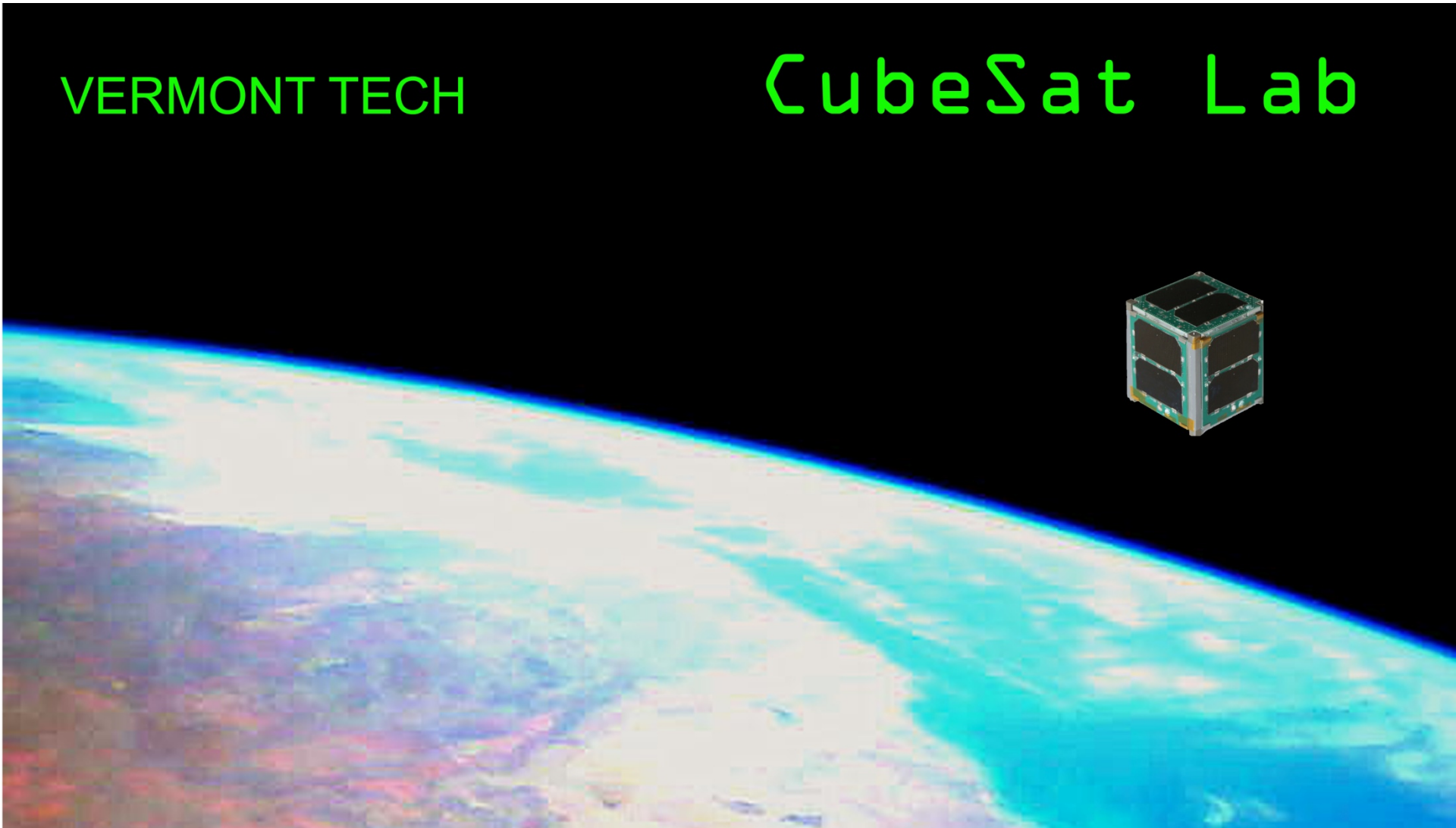
High Integrity Software for CubeSats and Other Space Missions

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



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, 40.5^{o} 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
- **Follow our project at cubesatlab.org**

Ada and SPARK

- The Ada language originally issued in 1983 has been revised in 1995, 2005 and 2012

- Although originally developed at the behest of the Defense Department, Ada has taken over the niche for very high integrity software, as SIGAda says: “When the software really has to work”

- As a result, Ada is used in all commercial airline avionics and all air traffic control systems worldwide, as well as high speed trains and nuclear power plants in Europe

SPARK/Ada is used in:

Commercial aviation:

- Rolls-Royce Trent jet engines (on the Airbus)
- 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)

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 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 during the development of the Lunar IceCube software 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 or other space 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 software only had to run for 40 secs
- The exception halted the reference platforms, resulting in the destruction of the flight at 37 secs.
- Financial loss over $500,000,000.
- SPARK/Ada would have prevented this failure

Ariane 5 initial flight failure:

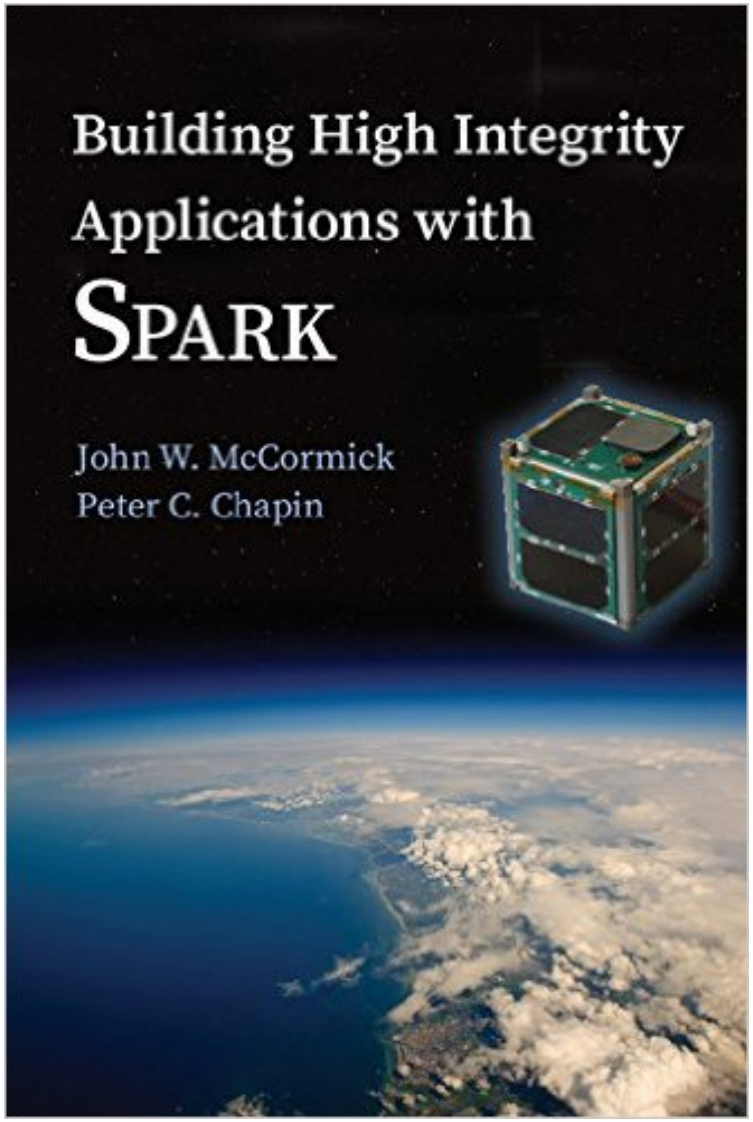
Good

Bad, 37 seconds later

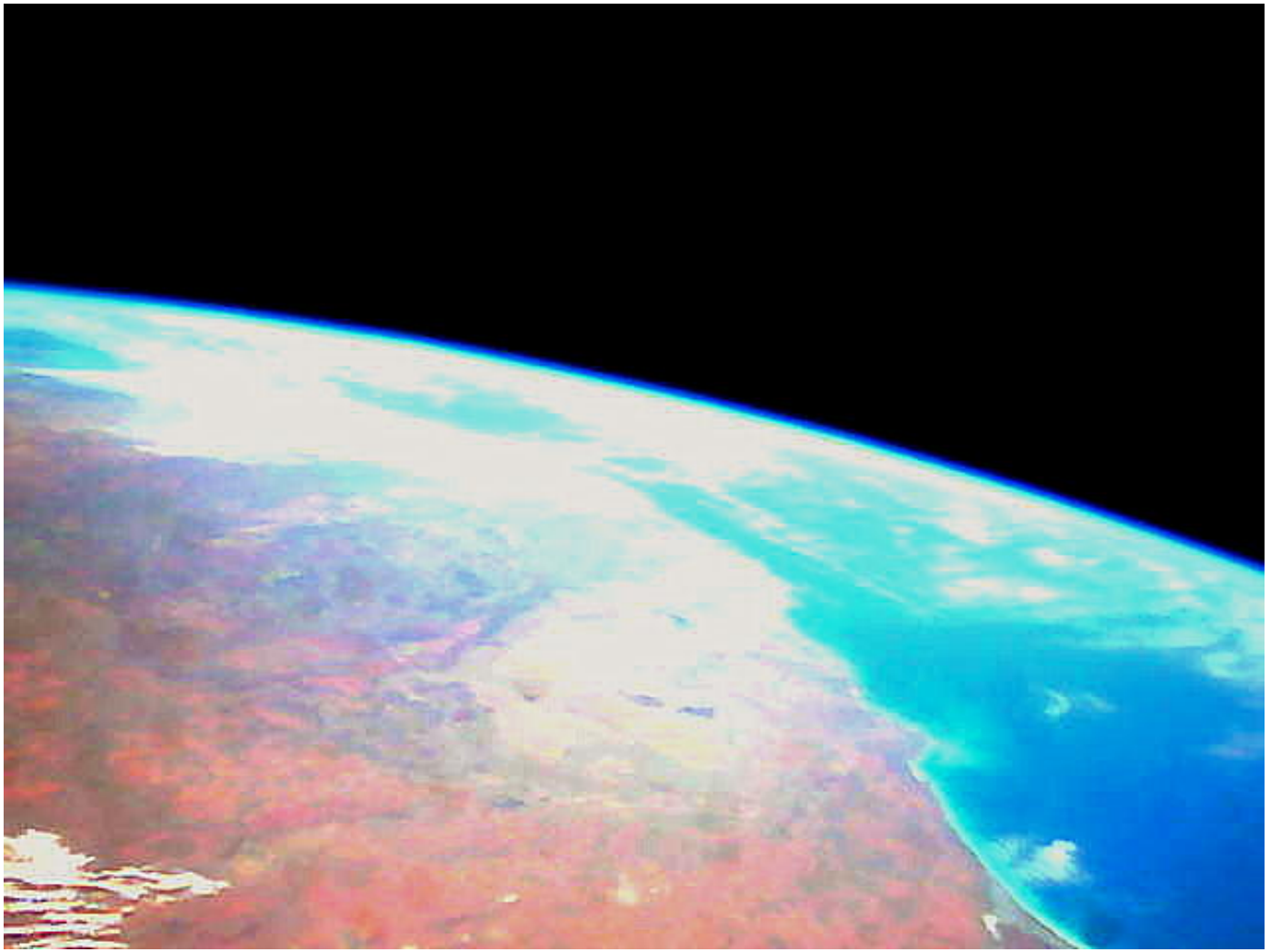
Boeing 787 generator control computer:

- 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:



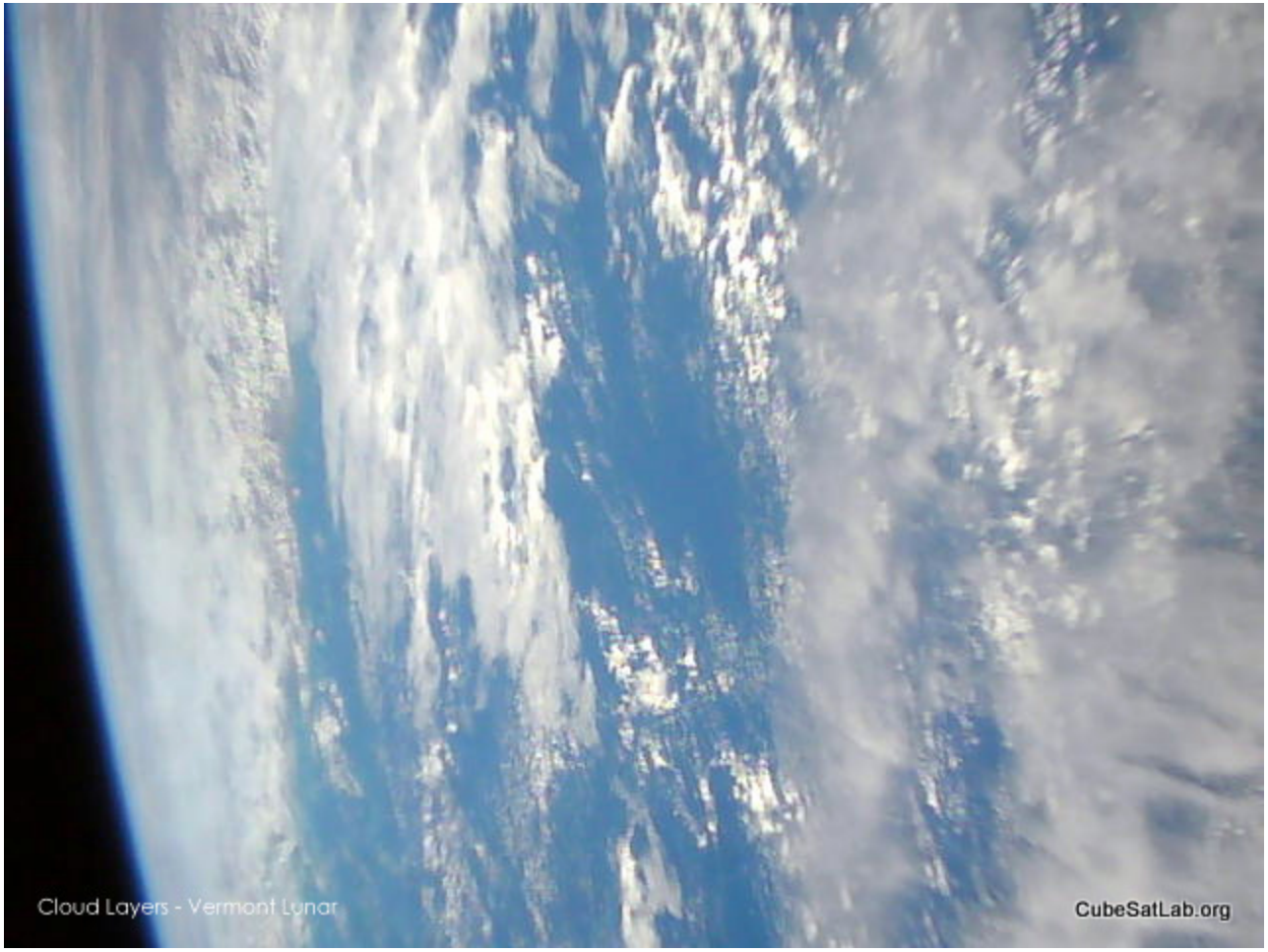
Vermont Lunar CubeSat



Our first picture of Earth

The North coast of Western Australia near Port Hedland

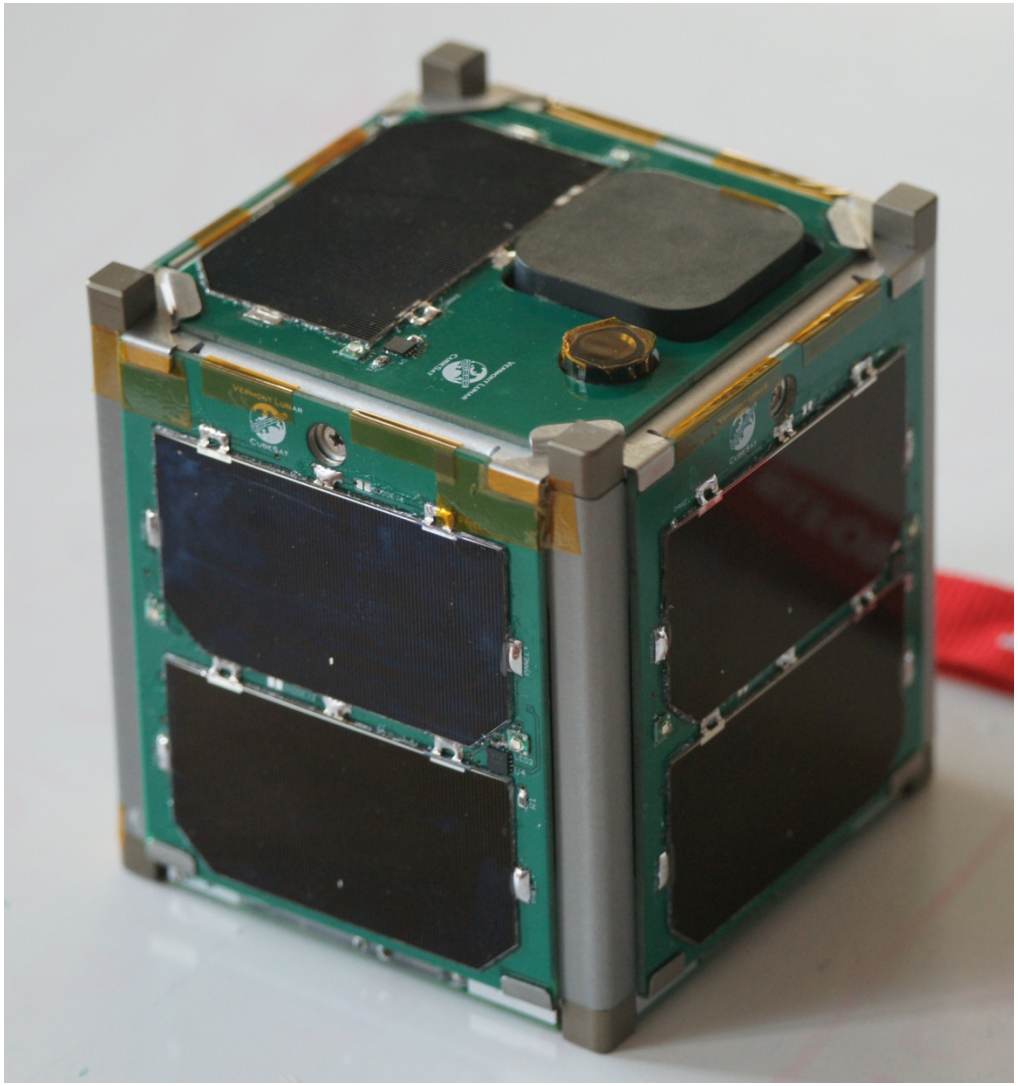
Vermont Lunar CubeSat



Clouds over the ocean, June 2015.

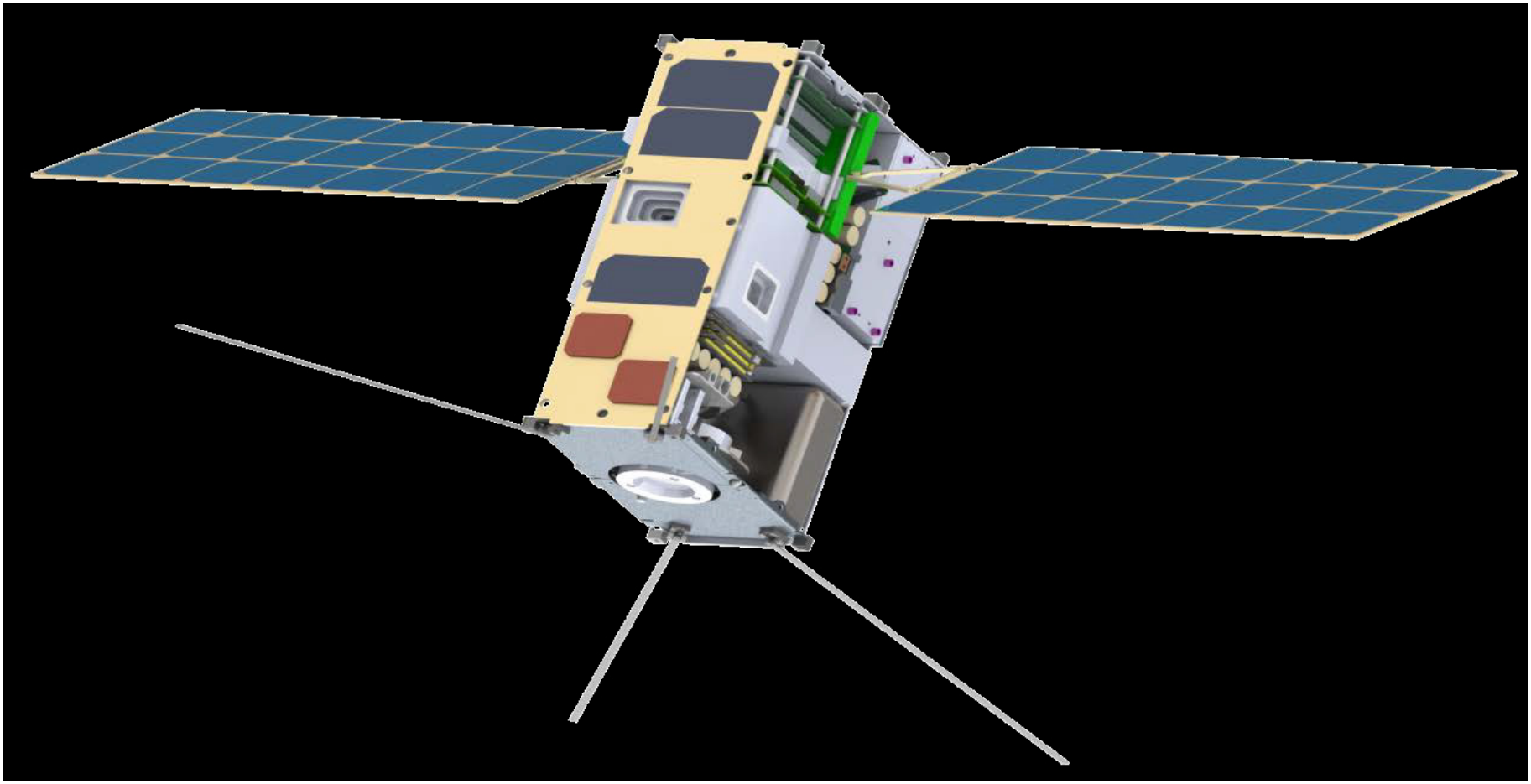
Vermont Lunar CubeSat

VERMONT TECH



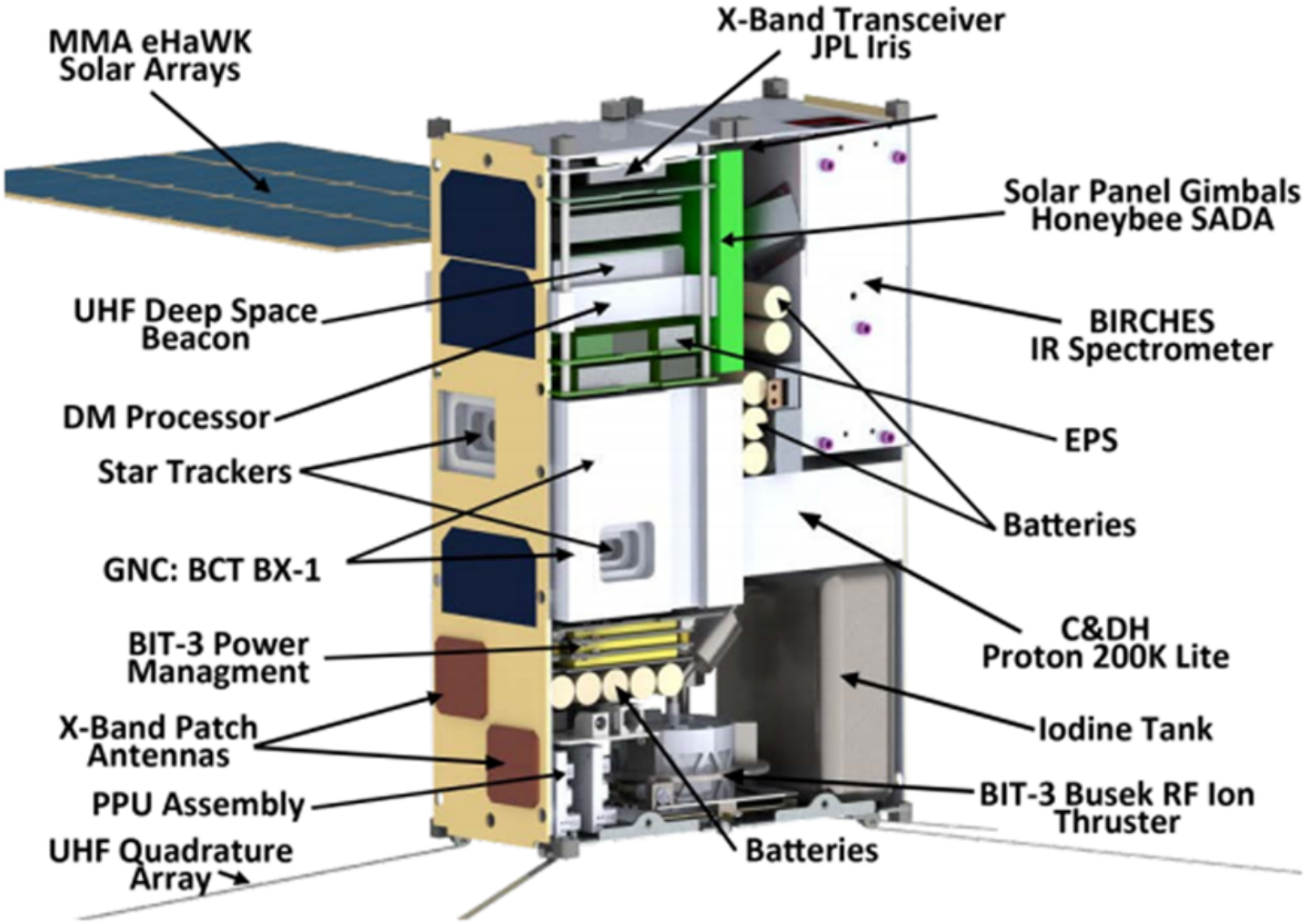
Vermont Lunar CubeSat (10 cm cube)

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

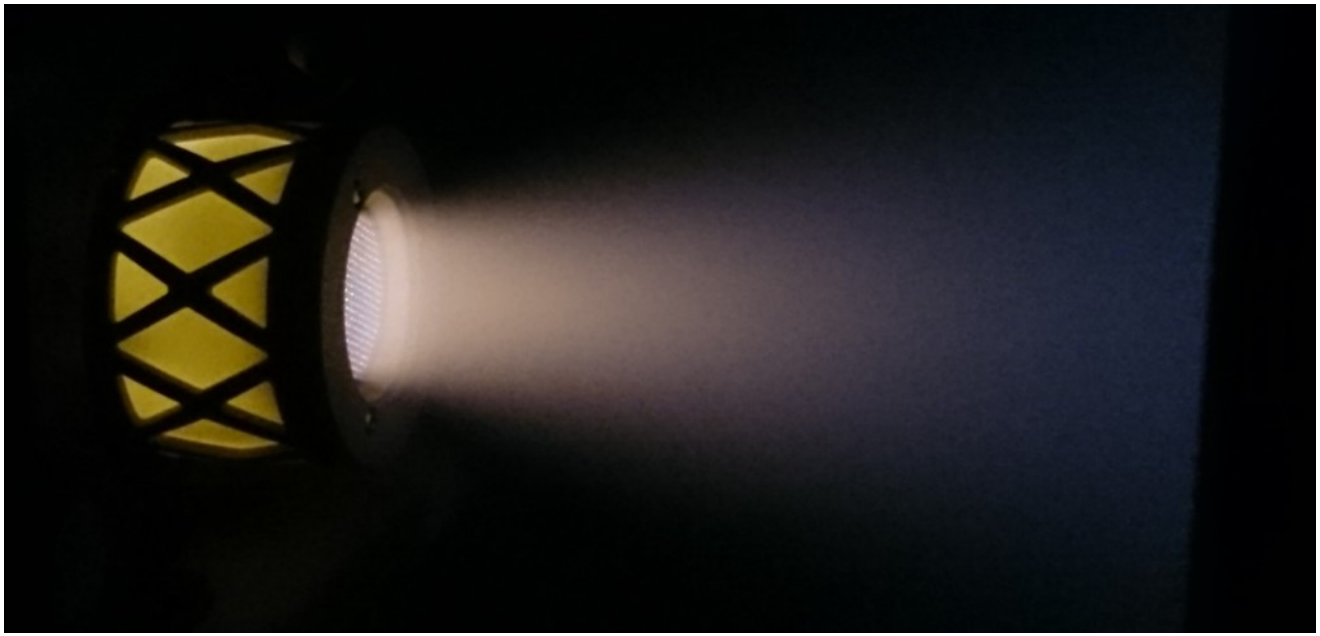


Lunar IceCube 6U CubeSat, Morehead State University, PI., Goddard (BIRCHES IR Spectrometer), JPL (Iris 2 data & nav radio) & Vermont Tech (Flight software). Busek ion drive with 1.5 kg Iodine propellant.

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

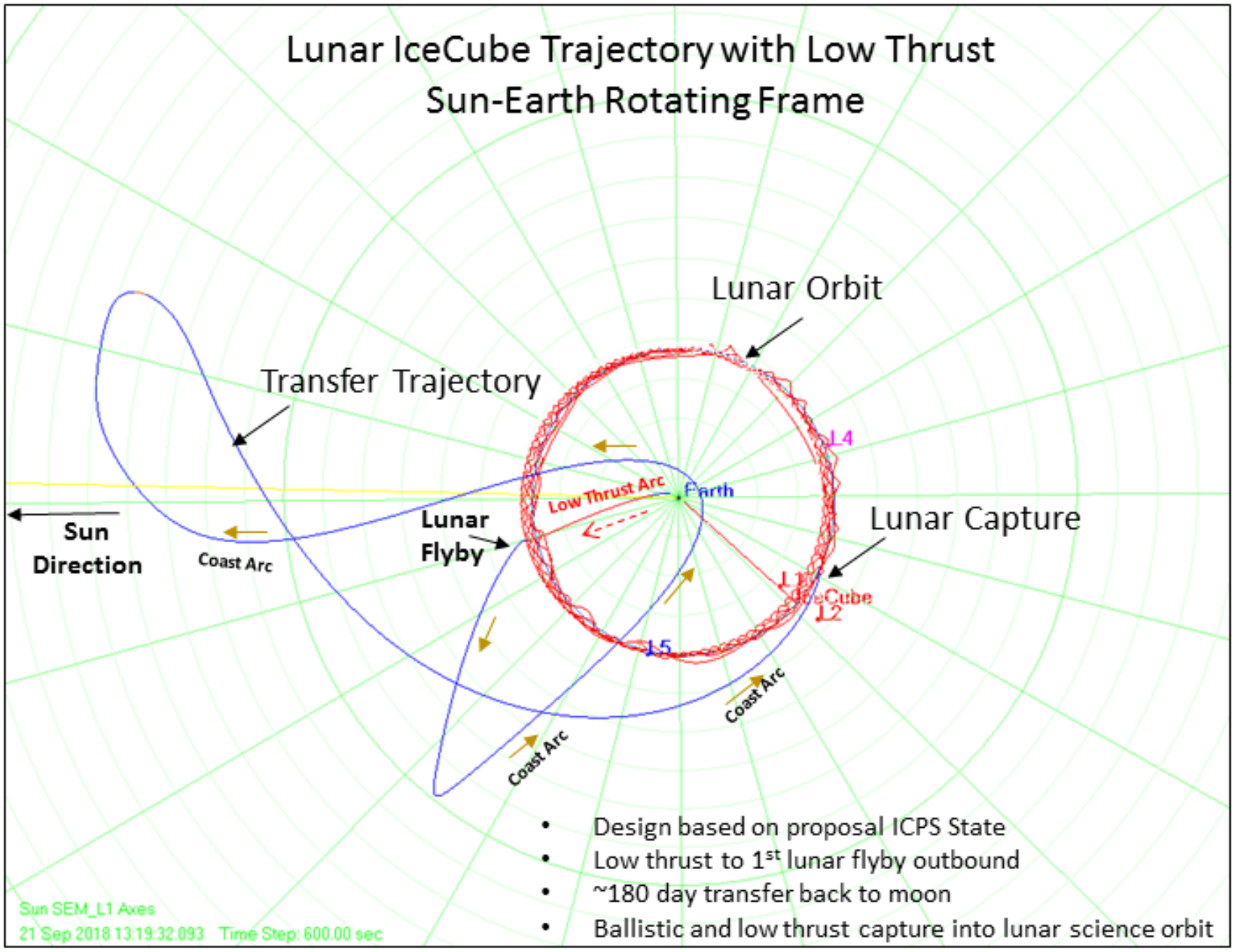


Busek Ion Thruster



BIT-3 Iodine Propellant

65W 1.4 mN, 3 cm beam width


Lunar IceCube Trajectory with Low Thrust
Sun-Earth Rotating Frame
Lunar Orbit
Transfer Trajectory
Low Thrust Arc
Earth
L4
L5
L1
L2
IceCube
Sun
Direction
Coast Arc
Lunar
Flyby
Lunar Capture
Coast Arc
Coast Arc
• 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
Sun SEM_L1 Axes
21 Sep 2018 13:19:32.093 Time Step: 600.00 sec

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)