**实训中心实验计划**

1. **一次设备数据包的篡改与变量控制**

针对变电站的一次设备，特别是断路器或则其它被GOOSE协议控制的设备，通过获取正在传输的GOOSE包，利用python脚本修改的三个字节：stNum、sqNum、Boolean Values。stNum是指当报文中数据有变化时，此值加一；sqNum是报文递增标识；Boolean Values是指传输data中所有的boolean值。通过修改这些字节，将数据包进行重新组装，利用软件选择网卡进行发送。

1. **非IP设备连续发包机制设计与一次设备的模糊测试机制实现与算法设计**

针对对变电站一次设备进行模糊测试，可以检查出一次设备代码可能出现的问题。首先我们必须要有在电脑中对非IP设备进行连续发包的能力，这是第一步需要实现的。现有的发包机制均为socket，只针对TCP/IP设备与协议。

在获得连续发包的能力之后，我们需要设计相应的模糊测试机制，这方面的方案包括两种，一种是基于生成的模糊测试机制，主要思路是重写协议，进行单字节或则多字节变异；第二种方法是基于变异，尝试利用现有的AFL工具进行定向变异，根据是否获得回复等反馈获得下一步应该继续变异哪些种子。

1. **变电站数据注入攻击实现**

SV协议为一次设备互感器将传感器测量值向上传递等协议，我们可以探索通过对SV协议的数据篡改对上位机设备以及调度中心的可能影响作一次评估。