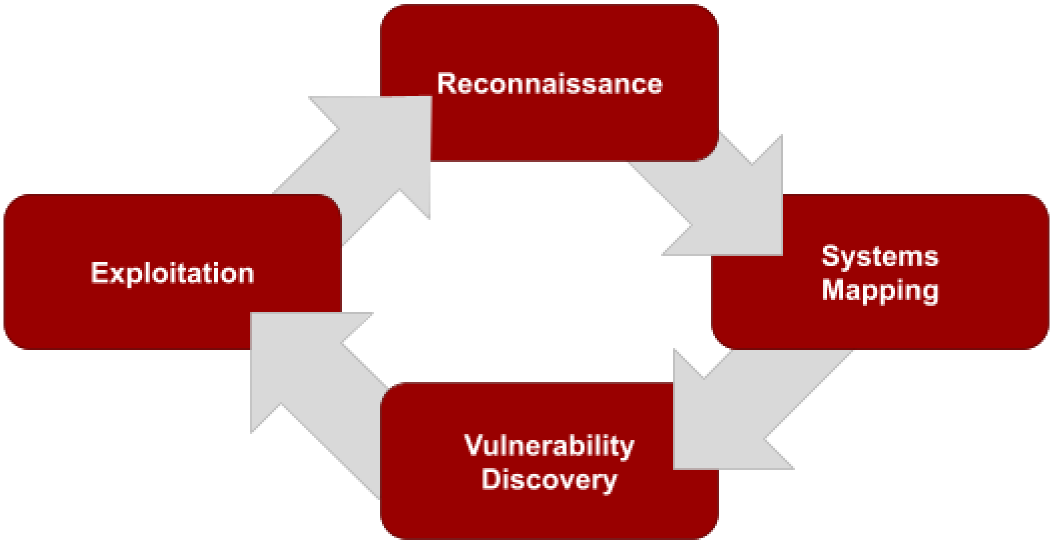
Secure Ideas follows an industry standard methodology for testing the security of embedded systems. This methodology is a four-step process as follows:



Note that the methodology is cyclical in nature. Successful exploitation may lead to additional iterations through the methodology.

Reconnaissance:
During reconnaissance, Secure Ideas staff will search public and private sources for information relative to the devices, to include: data sheets, as well as technical documentation and procedures. Examples of information that is gathered during reconnaissance include:

- Evaluating data sheets to identify hardware components
- Identifying any serial connections or JTAG interfaces
- Utilize information from FCC database for any prior testing and corresponding results
- Vulnerabilities that have been publicly disclosed in the past

Secure Ideas will include information discovered as part of the final report if it is relevant to any of the exploitable findings found during the penetration testing.

Device Mapping:
The next step in the methodology is mapping, which is where Secure Ideas will study the behavior and data in the target device. Secure Ideas understands that embedded device testing allows for the possibility that access to the firmware from the hardware may not be possible. In gaining access to any communication interface, the following items are examples of what would be covered in this step:

- Dumping firmware, flash, or memory from the device

- Understanding the device architecture (e.g. authentication mechanisms, file systems, update procedures)
- All communication where information is sent to and from the server
- Review of file system and configuration saved to the firmware or available in memory
- Identify custom security measures in addition to platform security controls
- Identify sensitive data in any inputs to the device, including encoded data

Note, the above list is not exhaustive. If Secure Ideas encounters service behavior that falls outside of the usual, it will be treated as an area of interest and scrutinized accordingly.

Discovery:
During the discovery stage of the embedded device penetration test, Secure Ideas will use the information gathered in the previous two steps to assist our staff in finding the vulnerabilities within the target devices. Additionally, the device's persistent storage and caching on the device will be examined. If possible, the embedded systems will be decompiled and examined. There are two decoupled portions to the test: the physical inspection and the client server communication. Using this information combined with manual testing, Secure Ideas will provide thorough coverage for all common embedded device vulnerabilities and will also seek out less common vulnerabilities depending on the device architecture and features. Testing will be comprised of the following investigations:

- Unencrypted communication
- Default credentials
- Poor service configuration
- Input sanitization with respect to services
- Update Mechanism for each device

Exploitation:
Exploitation is the final step of the embedded device penetration test. By exploiting the vulnerability, Secure Ideas is able to provide a realistic understanding of the business exposure from the target. Exploitation exercises are often limited to the minimum required to build a proof of concept so that security staff may reproduce the issue. Secure Ideas may go beyond a proof of concept if pivoting and post-exploitation is in scope for the test (uncommon). An example of post-exploitation would be if Secure Ideas is able to achieve access to an update server from the embedded system.