Up in Frames: AgroFlight
(Technical Report)

Cybersecurity in the Residence: An Application-Based Actor-Network Theory Framework

(STS Research Paper)

An Undergraduate Thesis

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Sean Benish
Fall, 2021

Department of Electrical and Computer Engineering

Portfolio Table of Contents

Ethics of a Soil-Probing Drone

An STS 4600 Sociotechnical Synthesis

Sean Benish, spb5yw

November 17, 2021

My technical project developed a drone that could analyze soil content like pH, potassium content, and nitrogen content. Farmers need to know the nutritional content of the soil as well as soil condition to keep their produce alive and well for harvest. Satellite- and drone-imaging already creates water distribution maps for farmers, so this project seeks to fill in the gap in other variables affecting crop health. Currently, farmers either manually sample their fields (once every 20 acres) or purchase expensive soil probes to create expansive networks to collect data. This project allows for flexibility in resolution compared to soil probe networks as well as savings in time available to a fast-flying drone.

Technology does not exist in isolation. A core tenant of STS theory asserts technology is what we make it, so a technology exists within a value system. Therefore, an engineer with a STS view can improve the new technology by understanding and "improving" the social and ethical impacts of this technology. For this technical project, this paper analyzes this new technology under four lenses: as a disruptive technology, as a risk, as a element in a broader social movement, and as a aspect of cybersecurity.

A Disruptive Technology

In its intentions behind its design, this drone technology seeks to disrupt the current technologies and replace them as the better option. As competition, the downfall of the previous methods benefits this method, but competition (although acceptable under a Western economic framework) may not be ethical if the societal impacts outweigh the benefits. For example, pushing for disruptive AI-technology without giving sufficient time for the education system, markets, and the affected to prepare for this technology would usually be considered unethical; the widespread collapse of a whole class of jobs sticks people into long-term suffering for the benefit of the few. Thus, this technology must know who will be affected and to what degree the effects will be.

Obviously, the farmer benefits from this new technology—they are the market base after all. The technology reduces the time for sampling or lets farmers sample when it was unfeasible to do so previously. Farmers wish to sample soil because it provides a feedback loop. When the soil becomes less nutritious, farmers would like to know *before* their crops show symptoms. Fertilizers can then be used to boost the soil's nutrition and maintain a good yield. Keep in mind that the use of fertilizers, especially at an industrial level, has ethical concerns involving public heath and the environment.

This technology will hurt the previous methods if adopted. Therefore, the labs who process soil samples as well as the technology companies developing probe networks will face the brunt of a supposed mass-adoption. The technology companies face an existential problem: they must compete or they will fail. As these companies are few and out-competing will not have far-reaching consequences to society, the benefits the farmers will gain outweighs the dissolvement of these companies. Soil labs, however, will not disappear from this loss in business. Civil engineers use soil labs to understand the properties of the dirt that they construct infrastructure and buildings on, and they use these labs a lot. Therefore, these labs will lose some business, but this loss poses no ethical dilemma.

Associated Risk

In general terms, an ethical product will announce its associated risks and outcomes to a consumer. At the same time, designers have an obligation to remove needlessly risks aspects from their design. As a prototype and as a system, the probing drone has legal, financial, and safety risks associated with it.

The primary legal risk from the drone comes from the FAA. As these drones will be used for commercial purposes, the owner not only needs to register the drone, but must also receive a commercial drone piloting license to operate the device. This poses a significant barrier, even if the technology becomes fully automated. Furthermore, drones must operate under 500 feet, which may be reduced if near an airport. Moreover, if sections of a field fall into controlled airspace, contact with air traffic controllers will be required.

As drones are fragile things, this system comes with an inherent financial risk. A multitude of factors could cause the drone to fall and require repair or replacement: rain, winds (sustained and gusts), improper charging, user input, and more. As the drone has a non-trivial price associated with it, an ethical design should entail safeguards to prevent users from putting their device at risk as well as indicating situations where the drone could fail. For example, the software that oversees the drone could connect to a weather site to get rain and wind data to determine the risk levels of operation. In a fully automated system, this could include scheduling the device to operate when the risk of poor environmental conditions is low.

Lastly, drones prove a risk to safety that owners of this technology need to be aware of. For starters, drones can cut, bruise, and puncture skin—a great risk if not using face protection. Moreover, the drone itself has sharp probes that could cause serious injury or death. Therefore, the system needs to indicate these risk and provide solutions to mitigate this safety risk to owners. Furthermore, the drone uses a lithium-polymer battery for its high energy density and high current capabilities. Although not as dangerous as lithium-ion batteries, lithium-polymer batteries still have a risk of fire. Therefore, charging of the device needs to be supervised, with the battery inside a fire-resistant bag. Furthermore, any fall could cause the battery to catch fire, which could burn through crops and put people's property and lives in jeopardy. No current solution exists to this problem, but one will be needed if the system is to ever deploy.

The Right to Repair

The right-to-repair movement opposes a growing trend of the technology-as-a-service model. In the agricultural market, this poses significant problems. If a combine breaks down and the part to fix it can only be sold to the manufacturer, farmers have to either call a technician (wasting valuable time and money) or find a method to fix it themselves (and perhaps violating copyright in the process). Furthermore, the companies who sell and maintain equipment have an incentive to keep this system going, legal binds to keep someone as a customer.

Western nations hold private property as a key value in their legal systems. Generally, someone should be able to use private property in any way they wish. This does *not* exclude one from the risks associated with improper or unlawful use. Therefore, this section focuses on how the technical project supports the spirit of the right-to-repair while noting areas where improper use can lead to legal or safety risks. Risks associated with the technology exist in the previous section, so this section will focus on how the technology supports the movement.

In supporting the spirit of the movement, the drone can be manufactured with off-the-shelf components that anyone can purchase. Furthermore, the project uses as many open-source libraries as possible. The flight controller and the flight computer both use open-source libraries, and the GPS and WiFi modules use well-documented standards. In addition, anyone can view the circuit board's layout, and the chassis for the drone is 3D printed, allowing anyone with access to the right machine and materials to build replacements to the drone.

Security Focus

Closest to my STS research paper, the drone's treatment of cybersecurity needs to be discussed. Farms exist as both a business and usually a home in the same place. Therefore, home security and business security become interchangeable. In the context of the research paper's framework, the drone fits in the LAN network of the home model. Therefore, one must understand the current flaws and possible revisions to the drone and its supporting technology.

As a prototype, cybersecurity was never the foremost aspect of design. The communication protocol, for instance, uses a one-way handshake built off user datagram protocol (UDP) in the goal of reducing power consumption from transmission control protocol (TCP) acknowledgement packets. An attacker then, for example, could forge a "drop" packet to cut off communication between the controller and the drone (man-in-the-middle attack) assuming IP spoofing is possible. To resolve this issue, the protocol could switch over to TCP (increased power consumption) or the drone's communication protocol could be extended to provide access control to connections (the drone knows who can connect and the identity of communicators gives them privileges).

The drone stores the wireless network's SSID (the network's name) and its password in the compiled source code for the project. As a result, theft of the drone easily leads to breaching the farmer's wireless network. Solving the problem of physical attacks, however, becomes challenging to overcome—if a user can update and read the software, how can you stop only the attacker? Erasing the ROM seems to be an option to prevent the leaking of network credentials, but other solutions may be better. Ultimately, securing the device against physical attacks would require extensive research that the technical project just does not have time to do nor the resources to do it.

Final Thoughts

The technical project—a soil-sampling drone—could benefit the lives of farmers by reducing costs and/or increasing data availability. However, this project has ethical concerns around it's disruptive nature, physical safety, rights of ownership, and cybersecurity. Some concerns can be resolved by fleshing out the prototype, others being a limitation of scope. The worst ones, however, have no clear solution, a concern that will exist in perpetuity. Yet, technology is incremental. To improve this technology, both in design and in ethics, engineers must work with the end goal and its effects in mind.