The LinkStar Cybersecurity Cubesat “Sandbox”

A Platform To Test Cubesat Vulnerabilities With The Small Satellite Community

CubeSat Developers Workshop
April 27-29, 2021

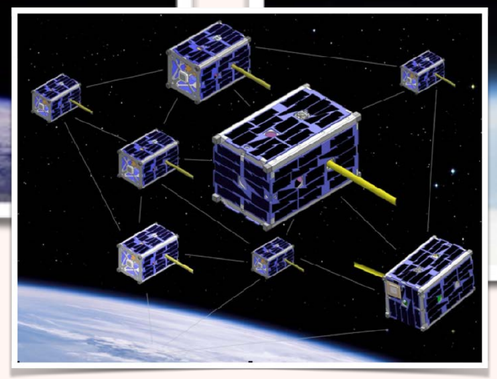
Andrew Santangelo, CTO

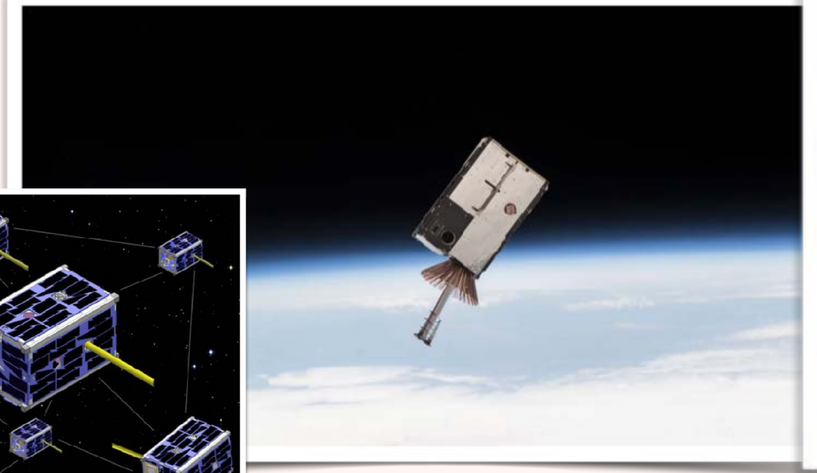
CONTRIBUTORS

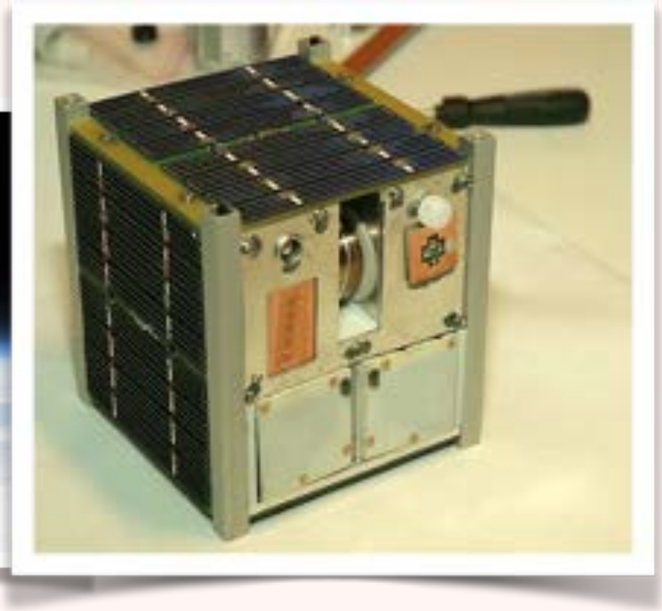
- Andrew Santangelo, SciZone
- Arun Viswanathan, Jet Propulsion Laboratory, California Institute of Technology
- Gregory Falco, Stanford University
- Jeremy Straub, NDSU
- Michel Ingham, Jet Propulsion Laboratory, California Institute of Technology
- Steve Lee, AIAA

AEROSPACE CYBERSECURITY WORKING GROUP

SITUATIONAL LANDSCAPE







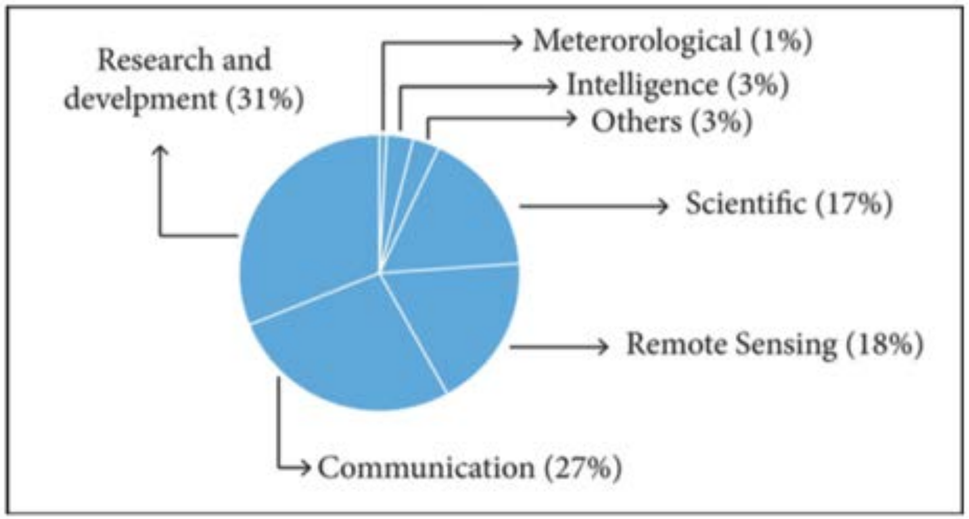
- Scientific Missions
- Military Operations

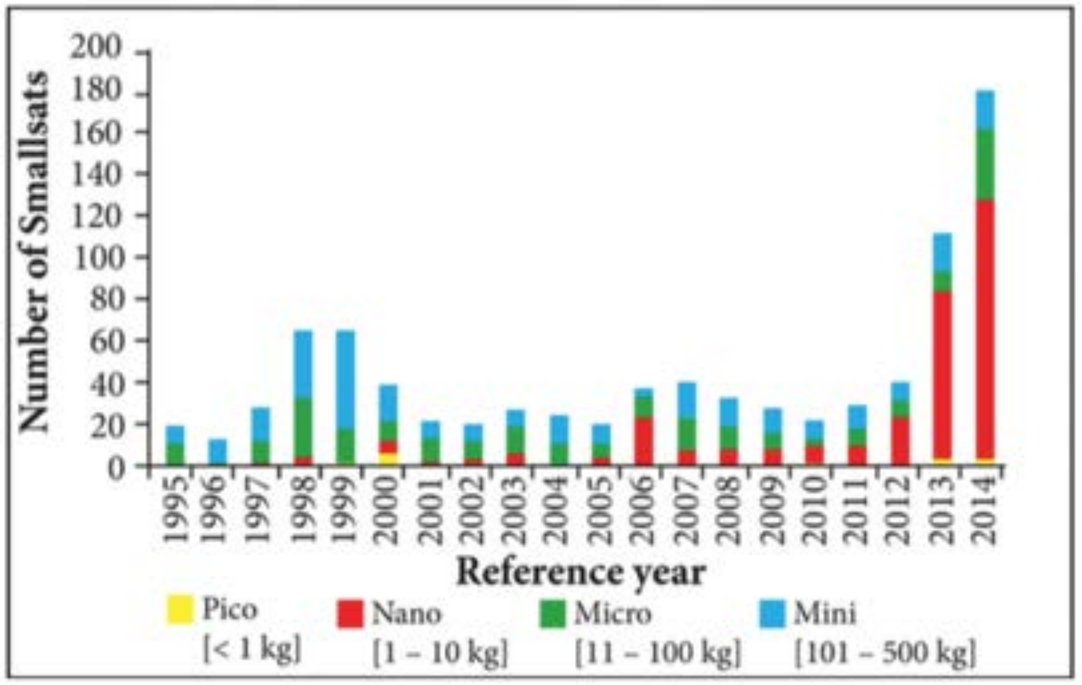
- Education Missions
- Commercial Enterprise

- Civic Operations
- Hobbyists

CUBESAT/SMALL SATELLITE MARKET SIZE

SmallSats	Wet Mass
Pico-Satellite	< 1 kg
Nano-Satellite	1 – 10 kg
Micro-Satellite	10 – 100 kg
Mini-Satellite	100 – 500 kg

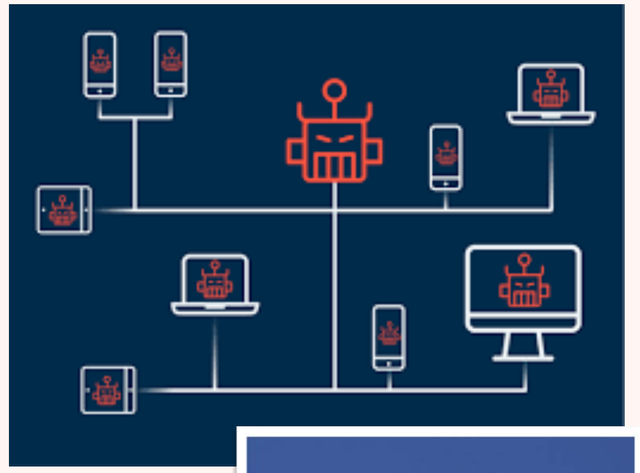


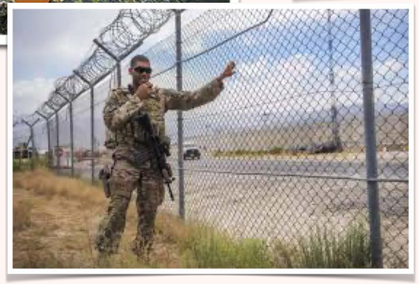


Cubesat growth >1,400 units/year by 2022
Mini-satellite Growth >250 units/year by 2022

"Status and Trends of SmallSats and Their Launch Vehicles, an Up-to-date Review", Journal of Aerospace Technology and Management, J. Aerosp. Technol. Manag. vol.9 no.3 São José dos Campos July/Sept. 2017

CUBESATS ARE IOTS IN SPACE!





The LinkStar Cybersecurity Cubesat "Sandbox" – a platform to test cubesat vulnerabilities with the Small Satellite Community

CubeSat Developers Workshop
April 27-29, 2021

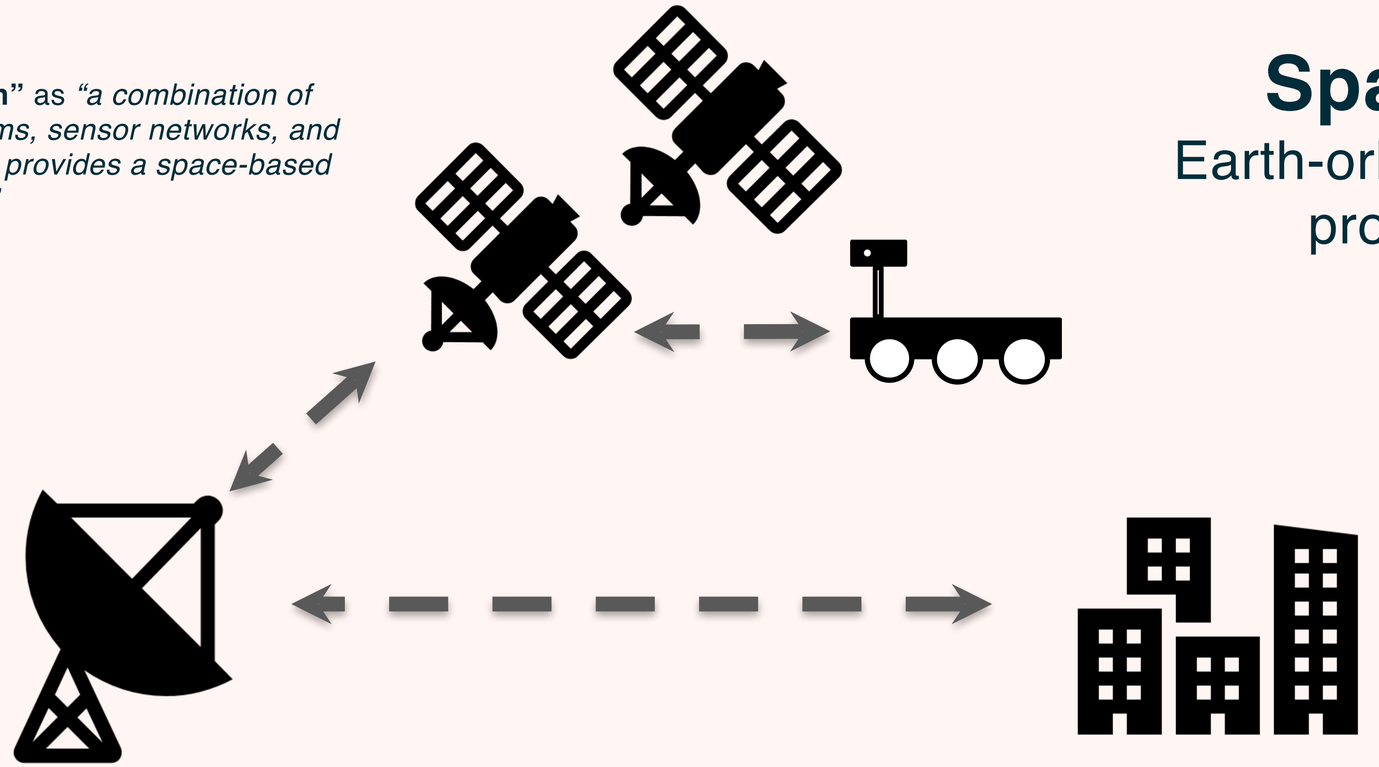
sci_Zone, Inc.
www.sci-zone.com

PROBLEM

- **Vulnerabilities in satellites of all sizes including CubeSATS**
- **Need to understand constantly changing landscape of *Cybersecurity***
- **Need to identify vulnerabilities**
- **Need to share lessons learned**
- **Need for collaboration in the community**

COMPONENTS OF A GENERIC SPACE SYSTEM

SPD-5[1] defines **"Space System"** as *"a combination of systems, to include ground systems, sensor networks, and one or more space vehicles, that provides a space-based service."*



Space Segment

Earth-orbit satellites, planetary probes, deep space

Link Segment

Ground-to-space communications

Ground Segment

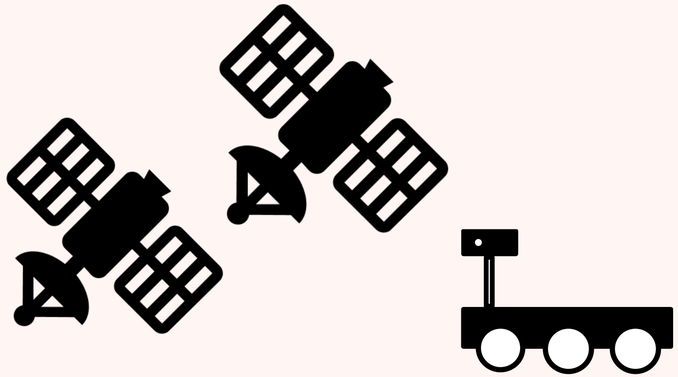
Operations & Support

1. As defined in, Memorandum on Space Policy Directive – 5 Cybersecurity Principles for Space Systems, Sep 2020

EXAMPLE CYBER INCIDENTS AGAINST SPACE SYSTEMS

April 2005[4]: A rogue program penetrated NASA KSC networks, surreptitiously gathered data from computers in the Vehicle Assembly Building and removed that data through covert channels.
2011[5]: Cybercriminals managed to compromise the accounts of about 150 most privileged JPL users.

Since 2007[3] several elite APT groups have been using — and abusing — satellite links to manage their operations — most often, their C&C infrastructure, for example, Turla.
Black Hat 2020[2]: Eavesdropping on Sat ISPs. Basically, ISP not protecting their links and it can be picked up easily.



June/July 2008[1]: *Terra EOS AM-1/Landsat-7, a*ttempted satellite hijacking, hackers achieved all steps for remote command of satellite.
2013-2014:[6] UT Austin Radio-Navigation Lab conducts GPS spoofing for UAV control and navigation interruption

1. 2020 Ascend Conference, Arun Viswanathan, et. al.
2. SPACE: Cybersecurity's Final Frontier, London Cyber Security Report, *June 2015.*
3. Black Hat 2020: Satellite Comms Globally Open to $300 Eavesdropping Hack, Threatpost, Aug. 2020
4. Turla APT Group Abusing Satellite Internet Links, Threatpost, Sep. 2015
5. Network Security Breaches Plague NASA, Bloomberg, Nov 2008
6. Hackers Seized Control of Computers in NASA's Jet Propulsion Lab, WIRED, Mar. 2012
7. UT Austin Radio Radionavigation Laboratory

HIGH-LEVEL THREATS AGAINST SATELLITES

Threat	Applicability	Description	Impact Example
Unauthorized control	Space segment, ground segment	A type of threat action whereby an entity assumes unauthorized logical or physical control of a system resource	Adversary assumes remote control of a spacecraft, or ground systems.
Corruption / modification of system and/or data	Space segment, ground segment, Link segment	A type of threat action that undesirably alters system operation by adversely modifying system functions or data. Subtypes: “tampering,” “malicious logic,” “hardware/software error”	A corrupted spacecraft command could result in catastrophic loss if either no action occurred (e.g., command is discarded) or the wrong action was taken onboard a spacecraft.

2020 Ascend Conference, Arun Viswanathan, et. al.
Adapted from CCSDS 350.1-G-2 Security Threats Against Space Missions

HIGH-LEVEL THREATS AGAINST SATELLITES

Threat	Applicability	Description	Impact Example
Interception of data	Space segment, ground segment, space-link communication	A type of threat action whereby an unauthorized entity directly accesses sensitive data while the data is traveling between authorized sources and destinations. Subtypes: "RF analysis," "wiretapping," "theft"	Interception of data may result in the loss of data confidentiality and data privacy if the data is not encrypted.
Jamming	Space segment, ground segment, space-link communication	A type of threat action that attempts to interfere with the reception of broadcast communications. Adversary can deny RF communications to/from spacecraft by injecting noise, by transmitting on the same frequency from another source, or by simply overpowering the original source.	Spacecraft commanding as well as the ability to receive science or engineering data from the spacecraft could be blocked. Authorized access may be impacted.

2020 Ascend Conference, Arun Viswanathan, et. al.
Adapted from CCSDS 350.1-G-2 Security Threats Against Space Missions

HIGH-LEVEL THREATS AGAINST SATELLITES

Threat	Applicability	Description	Impact Example
Denial-of-Service	Space segment, ground segment	The prevention of authorized access to a system resource or the delaying of system operations and functions.	Consumption of resources (e.g., communication bandwidth, processor bandwidth, disk space, memory), disruption of system/network configurations (e.g., routing changes), disruption of state information (e.g., persistent network connection resets), disruption of network components (e.g., router or switch crashes), or obstruction/destruction of communications paths.
Masquerade	Space segment, ground segment	A type of threat action whereby an unauthorized entity gains access to a system or performs a malicious act by illegitimately posing as an authorized entity.	If an external entity can masquerade as a spacecraft operator; unauthorized commands could be transmitted to the spacecraft resulting in damage, data loss, or loss of a mission.

2020 Ascend Conference, Arun Viswanathan, et. al.
Adapted from CCSDS 350.1-G-2 Security Threats Against Space Missions

HIGH-LEVEL THREATS AGAINST SATELLITES

Threat	Applicability	Description	Example
Replay	Space segment, ground segment, space-link communications	An attack in which a valid data transmission is maliciously or fraudulently repeated, either by the originator or by a third party who intercepts the data and retransmits it, possibly as part of a masquerade attack.	If the replayed commands are not rejected, they could result in a duplicate spacecraft operation such as a maneuver burn or a spacecraft reorientation with the result that a spacecraft is in an unintended orientation.
Software threats	Space segment, ground segment	Misconfigurations, programming errors, installation of malicious/unvetted software, and exploitation of vulnerabilities by threat agents.	Loss of data, loss of spacecraft control, unauthorized spacecraft control, or loss of mission.

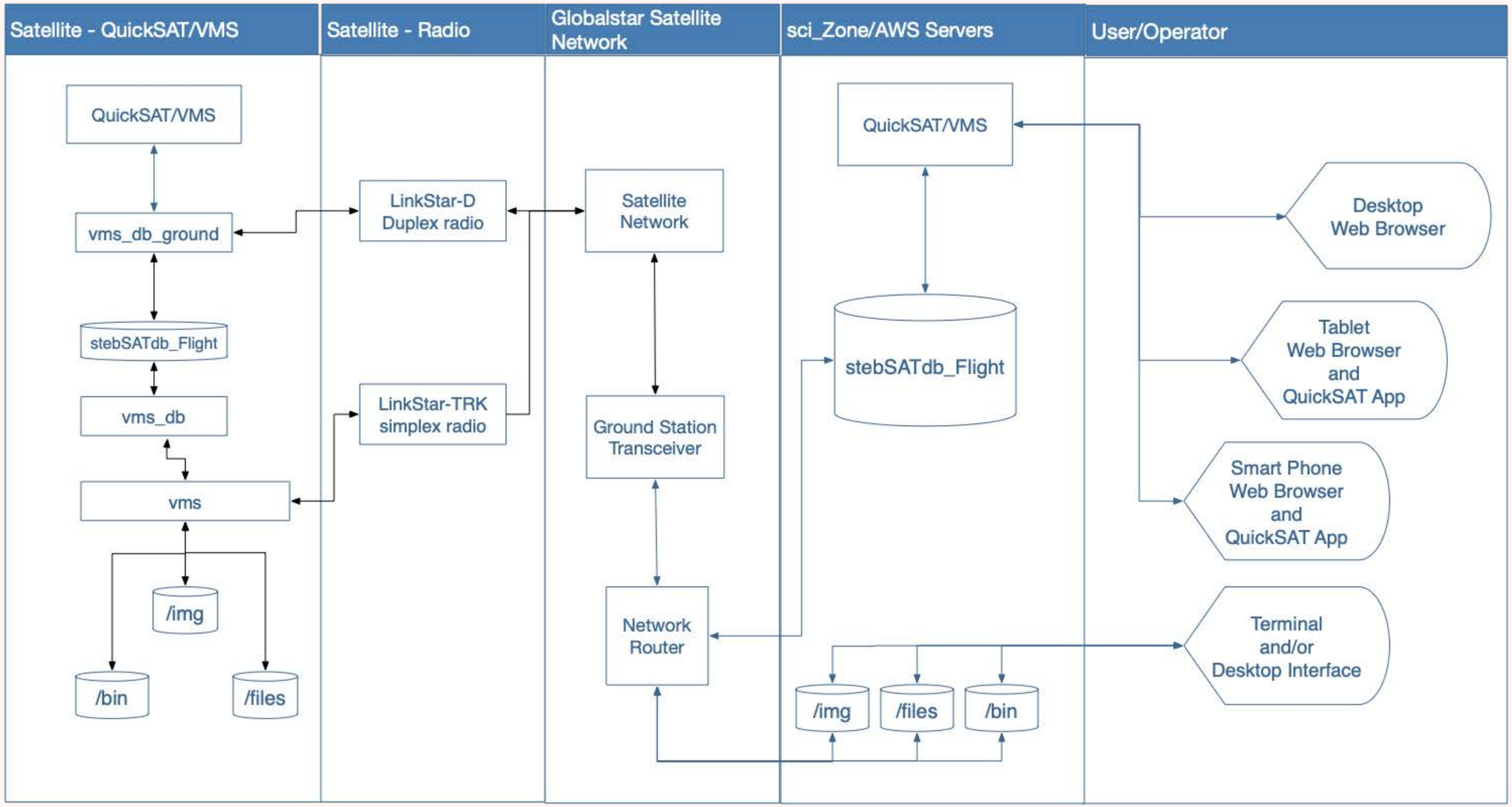
2020 Ascend Conference, Arun Viswanathan, et. al.
Adapted from CCSDS 350.1-G-2 Security Threats Against Space Missions

HIGH-LEVEL THREATS AGAINST SATELLITES

Threat	Applicability	Description	Impact Example
Supply Chain	Space Segment, Ground Segment	Attack in which extra electronic/ electrical components to Printed Circuit Boards (PCBs) schematics or layouts. Malicious firmware is added to embedded systems' microelectronic devices	Covert control of the power controller of the system management bus (SMBus) of a PCB would allow a threat agent to interfere with the communications of ground segment systems and space system sensors.

2020 Ascend Conference, Arun Viswanathan, et. al.
Adapted from CCSDS 350.1-G-2 Security Threats Against Space Missions

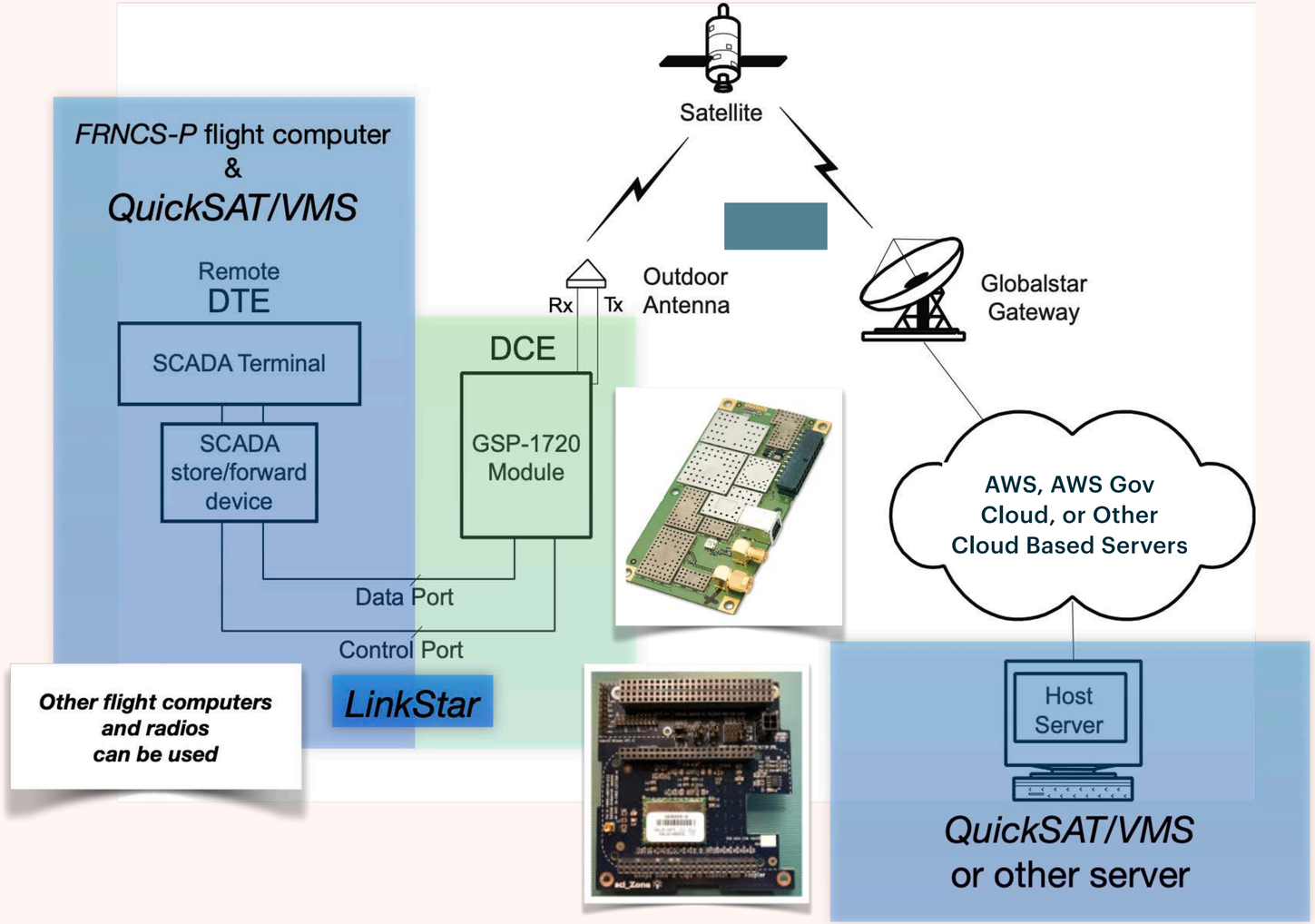
LINKSTAR CYBERSECURITY CUBESAT "SANDBOX"



- *QuickSAT/VMS* is the web based inteface
- **Communication is via "bent-pipe" to the ground**
- **Architecture supports a range of radios including the *LinkStar-TRK* (simplex) and *LinkStar-D* (duplex) plus S-Band, etc.**
- **The satellite "pushes" and "pulls" data to and from the ground. The ground terminals cannot push data to the satellite**

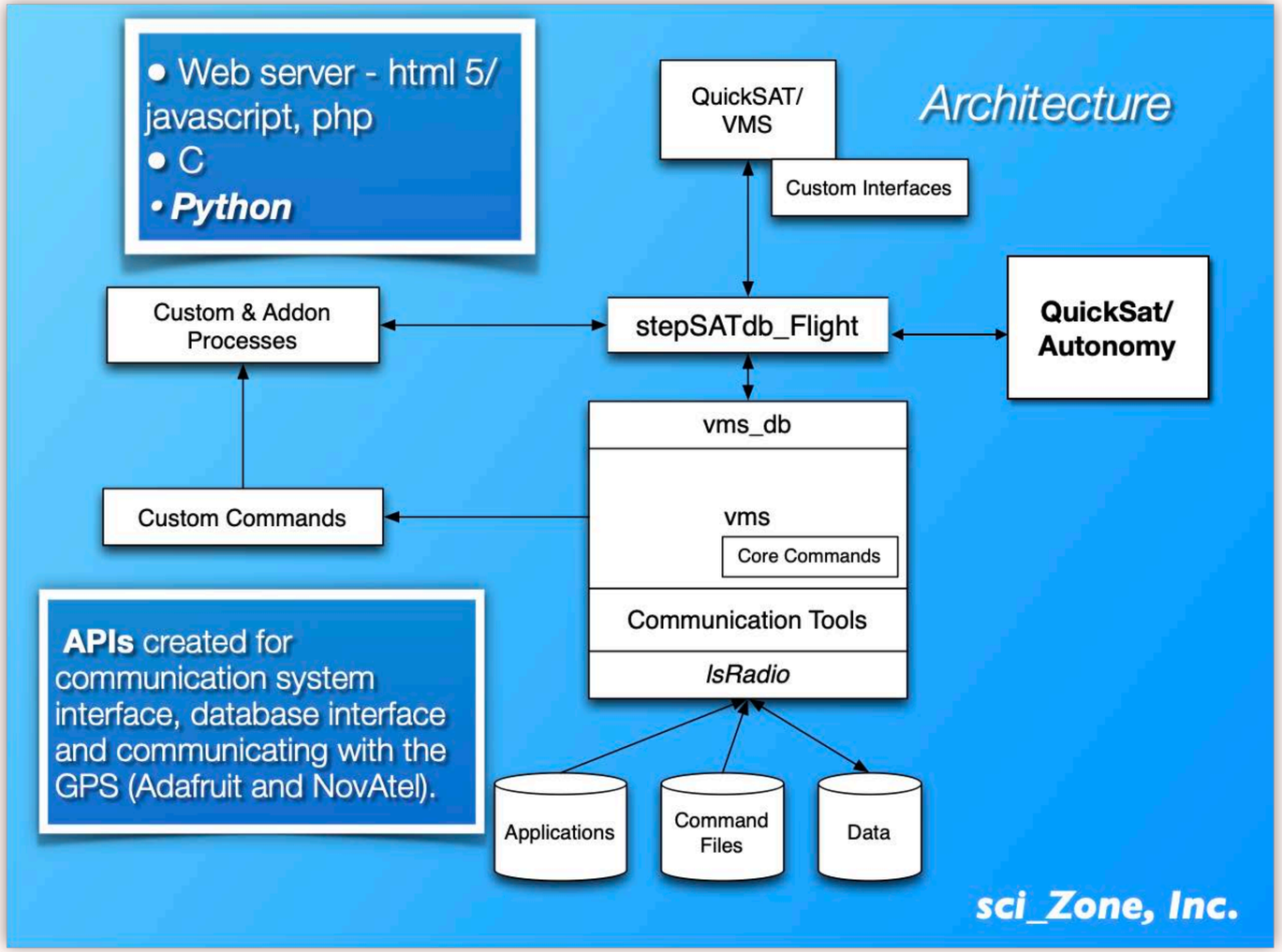
IoTs in Space: *LinkStar*

SCI_ZONE *LINKSTAR-QUICKSAT* ARCHITECTURE

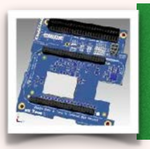


SCIZONE *QUICKSAT* ARCHITECTURE

- **Broad Use: Aviation, Satellites, Cars**
- **A complete Flight Management System**
- **Vehicle Health Management & Monitoring**
- **Vehicle Commanding Services**
- **Communications services**
- **Test/Monitoring interface**
- **Can serve as a stand alone ground station or part of an expanded environment**
- **Customizable**
- **Utilizes open source software where possible**
- **Works on a range of flight hardware**
- **Web based Interface - PCs, Tablets, etc.**

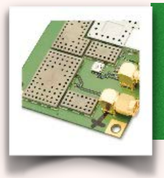


Components of *LinkStar* Architecture



LinkStar-TRK

LinkStar-D



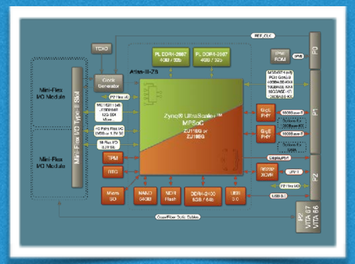
LinkStar-HD

S-Band/X-Band

- **Integrated ARM-53, FPGA or Modified *BeagleBone Black/AI***
- ***QuickSAT* Power Management**
- **0.5U form factor**
- **1-4W**
- **Watchdog timers and external signal reset**
- **Hypervisor**

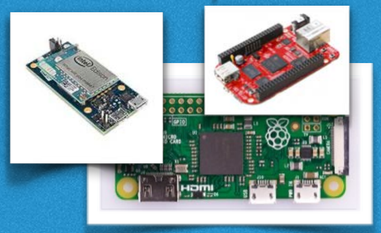
QuickSAT

Xilinx Zynq UltraScale MPSoC



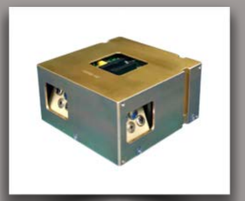
Flight Computer

Other Computers



OEM-719, ADA Fruit UltimateGPS

GPS



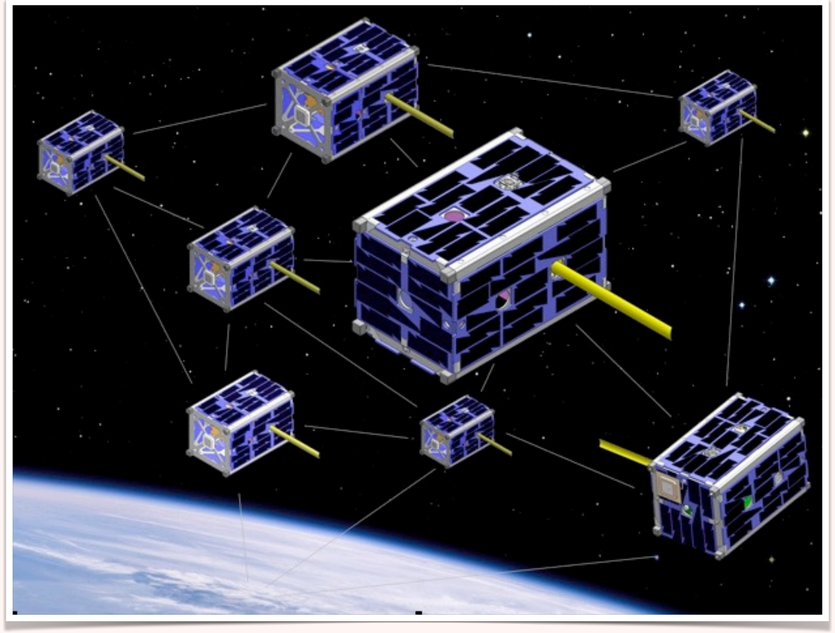
MAI-400

Sensors

Actuators

LESSON LEARNED TO DATE

- CubeSATs are IoT's in space!
- Despite cubesats being small, they are still highly calibrated machines that are sensitive to attack
- The types of attacks against cubesats are not significantly different than attacks on other cyber-physical control systems
- Traditional health monitors for satellites can be used to evaluate security of the cubesat as well



TEST SERVERS TO "HACK"

- **Virtual Machines are setup on the sci_Zone QuickSAT cloud environment for testing and exploring at** *https://www.sci-zone.com/cubesat-cybersecurity-challenge*
  - **Probe, explore, push, and "hack" the environment!**
  - **You will need to request access from andrew_santangelo@sci-zone.com**
- **Feedback from participants is welcome!**
- **Results will be shared with the CubeSat/Small Satellite and AIAA Community**