Hypersonic Re-Entry Deployable Glider Experiment (HEDGE)
Protection or Privacy? An Analysis of Satellite Surveillance Technology and Its Utilization

A Thesis Prospectus
In STS 4500
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Aerospace Engineering

By
Brandol Galicia

October 9, 2023

Technical Team Members:
Amy Paz Cuervo, Will Plunkett, Timothee Kampouris & Morgan Myers

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

ADVISORS

Joshua Earle, Department of Engineering and Society

Chris Goyne, Department of Mechanical and Aerospace Engineering

Introduction

Satellite imagery as a technology serves many purposes. Google Earth is the most well-known form of satellite imagery as it is commonly used to image bigger-scale environmental effects and the development of areas. The United States government, however, uses satellite imagery to watch over other countries and the United States itself, in a process known as satellite surveillance.

The government's satellites have a higher resolution than the commercially allowed 25 cm resolution. (Coffer, 2020) Former President Trump released satellite images of 10 cm resolution to the public confirming the government's higher satellite resolution capabilities. (Wang, 2019) The people of the United States do not know what higher capabilities the government's reconnaissance satellites have or what they are used for due to the lack of transparency. Therefore, I will be investigating the capabilities of reconnaissance satellites, how the United States government uses them, and their justification for why they can keep using them. The information will aid in answering the question: will the advancement of satellite surveillance technology used for the sake of national security be a compromise of the privacy rights of United States citizens?

For my technical project, I will be working on the Software and Avionics team of the Hypersonic ReEntry Deployable Glider Experiment (HEDGE). The purpose of HEDGE is to make the evolving hypersonics field more accessible to undergraduates studying aerospace engineering. Experiments in the aerospace field, specifically hypersonics testing, cost millions of dollars to execute. Therefore, the project will utilize small and cheap spacecraft, like a CubeSat, to minimize cost and increase reproducibility.

My projects relate to each other as smaller and cheaper spacecraft can potentially make surveillance from space more accessible. Surveillance technology can be put onto the small spacecraft and launched at a lower cost leading to more surveillance spacecraft circulating the Earth. The prospectus, however, will not dive deeper into this as I will first discuss how my team and I plan to approach designing and possibly fabricating the software and avionics for HEDGE. Afterward, I will outline the frameworks, methods, and resources I will use to formulate my final STS thesis.

TECHNICAL PROJECT

I. Problem Outline

The Hypersonic ReEntry Deployable Glider Experiment (HEDGE) is a CubeSat that will be launched into orbit and reenter the Earth's atmosphere at hypersonic speeds to collect data. A CubeSat is a small satellite that uses standard size and form factor (Caldwell, 2023). The Software and Avionics subteam has the responsibility of designing the hardware and software system of HEDGE so that it can collect, store, and transmit data during the mission. More specifically, our subteam will be connecting the onboard computer (OBC) to the rest of the hardware components. This is important because the other subteams have components that need to connect, interact, and communicate with the OBC.

II. Objective of Research Work

The main objective of our research this year is to construct and test a prototype that embodies both essential hardware and software components for the HEDGE mission. Our duties include furthering the advancements of last year's team who selected the critical electronics such as the pressure transducer, the Endurosat onboard computer, and the thermocouple. The

challenge lies in ensuring seamless communication amongst these components and guaranteeing that the data is effectively transmitted through the Iridium transceiver module back to Earth.

Building upon the existing groundwork, our responsibilities extend to developing the required software that facilitates real-time data acquisition, processing, and transmission during the CubeSat's operational phases. Once the prototype construction is finalized and the software is comprehensively developed, it will need to be tested. The tests must validate both the software's functionality and the hardware's resilience for the conditions of hypersonic re-entry.

III. Approach and Methods

The first step is integrating the selected components. The team will collaborate with the electrical engineering students to design and fabricate circuit boards that can connect the thermocouple, pressure transducer, and receiver. These circuit boards will be based on the data flowchart as seen in Figure 1.

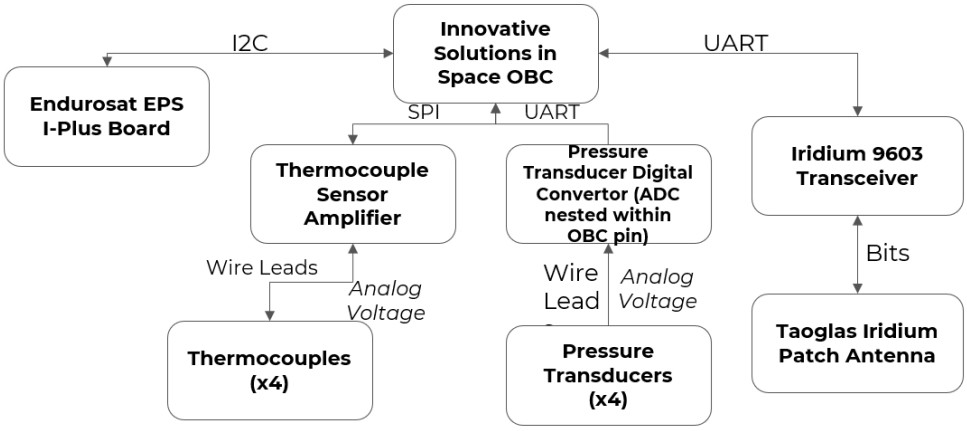

Figure 1: Hardware data flowchart (UVA MAE 4700 2023 Students, 2023)

The software, which consists of freeRTOS, COSMOS, and cFS, will be developed to work alongside the hardware. Then, multimeters and microcontrollers will test the hardware and software to ensure the OBC communicates well with all components. The team will show and

discuss the final design with other subsystem teams to streamline the integration process for the final HEDGE prototype.

IV. Resources

For command and control, the Endurosat onboard computer will be used. The Endurosat onboard computer user manual is a great resource that has key information about hardware and software integration, application programming documentation, initial configuration procedures, troubleshooting, and safety guidelines (Endurosat, 2018). To manage onboard processing, NASA's core flight system, a reusable software framework, will be used due to its reliability and portability (NASA). The COSMOS operating system will be used to set up the ground-based system and run simulations of software and hardware components (OpenC3, 2023). Both cFS and COMOS are open-source, which allows for collaboration with others. University of Virginia professor, Mike McPherson, has lots of knowledge about avionics, adding another great resource. Lastly, the electrical and computer engineers are collaborating with our subteam and will greatly help in designing the circuit boards and initial software setup.

V. Objectives for Spring Semester

By the end of the Fall 2023 semester, the Software and Avionics team plans to deliver the hardware components for the MSP300 pressure transducer and the RockBLOCK9603 Iridium transceiver module for hardware. Because the OBC will not be in person for testing until the Spring, the software that the team plans to deliver contains CFS programs corresponding to both the pressure/temperature and communication hardware components on a Raspberry Pi 4b running FreeRTOS (TImada). The biggest objective of the Spring 2024 semester is to port the CFS software to the Endurosat OBC and ensure that input/output (IO) between the software subsystems and their respective hardware components functions correctly. To ensure that

components are working properly, a testbench for the hardware and software will be created. OpenC3 COSMOS provides a framework for CubeSat testing that the team plans to utilize to create an exhaustive set of tests that accurately simulate the working environment of the satellite (OpenC3, 2023). Alongside these objectives, the team plans to update the CFS project ported to the OBC to align directly with the information transfer/data storage mechanisms described in the HEDGE documentation. For the fall semester, the software and avionics team will work together to prepare for a Technical Interchange Meeting (TIM) with the rest of the subteams. For the second semester, all the subteams will collaborate to make a System Integration Report (SIR) and one technical thesis.

STS PROJECT

I. Introduction and Research Question

The government's satellite surveillance and reconnaissance satellite technology is more advanced than what is known to the public. The purpose of this is to keep the nation "safe" from dangers by continuously monitoring parts of the world, including parts of the United States. The advancement of the technology will also start to add other surveillance technologies such as facial recognition.

The government is not transparent with how and where they use satellite data, specifically surveillance. (Fried, 2019) They claim that it is for the sake of national security because they are watching the actions of their adversaries. The lack of transparency causes the people of the United States to become worried about being continuously monitored. The government is essentially breaking the 4th Amendment's promise of being safe from unreasonable search if it continues to use satellite surveillance. (Kelly, 1995). The situation

creates the question as stated before in the introduction: will the advancement of satellite surveillance technology used for the sake of national security be a compromise of the privacy rights of United States citizens.?

II. Social Groups

I will analyze two main social groups which are the United States government and the people of the United States. The government will consist of the military, the police force, and the Supreme Court. The military is a part of the group because they are continuing the advancement of satellite surveillance technology. The military also acts similarly to the police force because they use satellite or aerial surveillance to perform unwarranted searches. The Supreme Court is part of the government as they justified satellite surveillance use because they claim citizens do not own the air above their property.

The people of the United States are the ones who are facing the dangers of having their privacy rights disappear. As mentioned above, there have been instances where the government has gone against the people in these types of cases. For example, in the case of Florida vs. Riley, the police proceeded to fly over and take images of Riley's properties because they had a suspicion that he was growing marijuana. The police did the flyover without a warrant and proceeded to arrest Riley. When Riley appealed the case, the Supreme Court ruled in favor of the police. The Supreme Court stated that the action did not infringe on Riley's privacy rights. (*Florida vs. Riley*, 1988)

III. Methods and Frameworks

I will use the Social Construction of Technology (SCoT) framework to help answer the research question. The SCoT framework entails a "multidirectional" view of how a technology interacts or influences the common social groups around that technology. (Bijker et al., 1987) I

will analyze the government's belief in continuing to advance satellite surveillance and how the citizens of the United States feel about the technology infringing on their privacy using the SCoT framework.

Along with the framework, I will use a historical, public policy, and case study to research the government's standing on surveillance for national security without regard for people's privacy. The historical research method will also be further used to determine the state of where satellite surveillance is at and how much it can be improved. Finally, I will take a philosophical approach to determine the line between national security and privacy.

IV. Timeline

Throughout the fall semester, I will continue to do research on the state of the technology and the possible advancements it may have. At the same time, I plan to start researching cases that deal with surveillance and citizen's privacy. I will conduct a web search on recent events that deal with satellite surveillance to see if there are any more examples. I expect to finish my research at the end of winter break so that I can begin writing my thesis in the spring semester.

V. Key Texts

[1] Florida vs. Riley, (Rehnquist Court January 28, 1989). https://www.oyez.org/cases/1988/87-764

The case revolves around Florida police using aerial surveillance to look into Riley's greenhouse because they could not tell what he was growing from the ground. The case is important to the research paper as it discusses the different opinions about whether or not aerospace surveillance infringes on the privacy rights of people.

[2] Bijker, W. E., Hughes, T. P., & Pinch, T. (1987). *The Social Construction of Technological Systems*. Massachusetts Institute of Technology.

The paper discusses the STS framework of the Social Construction of Technology. It talks about viewing the influences a piece of technology has on different involved social groups. SCoT will be the main framework used to analyze how satellite surveillance influences the government and the people of the United States.

[3] Kelly, K. C. (1995). Warrantless Satellite Surveillance: Will our 4th Amendment Privacy Rights be Lost in Space? *Journal of Computer & Information Law*, *13*(4), 729–762. https://repository.law.uic.edu/cgi/viewcontent.cgi?article=1367&context=jitpl

The journal article discusses satellite surveillance and the 4th Amendment from a law-based point of view. It mentions the *Florida vs. Riley* case that will used in the paper. This is more of a law-based and factual argument that will aid in the philosophical discussion of the paper.

[4] Fried, S. J. (2019). *Landsat in Contexts: Deconstructing and Reconstructing the Data-to-Action Paradigm in Earth Remote Sensing*. Virginia Polytechnic and State University.

The thesis talks about the satellite's remote sensing capabilities, specifically looking at NASA's Landsats. It uses STS methods to discuss the conflicting narratives and values of satellites. The piece will be helpful in the argument that satellite capabilities can be so advanced that people should start worrying about their privacy.

[5] Beam, C. (2019, June 26). *Soon, satellites will be able to watch you everywhere all the time Can privacy survive?* MIT Technology Review. https://www.technologyreview.com/2019/06/26/102931/satellites-threaten-privacy/

The webpage article discusses some of the uses of satellite surveillance and how they have impacted individuals. The scenarios in the articles are good examples of how satellite surveillance can be beneficial or harmful.

References

Beam, C. (2019, June 26). *Soon, satellites will be able to watch you everywhere all the time Can privacy survive?* MIT Technology Review. https://www.technologyreview.com/2019/06/26/102931/satellites-threaten-privacy/

Bijker, W. E., Hughes, T. P., & Pinch, T. (1987). *The Social Construction of Technological Systems*. Massachusetts Institute of Technology.

Caldwell, S. (Ed.). (2023, August 23). *What are SmallSats and CubeSats?*. NASA. https://www.nasa.gov/what-are-smallsats-and-cubesats/

Coffer, M. M. (2020). Balancing Privacy Rights and the Production of High-Quality Imagery. *Environmental Science & Technology*, *54*(11), 6449–7024. https://pubs.acs.org/doi/epdf/10.1021/acs.est.0c02365

Endurosat. (2018, June 20). *Endurosat User's Manual.*

Florida vs. Riley, (Rehnquist Court January 28, 1989). https://www.oyez.org/cases/1988/87-764

Fried, S. J. (2019). *Landsat in Contexts: Deconstructing and Reconstructing the Data-to-Action Paradigm in Earth Remote Sensing*. Virginia Polytechnic and State University.

Kelly, K. C. (1995). Warrantless Satellite Surveillance: Will our 4th Amendment Privacy Rights be Lost in Space? *Journal of Computer & Information Law*, *13*(4), 729–762. https://repository.law.uic.edu/cgi/viewcontent.cgi?article=1367&context=jitpl

NASA. (n.d.). *Core flight system*. NASA. https://cfs.gsfc.nasa.gov/

OpenC3. (n.d.). https://openc3.com/

TImada. (n.d.). *Timada/raspi4_freertos: FreeRTOS UART sample porting to Raspberry Pi 4b.* GitHub. https://github.com/TImada/raspi4_freertos

UVA MAE 4700 2023 Students. (2023). *HEDGE Critical Design Review*.

Wang, B. (2019, September 1). *US Spy Satellites at Diffraction Limit for Resolution Since 1971*. Next Big Future. https://www.nextbigfuture.com/2019/09/us-spy-satellites-at-diffraction-limit-for-resolution-since-1971.html