

SCADA Attack System

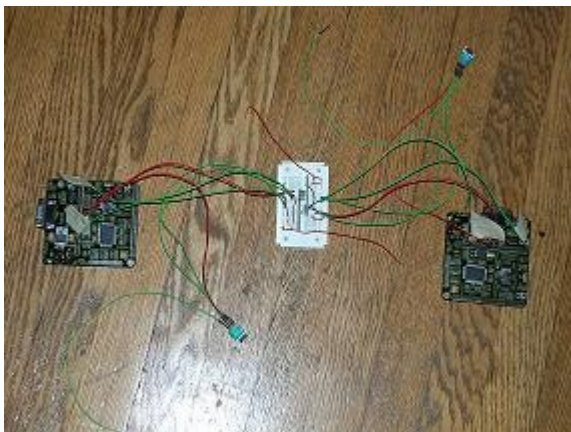
Real-Time Embedded Systems, George Washington University, Spring 2006

Ryan Festag – rfestag@gwu.edu

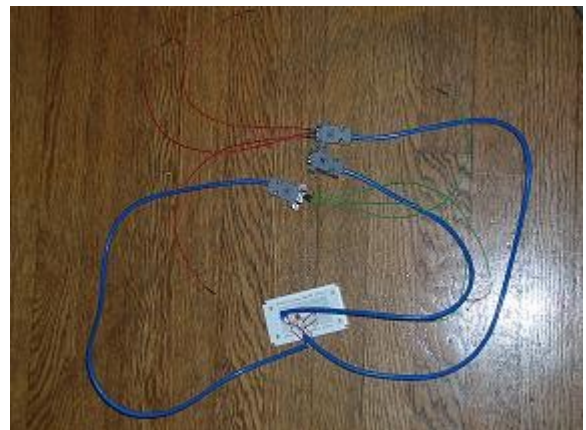
Project Abstract

The SCADA Attack System (SAS) provides wireless attack vector for devices receiving commands via a serial connection. Two devices are used in order to accomplish this: a SAS-Listener and a SAS-Attacker. The Listener utilizes a spy cable to eavesdrop on transmissions from a command station, and to send data to a Remote Terminal Unit. Anything it receives from the command station is automatically forwarded to the Attacker for analyses. The attacker can then send commands back through the RF Link to the Listener, and that data will be injected.

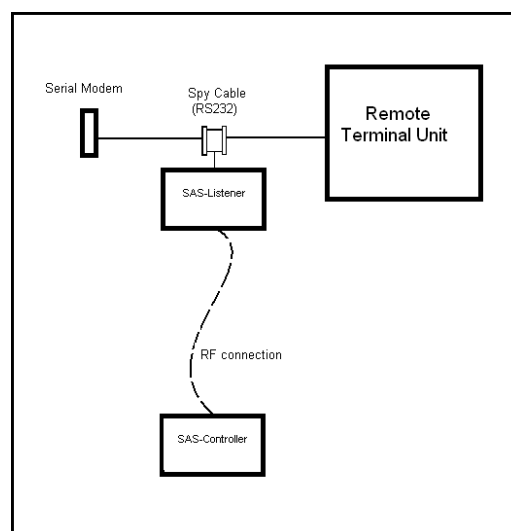
Final Project



Attacker and Listener

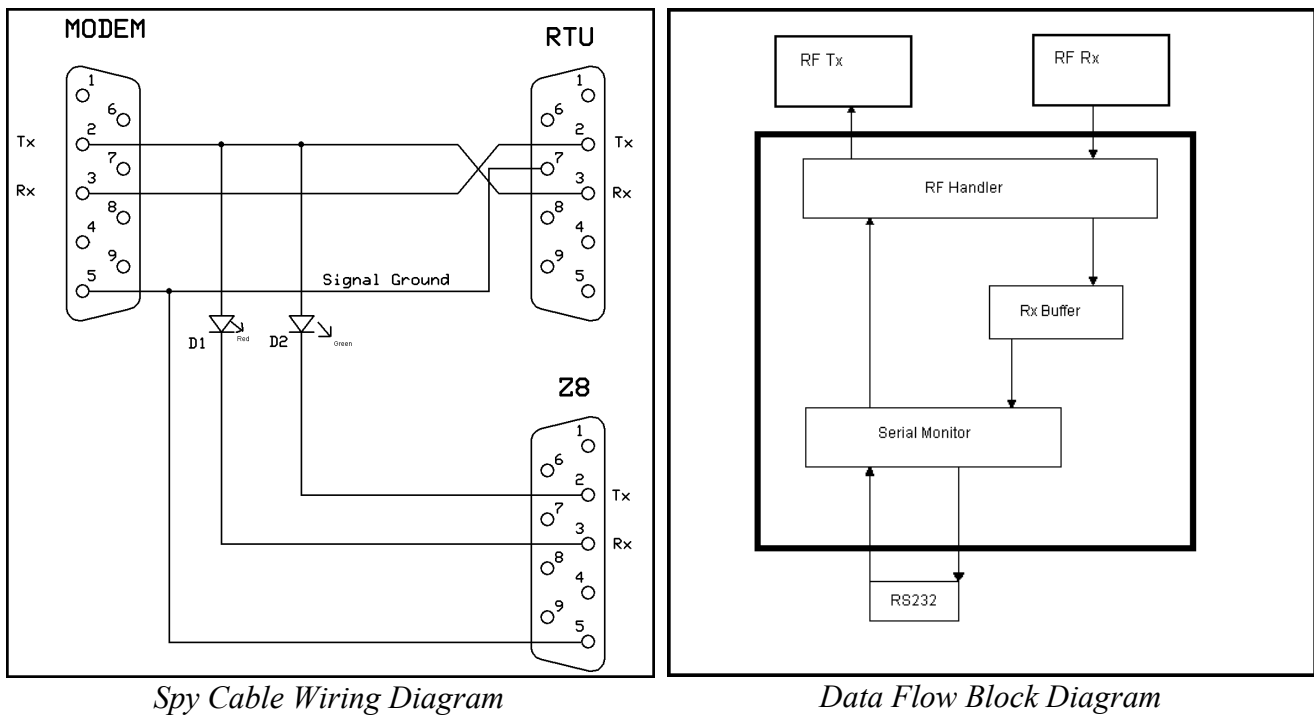


Spy Cable



Overall Layout

Implementation and Design:



Lessons Learned:

- Interference is a very difficult problem when dealing with wireless communications. Even simple systems need to find some way of validating data. Framing the data with start and stop bytes works, but it still leaves room for errors.
- RF Receivers don't seem to like it when their transmitters are on the same breadboard. In general, it appears to be best if the transmitter is not resting on the same breadboard as its receiver.
- RF is difficult to troubleshoot. Development should be done in a location where you know exactly what frequencies are being used.