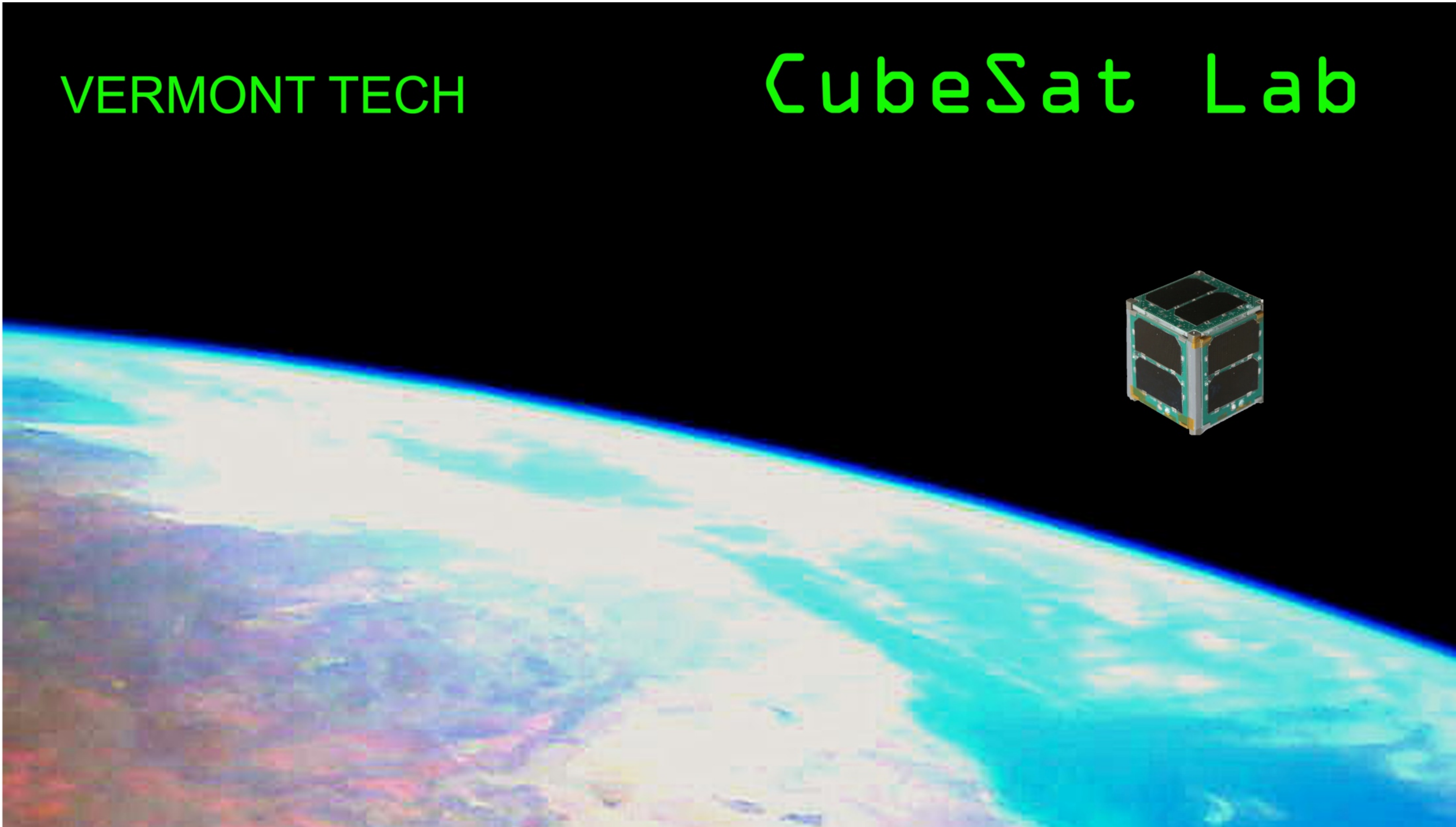
High Integrity Software for CubeSats and Other Space Missions

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



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% proofs

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:

- 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

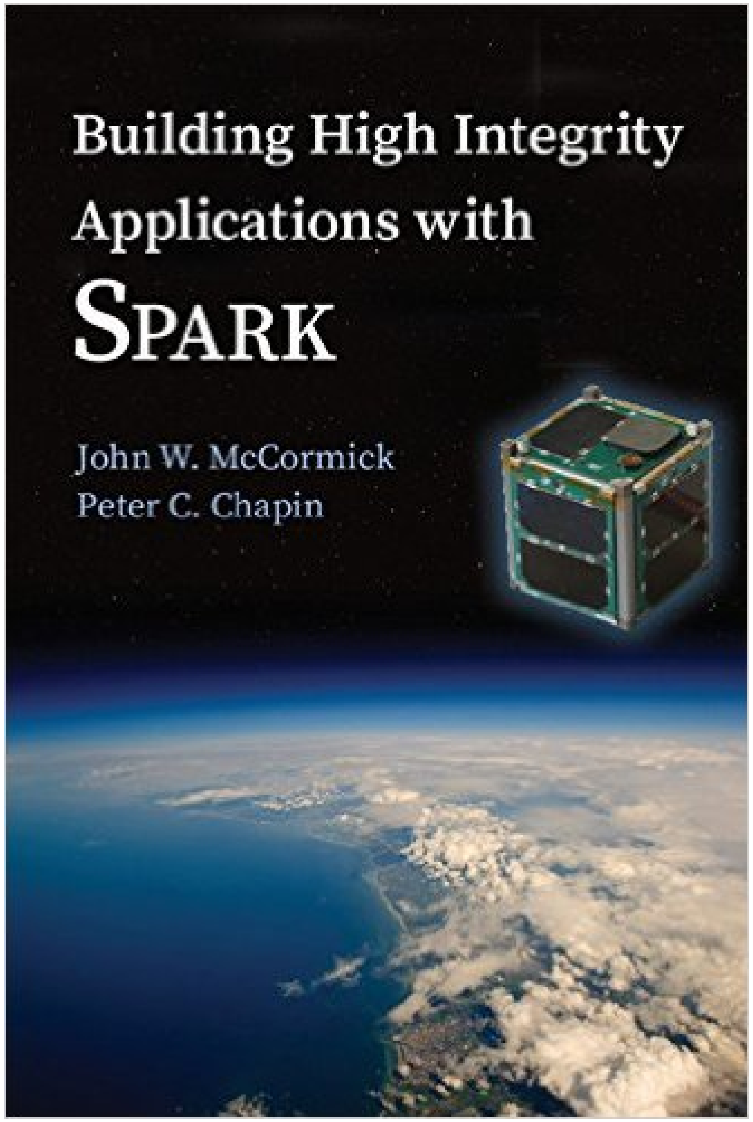
Ariane 5 initial flight failure:

- 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

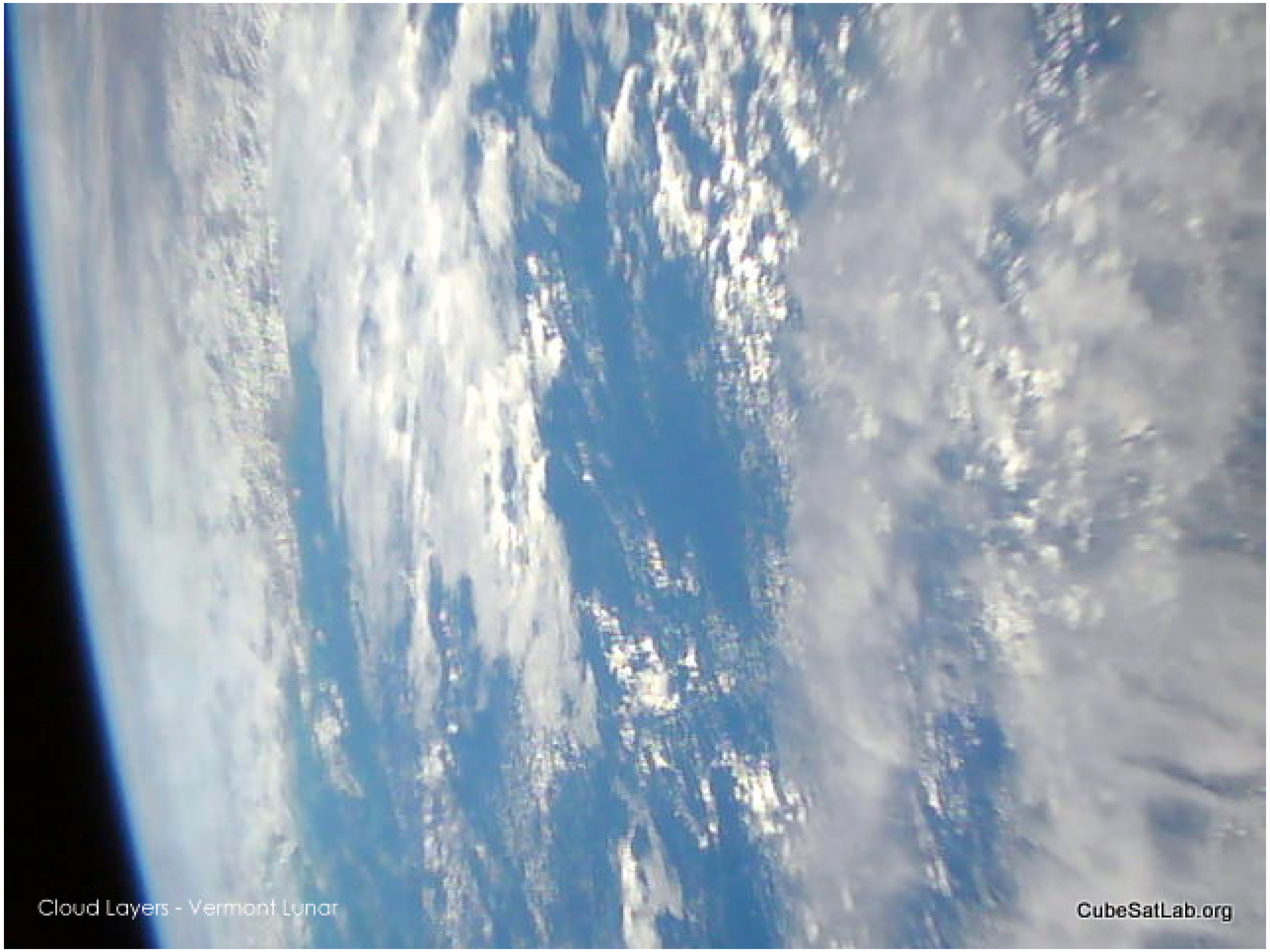
A SPARK 2014 book is now available:



Building High Integrity Applications with SPARK

John W. McCormick
Peter C. Chapin

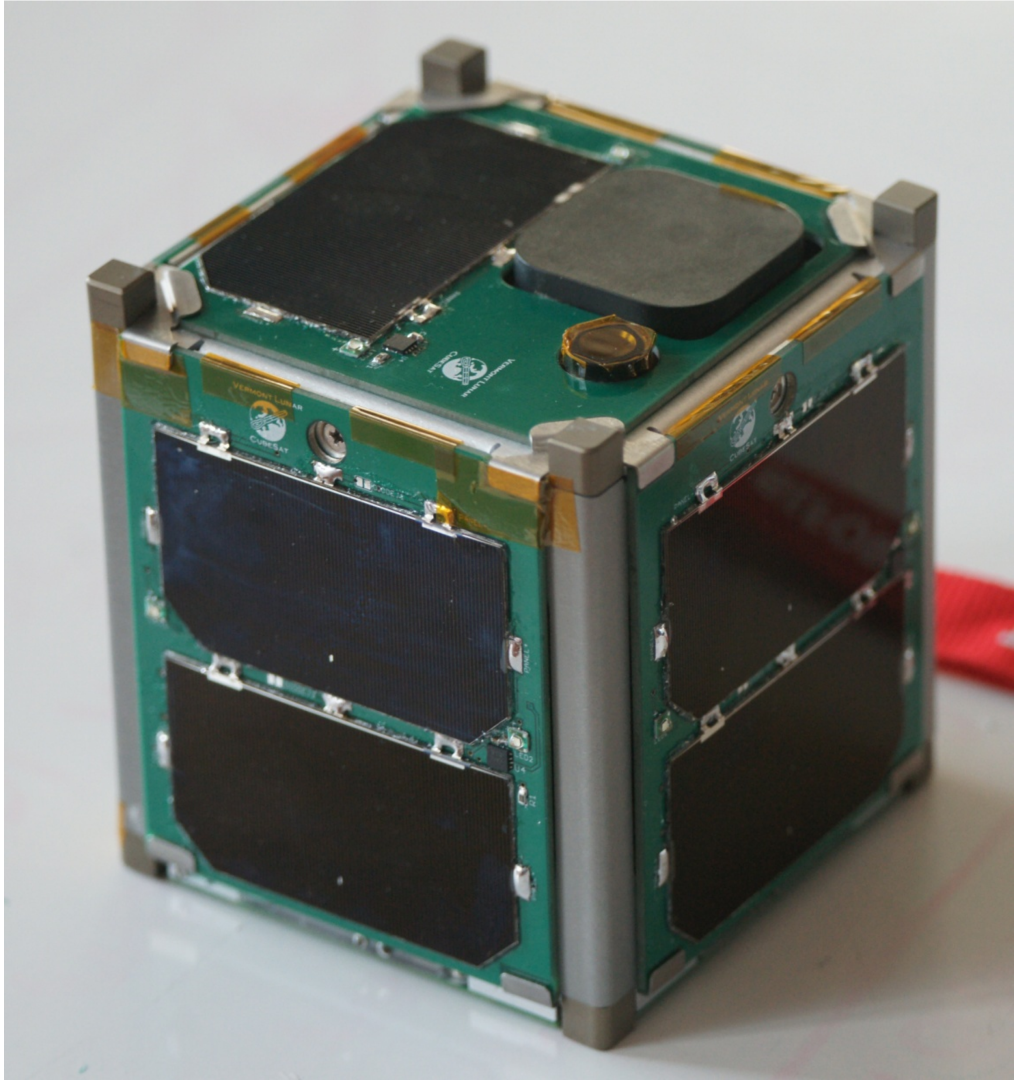
Vermont Lunar CubeSat



Clouds over the ocean, June 2015.

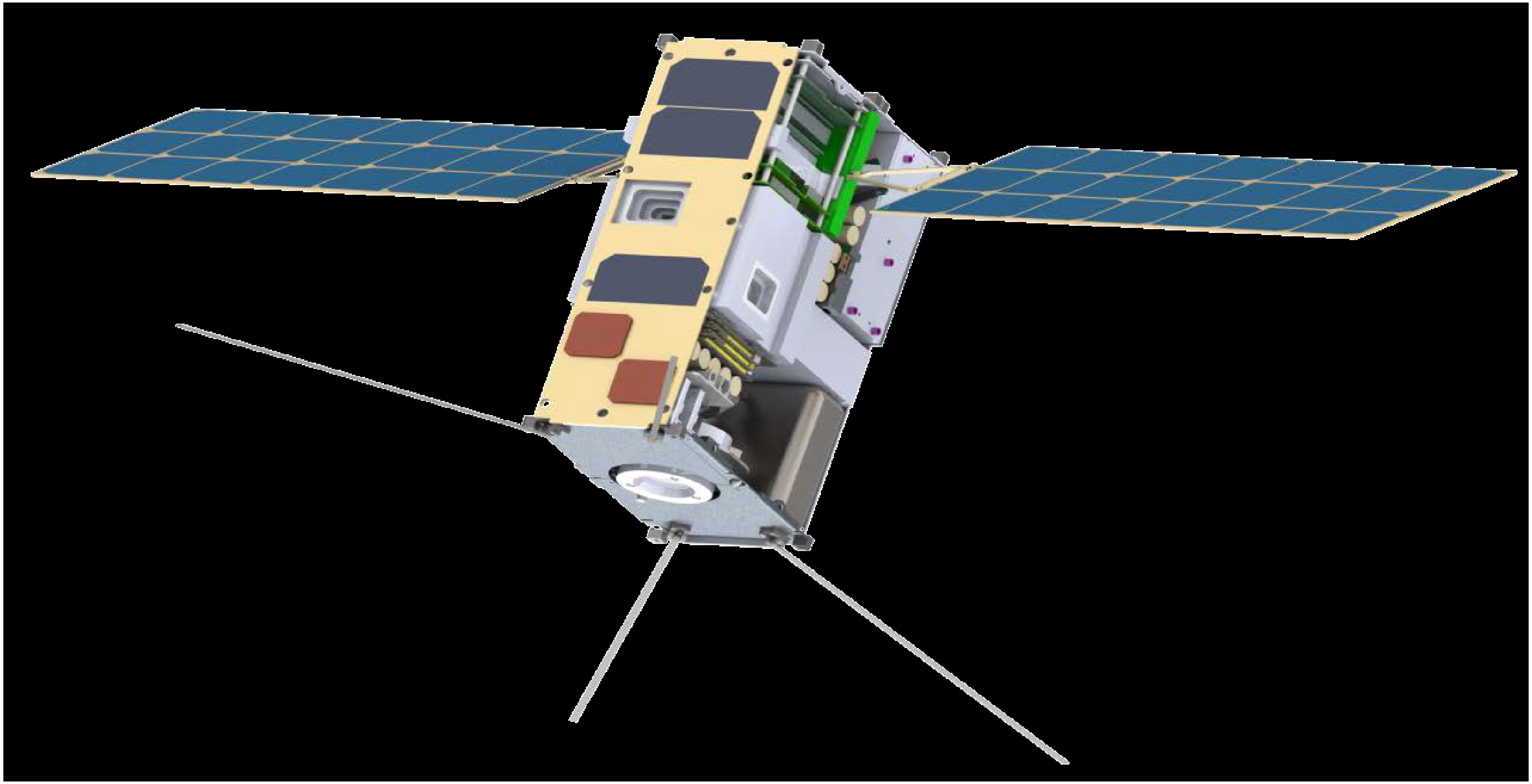
Vermont Lunar CubeSat

VERMONT TECH



Vermont Lunar CubeSat (10 cm cube)

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.