#### 1.1测试环境简介



图1-1 工业控制系统信息安全实验平台的拓扑结构

如图1-1工业控制系统信息安全实验平台的拓扑结构，测试环境，包括防护模块规则配置端，模拟攻击端，PLC监控端，防护模块，以及模拟控制端。防护模块规则配置端可以实现对防护模块的访问控制规则以及深度包检测规则的配置。根据不同的工业控制协议，我们分别在模拟供给端和模拟控制端，安装基于不同工业控制协议的客户端与服务器端软件。模拟进行基于工业控制协议的通信过程。通过发送不同的数据包来观察防护模块对于不同数据包检测与防护能力。

#### 1.2基于EtherCAT协议的测试

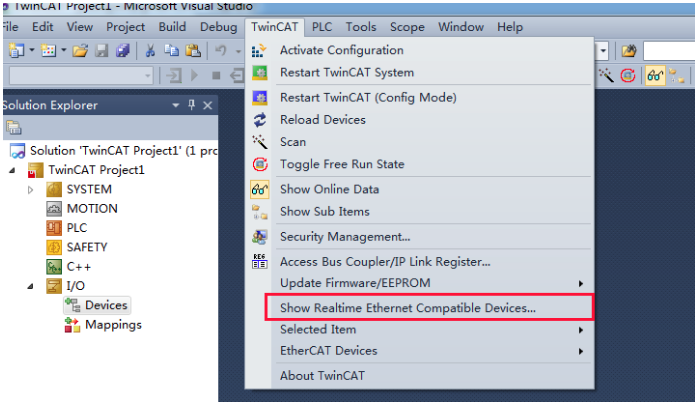
试验测试通过分别在模拟攻击端和模拟控制端分别安装EtherCAT客户端软件SOEM与服务器软件SOES建立通信过程，客户端发送数据包通过工业控制防护系统到服务器端来进行验证。

#### 1.3测试过程

试验测试通过分别在模拟攻击端和模拟控制端分别安装EtherCAT客户端软件与服务器软件建立通信过程，客户端发送数据包通过工业控制防护系统到服务器端来进行验证。.

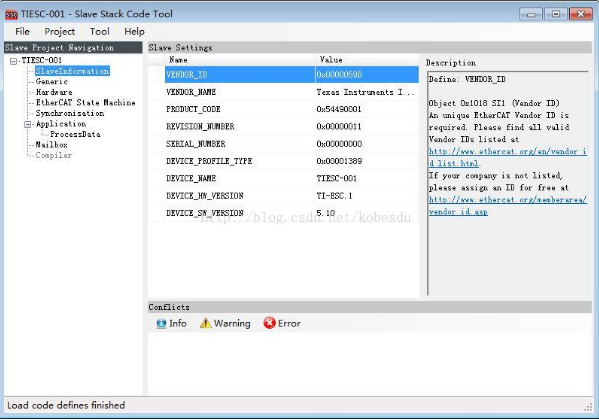
1）利用 TwinCAT 3 搭建 EtherCAT 主站环境

安装驱动



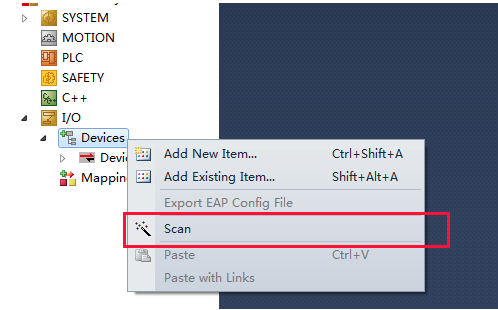
2）[EtherCAT从站配置](http://blog.csdn.net/kobesdu/article/details/41869995)

参考EtherCATSlave Implementation Guide（EtherCAT从站实施指南）作为从站实施的开始。所使用的从站配置工具SSCtool如图所示

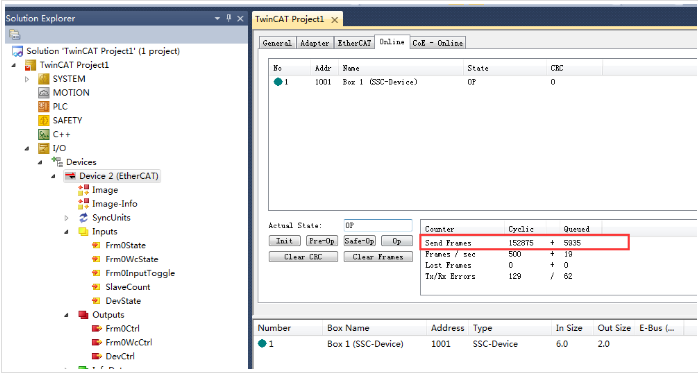


3）建立项目并捕捉数据

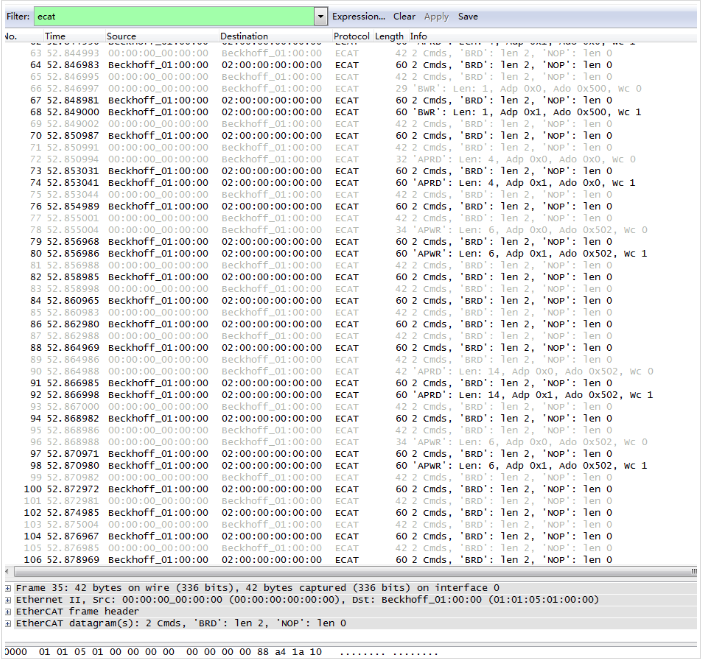
新建 TwinCAT XAE Project 项目，建立完成之后连接 EtherCAT 从站，在工程 I/O 下面 Devices 处扫描设备，如下图：



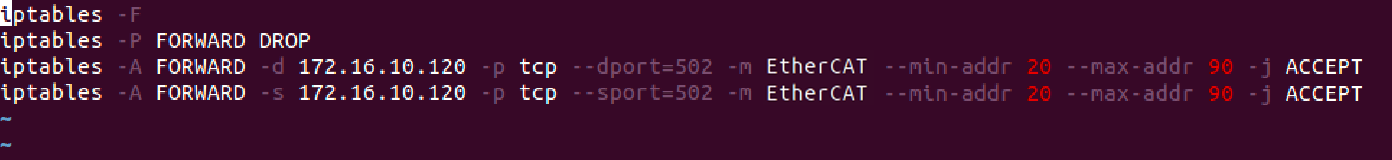
4）发送数据帧



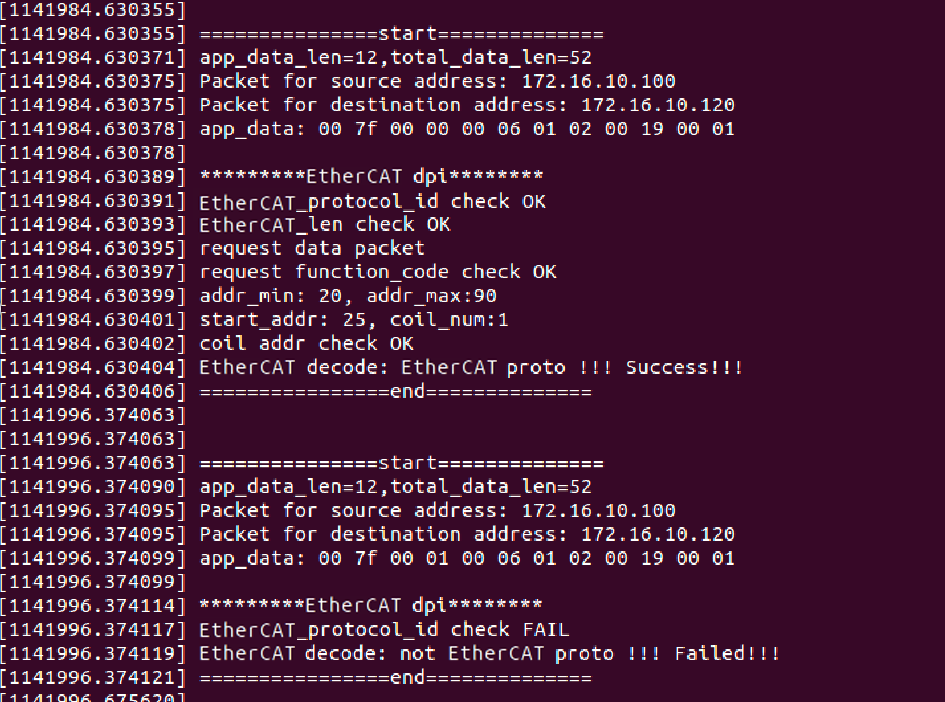
查看通信数据：



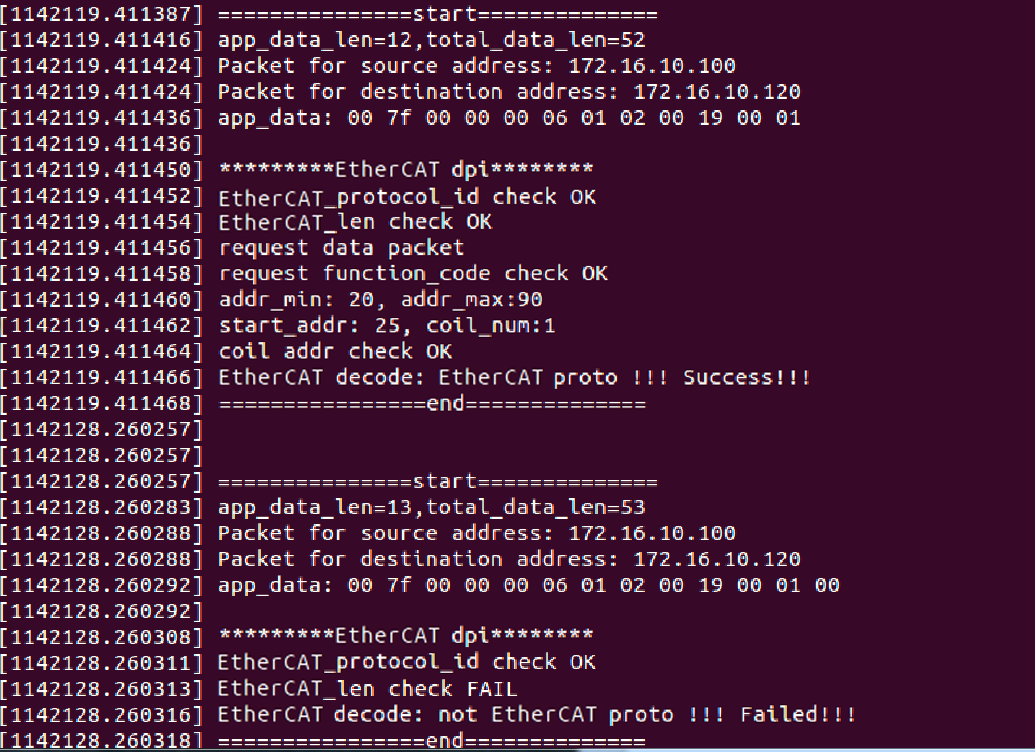
5）防火墙规则：



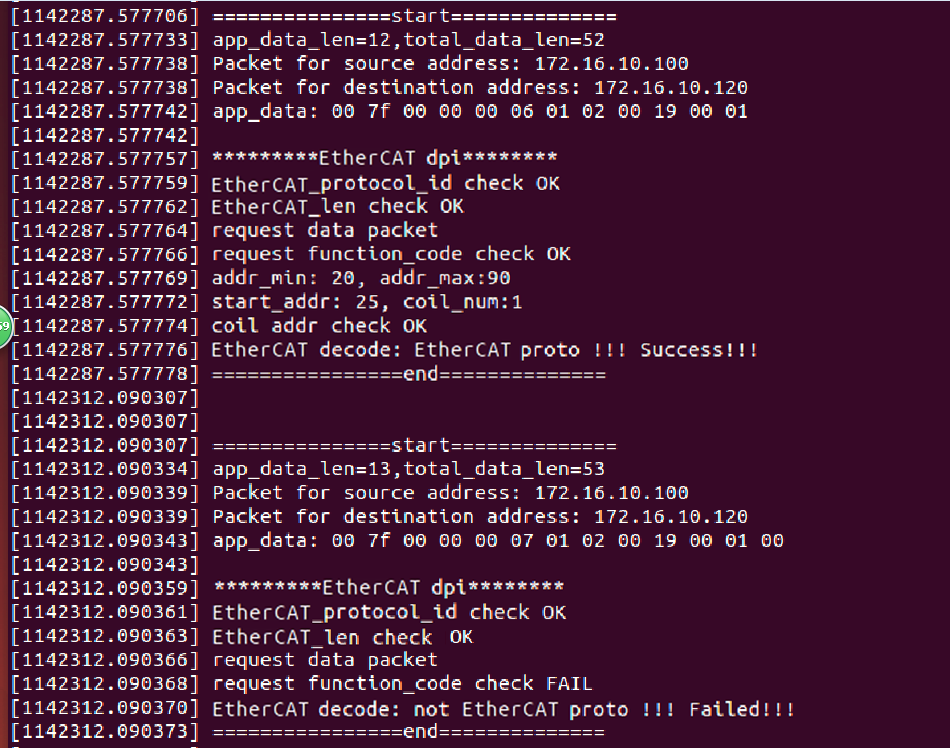
6）EtherCAT协议头检测：



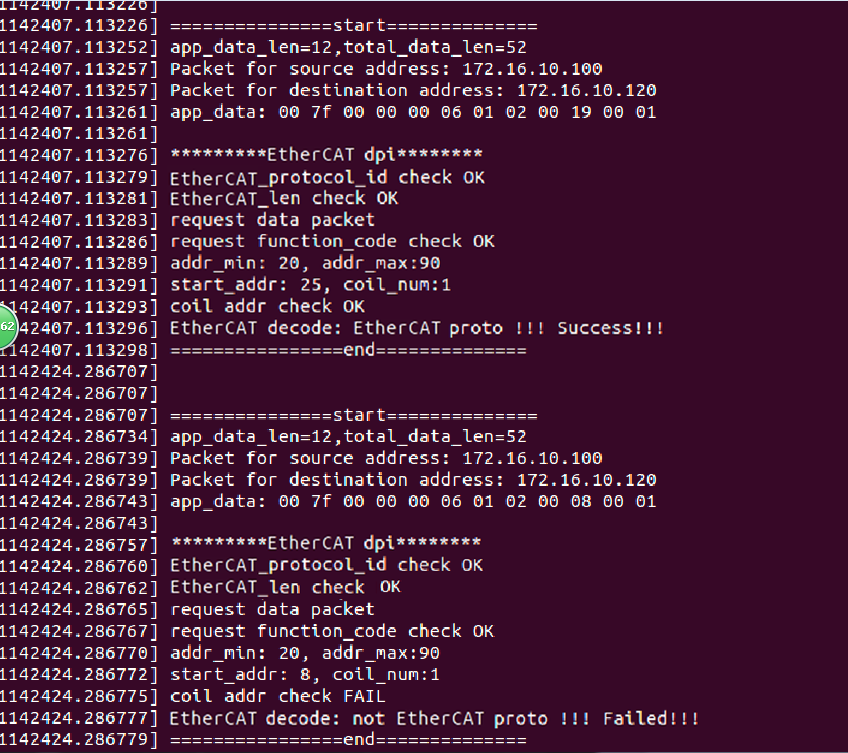
7）EtherCAT数据长度检测



8）EtherCAT地址区检测



9）EtherCAT数据区检测：



#### 1.4总结

通过实验测试可知，该防护模块基于EtherCAT进行深度包解析，实现访问控制和通信管理,从而有效的实现防护功能。