Assignment # 4

**Create a purpose statement for the introduction you created in Assignment # 2.**

The development or research of hardware/software-based vulnerabilities for embedded devices, especially those in industrial control systems (ICS), is a long and drawn-out process. Because most researchers do not have access to the source code, or compiled firmware images built with debug symbols, it is difficult to understand what certain functions of a device might do without needing to intentionally trigger those mechanisms. By facilitating a compromised and more observable firmware image that’s applicable to a wide swath of devices, researchers could easily document hidden functions or discover physical limitations of hardware. This is something not readily available and nonstandard.

**What is the difference between a hypothesis and a null hypothesis?**

A hypothesis suggests that there is some kind of observable or measurable effect on the population or data. Whereas the null hypothesis suggests there is no effect at all. For example, a hypothesis would be that certain nutrients affect plant growth. A null hypothesis would say that fertilizing with skittles has zero effect on plant growth.

**What is the difference between a hypothesis and a research question?**

Hypotheses are typically statements structured around the relationships between 2 or more variables, that includes the predicted or expected outcome of the research. A research question is like a hypothesis, but less encompassing about variable relationships and more focused on specific aspects of the research. For example, the following two sentences:

* Hypothesis: Blue light from phones heavily disturbs the quality of sleeping. By reducing the amount of blue light, a subject is exposed to, their sleep should improve as well.
* Research Question: Does the level of blue light affect sleep quality?

**Write as many research questions as possible based on your planned research topic. Remember, they are to answer/address one focused part of your purpose.**

1. I mentioned using RTOS as the base firmware before for the foundation of the vulnerability dev suite; however, is it worth considering other images like Yoctow?
2. What types of devices will I be targeting? Embedded devices are a broad category with varying processing capability. Some run embedded Linux and others will be using smaller, scheduler based operating systems.
3. How will I address compatibility issues with generic libraries for hardware?
4. Will there be logging capabilities to capture the traffic/events?
5. Why did I pick one operating system or type of device versus another (RTOS or Yoctow)?
6. Are there any system limitations for remote debugger attachment?
7. What is there to gain from this over a specialized/custom firmware image for the targeted device(s)?