

# Project Proposal SCADA Attack System

February 10, 2007

Ryan Festag, [rfestag@gwu.edu](mailto:rfestag@gwu.edu)

## Project Abstract

The SCADA Attack System (SAS) will provide wireless attack vector for devices receiving commands via a serial connection. A single SAS-Listener device will be placed between the serial modem and the target device. It will transmit all data sent to it from the serial modem to a SAS-Controller device via an RF connection. The SAS-Attack device can then be used to analyze protocols used or inject data into the via the wireless RF connection.

## Strategy

Description of the overall design: Above

Platform: Both devices will be based on the Zilog Zneo chip and development platform

Capabilities: Both will implement serial inputs, timers, GPIO outputs (for RF)

External: RF transmitter/receiver

Software modules:

Both: *RF manager*- Transmit/receive from other device. To be designed so that both devices can use the same RF drivers.

*Main loop*- Controls operations (different for each device)

SAS-Listener: *Serial manager*-Transmit to RTU, receive from serial modem. Will buffer input (at 9600 bps) to transmit at 4800 bps. Place received data into the RF transmit queue. Data to transmit will be received from the RF received queue.

SAS-Controller: *Interrupt Handler (Button)*- Tells what message to transmit to the SAS-Listener.

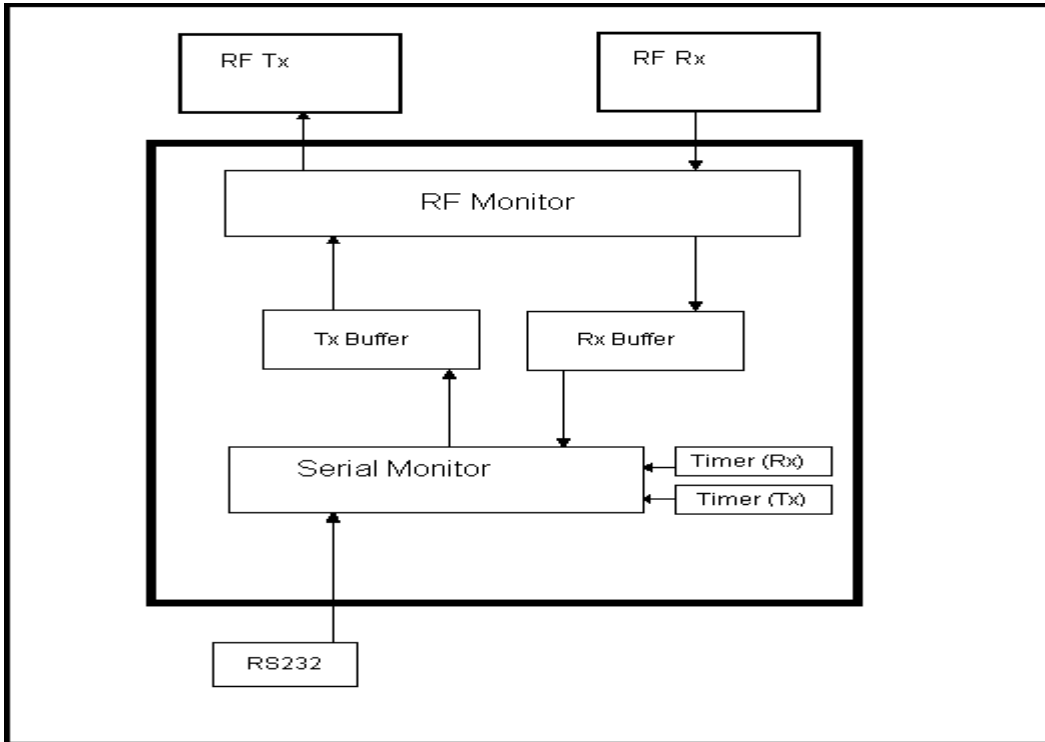


Figure 2: SAS-Listener Software Diagram

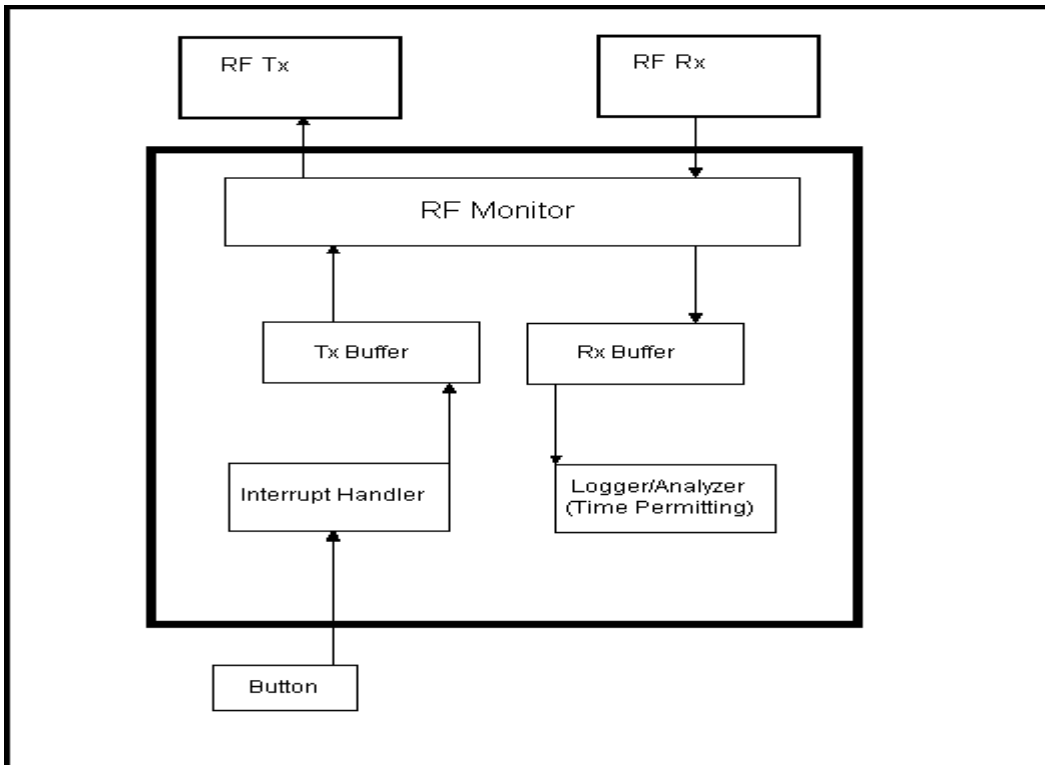


Figure 3: SAS-Controller Software Diagram

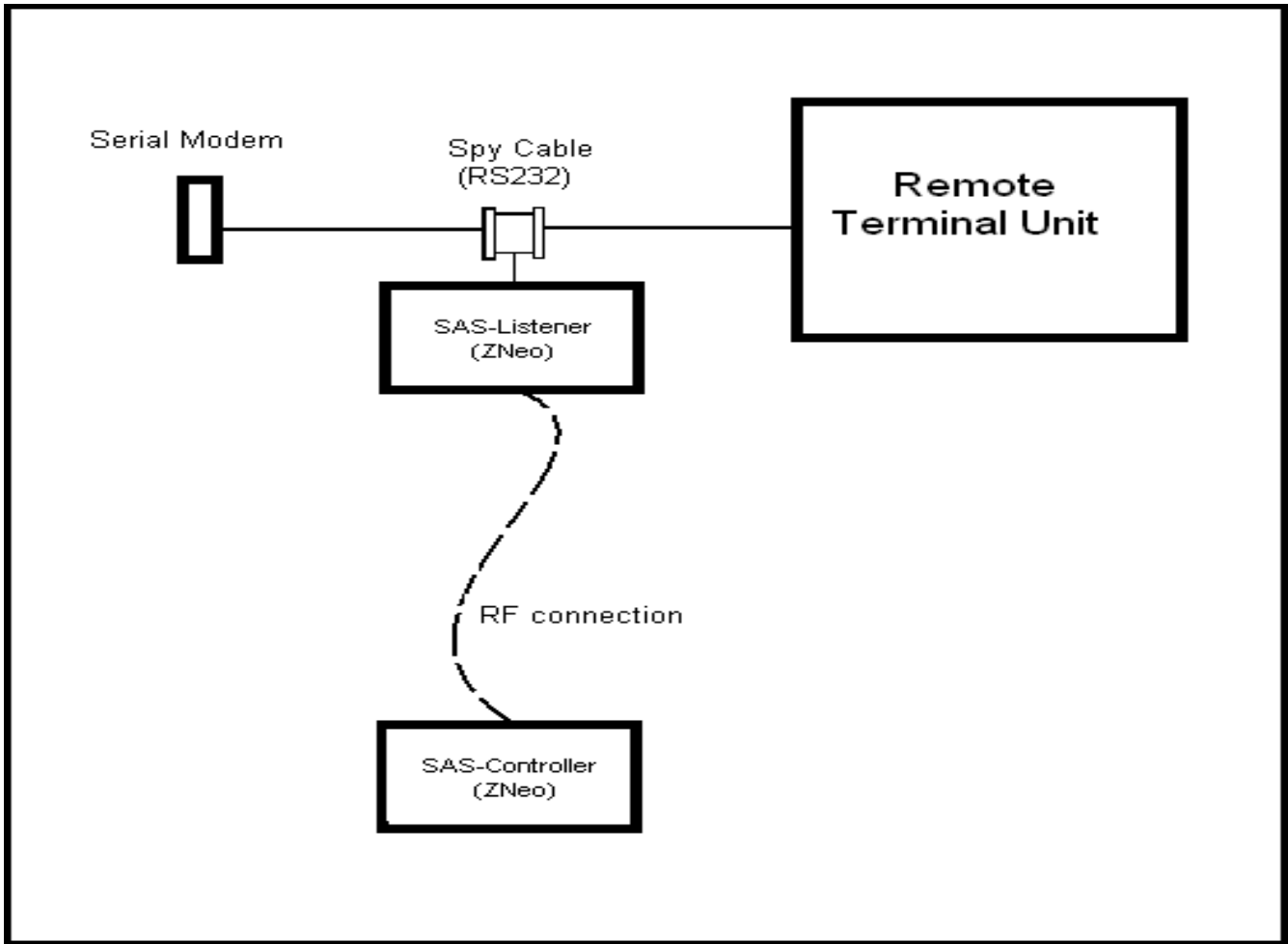


Figure 1: General Setup Diagram

## Unknowns

Ideally, I would like to power the SAS-Listener with a battery. However, due to the Zneo's design, I may choose to use AC power for demonstration purposes.

I will have to work out the details of the spy cable. I have found some documentation on how the 9-pin RS232 works, and have found a diagram for a spy cable. However, it looks like I may have to construct my own. To simplify the implementation, I plan to only monitor in half-duplex mode (ignoring data sent from the RTU)

## Implementation Plan

Purchase two small Zneo kits and two 4800 bps Tx/Rx pair RF transmitters (433 Mhz)

Write RF driver and implement simple communications protocol for the Zneos

RF Monitor

Construct a working RS232 9-pin “spy” cable

Serial Monitor

Create buffer between Serial Monitor and RF Monitor for Tx/Rx

Send attack when button pressed on SAS-Controller.

Build logger (perhaps output to serial monitor)

Build battery pack and test lifetime.

Write logger/analyzer (Display data on serial terminal at SAS-Controller).

By Spring Break, I hope to have the RF communication between the Zneos completed, and to also be capable of transmitting from the SAS-Controller device to the SAS-Listener. The Listener should at least be putting the data on the UART's transmit line (which will be tested with serial analyzing software).

During an after Spring Break, I hope to build and complete the “spy” cable, and to have the SAS-Listener send the data from the cable to the SAS-Controller.

There are two primary challenges in this project. The first will be the RF communications between the two boards. Since I am using a simple RF link, I will have to find some way of telling the controllers to ignore the data that they are actually sending. The simplest way around this is probably to simply disable the receiver on the transmitting board whenever sending; however, this could cause loss of data when sending. A more robust solution would be to transmit a “sending” message first. The receiving board would then know not to send data until it receives a “done” message. Initially, however, I will probably just disable the receiver when transmitting data.

The second challenge will arise when I am retransmitting the data recorded from the “spy” cable to the SAS-Controller, because the UART will be operating at twice the maximum transmit frequency of the RF links. However, if the buffers are implemented properly, this shouldn't prove to be overly difficult to implement.

## Resources

2 small Zneo boards (Purchase through NDU)

2 RF Links (Purchase through NDU)

Small breadboard (Purchase through NDU).

Single button (Purchase through NDU)

Equipment for “spy” cable (Purchase through NDU)

RTU (From NDU)

Serial Modem (From NDU)