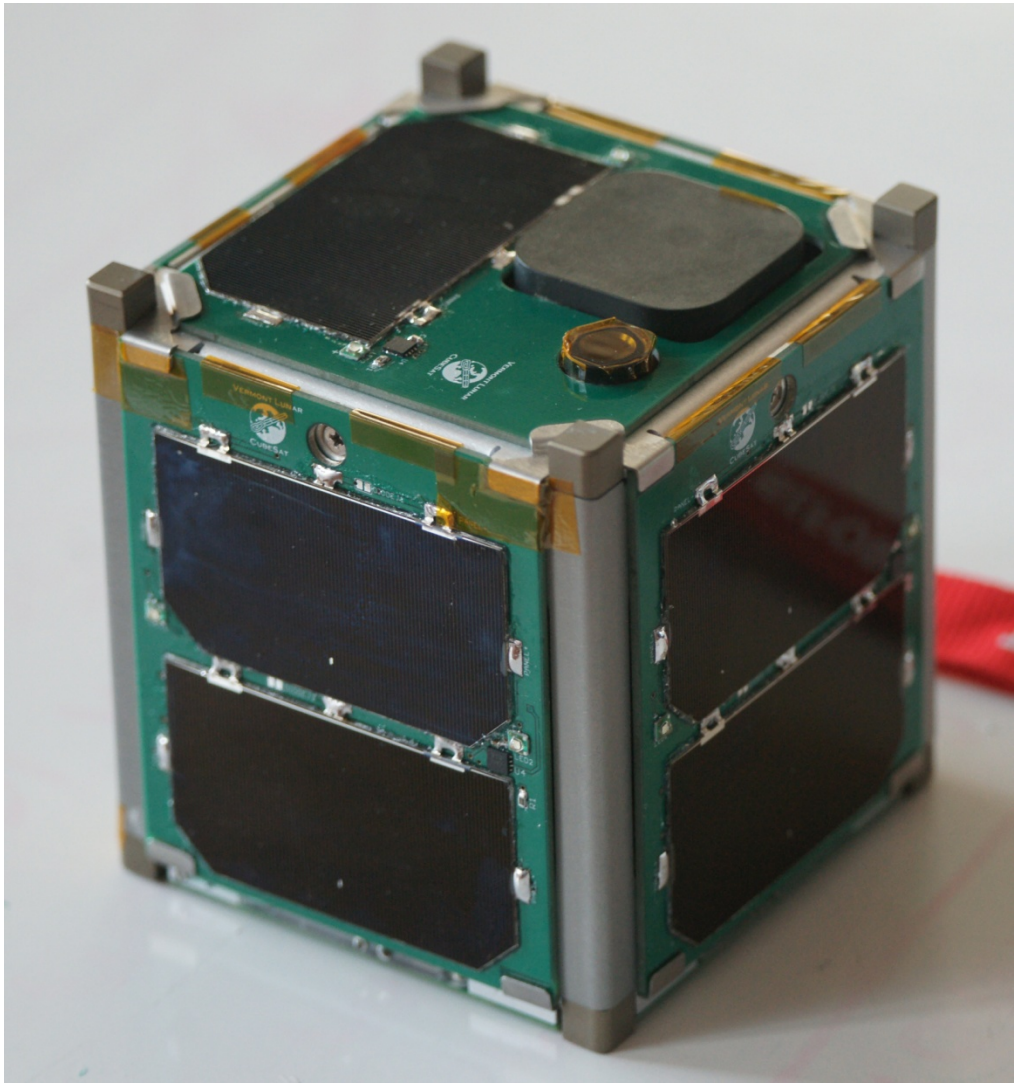
Clouds over the ocean, June 2015.

Vermont Lunar CubeSat

Clouds over the ocean, September 2015.

Vermont Lunar CubeSat

VERMONT TECH



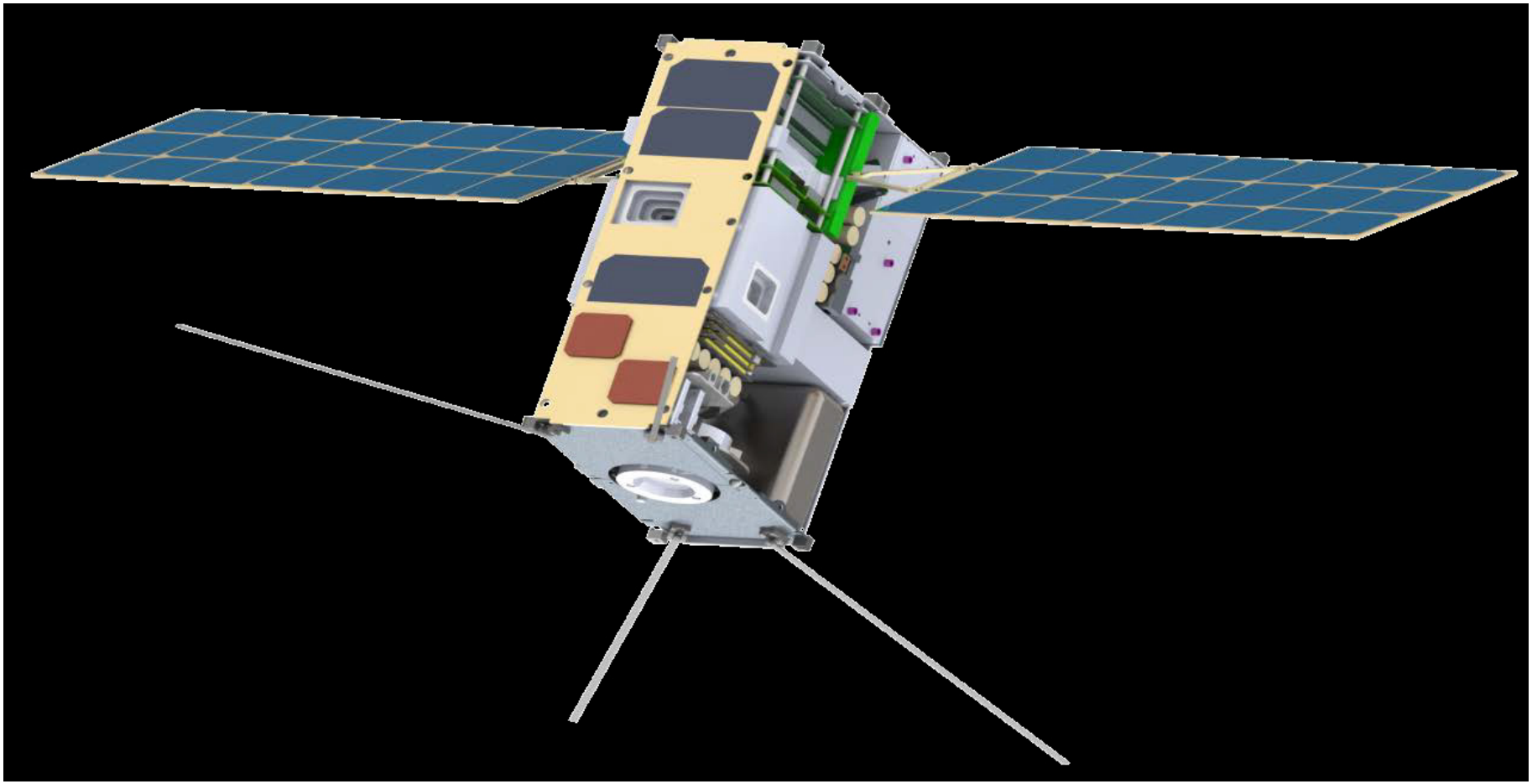
Vermont Lunar CubeSat (10 cm cube)

Software Development Comments for our first CubeSat

VERMONT TECH

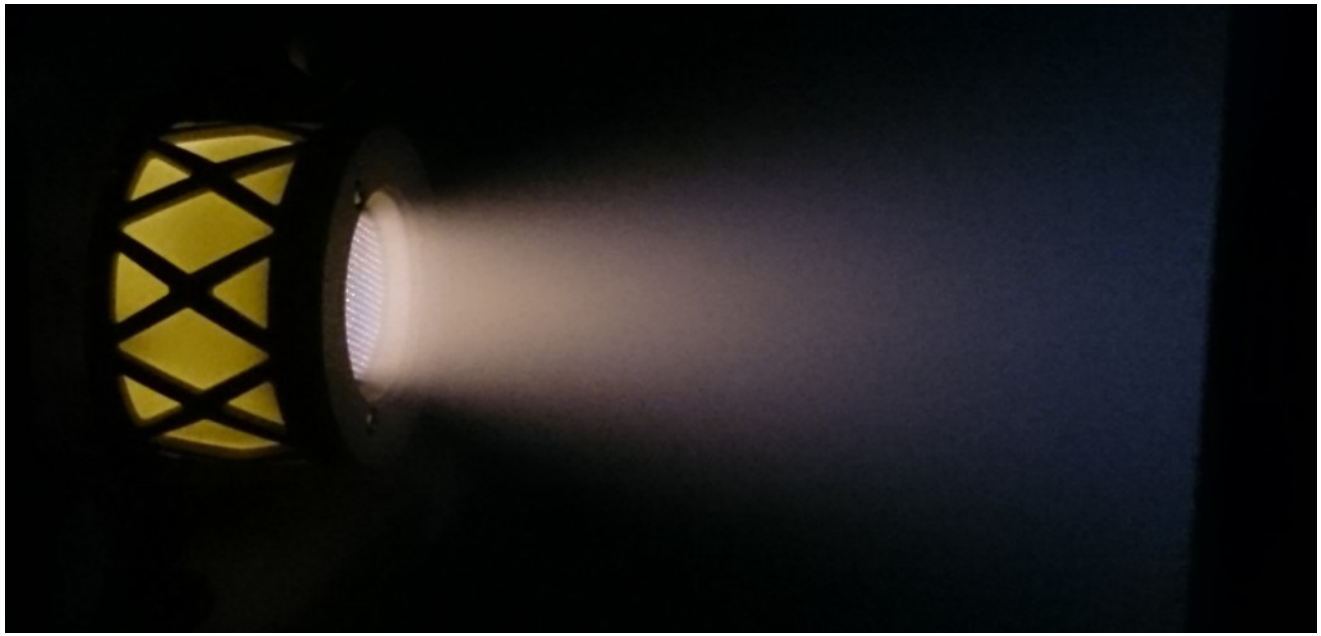
- SPARK caught errors as we refactored the software as we developed greater understanding of the hardware
- SPARK helped the discipline of the software during turnover as some students graduated and were replaced
- Although we did not have a formal development process, without SPARK we probably would not have completed the project with the limited personnel resources and tight time constraint
- Although the CubeSat is limited to 1.3kg, the paperwork might be 13 kg ;-)

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.

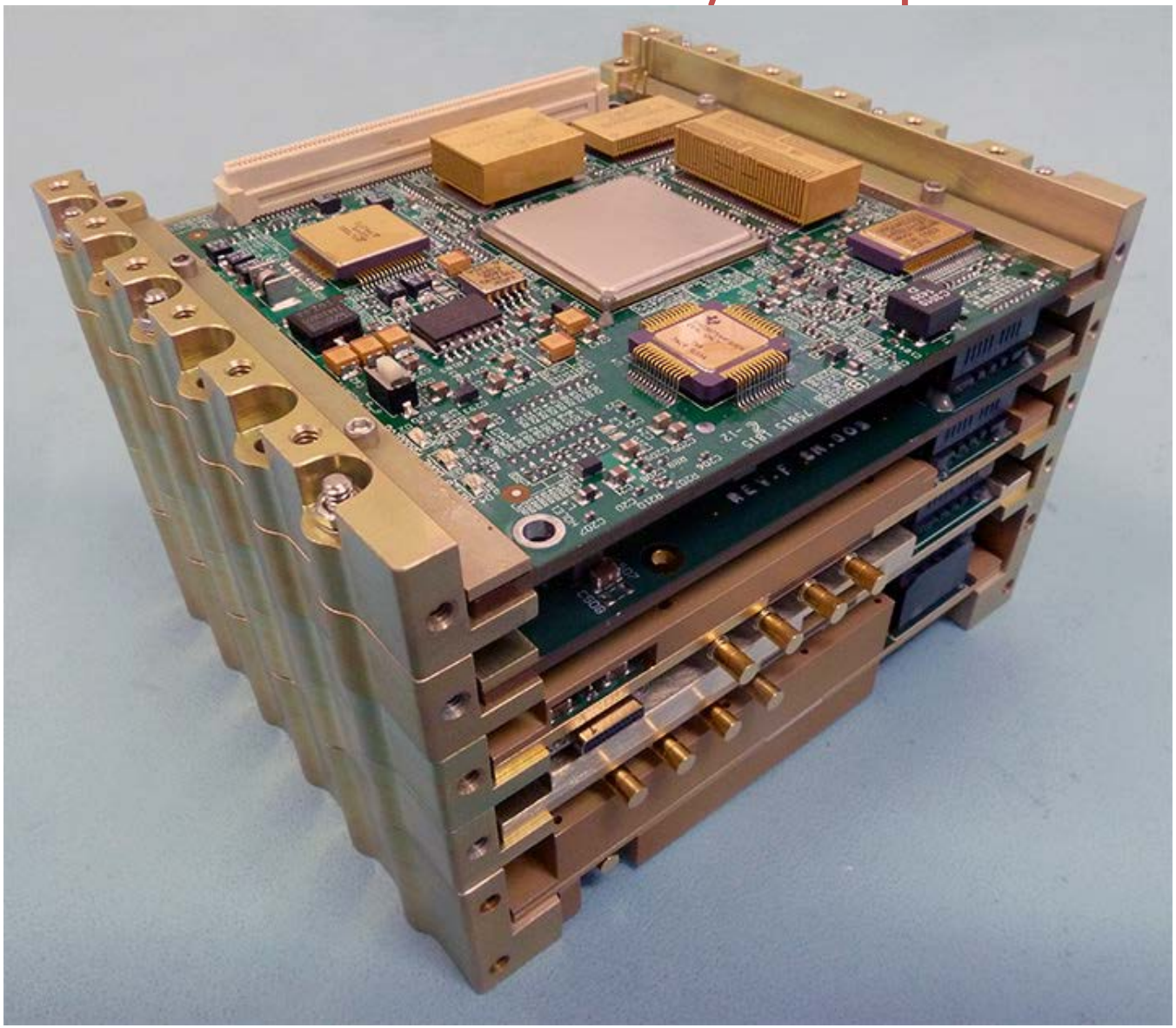
Busek Ion Thruster



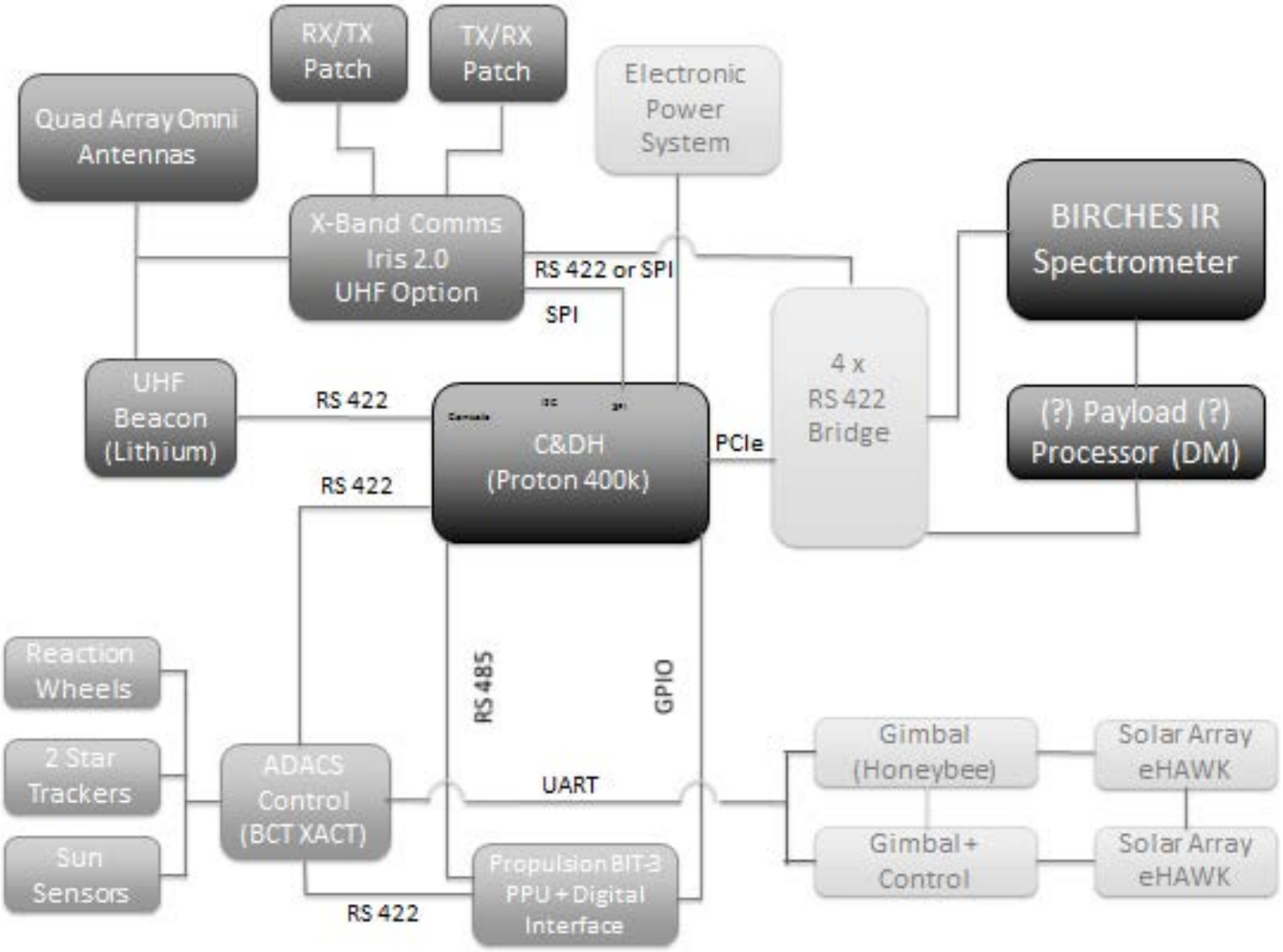
BIT-3 Iodine Propellant

65W 1.4 mN, 3 cm beam width

JPL Iris 2 X-Band Radio/Transponder



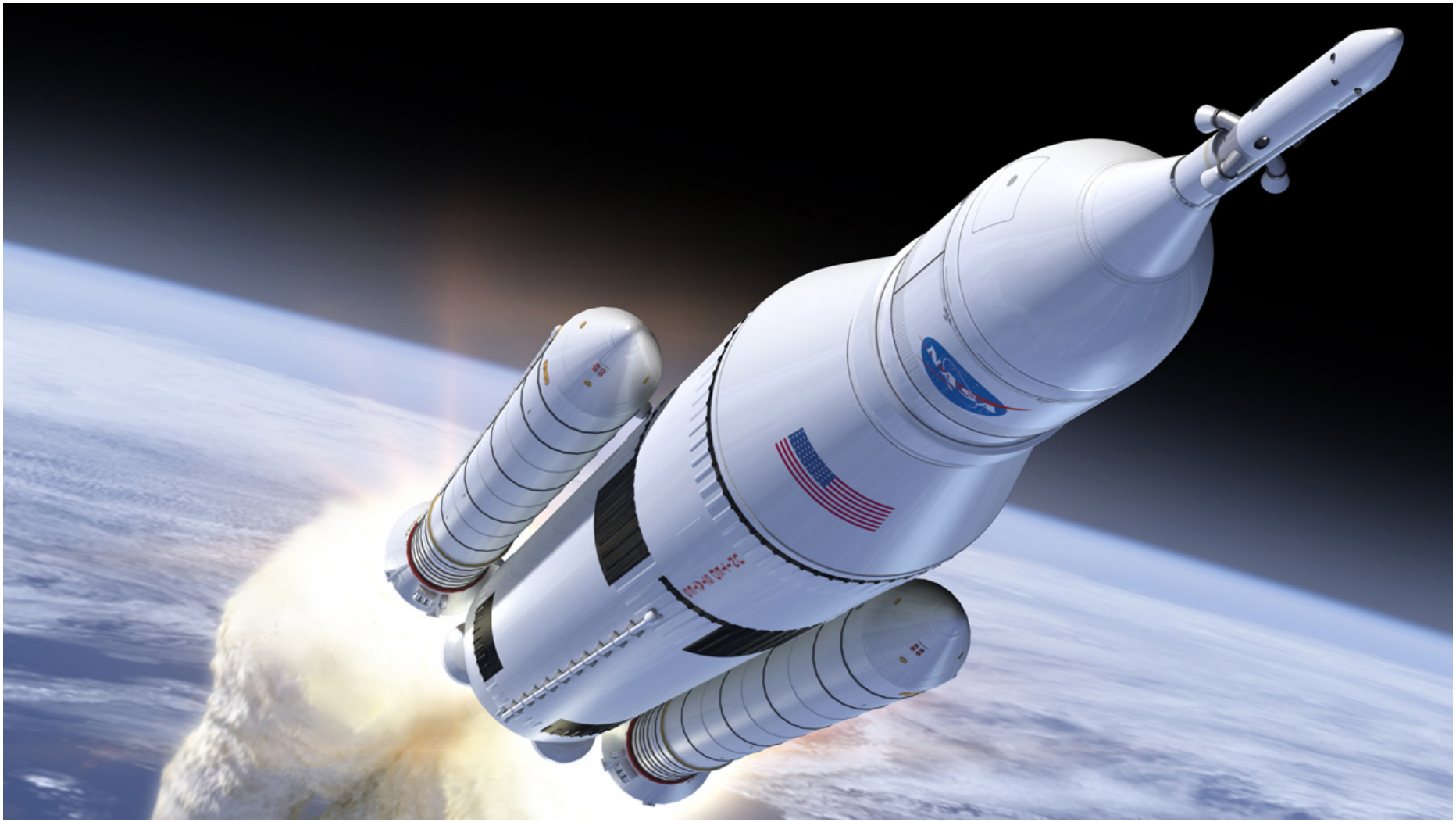
Lunar IceCube Block Diagram



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

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

Lunar IceCube Launch Vehicle



NASA's Space Launch System 2018

Acknowledgements

- NASA Vermont Space Grant Consortium
- NASA
- Vermont Technical College
- AdaCore, Inc. (GNAT Pro)
- Altran Praxis (SPARK)
- SofCheck (AdaMagic)
- Applied Graphics, Inc. (STK)
- LED Dynamics (PV boards)
- Microstrain (IMU)

High Integrity Software for Spacecraft

Dr. Carl Brandon & Dr. Peter Chapin
Vermont Technical College
Randolph Center, VT 05061 USA

carl.brandon@vtc.edu
+1-802-356-2822 (Voice)
http://www.cubesatlab.org