Safety & Acceptable Risks

Does the design pose any risk to users, operators, or the public?

While our design will be made to be as safe as possible, there are still risks. Due to the remote location, we will be using a battery to power our station. This battery will be rated to be outdoors, but outside factors could still damage the battery. We will have to consider that if the battery is damaged it does cause a fire risk. Outside manipulation, from animals chewing through casing, lightning strikes, or farming equipment damaging our equipment could pose a risk to our battery. Another risk is to the field technician that will service our design. Although we are choosing sensors that are easy and safe to replace, there is always a risk when working with electrical equipment. Lastly, given high wind speeds or tornadic conditions, if our design becomes unsecured from its mount, it could become a projectile.

Have you accounted for potential misuse or failure modes?

Our system is well made to avoid misuse. Because it will have set spots for specific sensors and placement for larger parts like the battery, solar panel, anemometer and rain garage, it is difficult to mess up the installment and misuse the station for other purposes. For failure modes, we could send data to the main server saying that the battery is almost dead (meaning something is wrong with charging). For sensors, we can physically see that the data is wrong on the receiving end, the only large failure for sensors is the rain gauge. If the water does not dump then the system should throw an error saying that the water is not dumping so someone can go fix it.

What safety standards or codes have you applied/considered?

The power system design, ethically, is one of the biggest considerations our team has in terms of safety. The reality of harnessing electricity, while the most powerful tool in our technology saturated society, is stark: it's dangerous. Amperages of mA magnitude can potentially be life ending for individuals. That being said, our power system needs to have the correct precautions in place to ensure the user's protection against accidents that could put this kind of current through someone's body. Codes from IEEE that we will reference include IEEE Std 1547-2018, the golden standard for interconnecting power distribution systems; IEEE Std 1547.1-2020, which outlines the standard testing procedures for ensuring the correct functionality of your system; and IEEE Std 1547.9-2022, which focuses more on small scale power distribution systems for individual applications. This is by no means an exhaustive list, but this will help give us an idea about how to design the system with these things in mind, as up to this point we've largely just considered applications in theory, where safety isn't a priority at all.

As for data distribution and transmission, we will have to comply with FCC Title 47 CFR Part 15 for unlicensed transmitters. Our device is an unlicensed transmitter which will need to be certified in order to sell the product. With this certification, this makes the data being transmitted legal.

Data, Privacy, and Security

How is data collected and how is that data protected?

The weather data we will collect in our final project is to be collected via sensors, as specified in our prior assignments. This data will be owned by the KSU Mesonet weather service and stored on their servers. Data will be transmitted via a cell modem and SIM card to the main KSU Mesonet data collection center, where it will be processed. For our project, we need to set up password protection to not allow outside users to ping our system, which would both use data and show up as data to the KSU Mesonet. Another protection we plan to put in place is encrypting our collected data when transmitting. The SIM card we chose already supports encryption algorithms, such as TLS, as does our microcontroller (the ESP32), which supports AES encryption (4G LTE uses AES), and we need to ensure that they are implemented into our final design.

If working with a client, who owns the data generated by the system?

The client for our project is the Kansas State University (KSU) Mesonet. The KSU Mesonet owns all raw data collected by our weather station design. They have the right to keep this data private while it is being processed and filtered for quality assurance. Once the data has been verified and prepared for release, it will be published on the official KSU Mesonet website for public access and research use. Our job is making sure that the raw data is secure and only sent to the KSU Mesonet. Only the KSU Mesonet will have access to the raw data until they decide to publish it. To keep the raw data secure, our system uses the MQTT communication protocol. MQTT is a reliable messaging system designed for IoT devices. It makes sure data transfer is secure through encrypted communication, authenticated access, reliable delivery, and data integrity. This makes sure that all information is accurate, reliable, and properly managed before being shared with the public.

Environmental Impact & Sustainability

Could materials or energy use be reduced without compromising performance?

The battery and solar panel size is a point of potential material minimization. Both batteries and solar panels are tough on the environment in harvesting the resources needed to manufacture them, so this is a big point of environmental impact. In terms of building materials, the body of our design will be minimized. This will limit the amount of plastic needed to 3D print its components. Energy use minimization is not as crucial, as our device will have its own power distribution network that does not interact with the grid in any way. The bigger issue, as mentioned in the risks above, is a battery fire. This could wreak havoc on the ecosystem surrounding our weather module, especially considering the wildfire risk in the dry Kansas climate.