**CYBR 3520 Introduction to Cyber-Physical Systems Security**

**Homework #4**

Please read the textbook from page 116 to page 121 and answer the following questions.

***Strict Real-Time Requirements***

1. [2 pts] How can a slowed-down SCADA cause a disaster? Explain and show an example.

A slow down in response time can cause incorrect actuations. If a device needs another device to hand off a manufactured part to and one is falling behind, this can stop an entire line and even cause lots of damage.

***Continuous Availability***

2. [2 pts] Briefly describe how the requirement of continuous availability may contribute to a buffer overflow vulnerability of SCADA field devices. Since these devices are not focused on security, certain countermeasures may not be enabled in effort to save time. They may also not be enabled just because the system operators don’t feel the need to have them on, which is a bad idea.

***Misguided Security Perceptions***

3. [4 pts] In most cases, relying on security by obscurity is considered a mistake. Provide two reasons why this is the case for SCADA systems. Well one reason is that if someone finds out your secrets within your system, they will probably have dangerous amounts of access. It will also be a problem because you then have to implement brand new security measures as the previous ones would then be obsolute.

***Commercial-off-the-Shelf Hardware and Software***

4. [2 pts] What might be a problem using COTS hardware and software? This type of software might not have what you need inside it, but is also hard to configure too deeply as they are usually proprietary.

***Interconnectivity***

5. [2 pts] Even if there is no network connection between a system and the outside world, it is still possible to infect the system. Explain how this would be possible. A malicious actor could still bring in an infected device and plug it into the network. It is more difficult but still possible.

***Internet Accessibility***

6. [4 pts] Describe the pros and cons allowing access to a SCADA system’s HMI and databases through the Internet. This is very convenient, but any internet access to devices is always a vulnerability, and a possible vector for an attack. Information can be intercepted and compromised that way.