附件 2

2020 年度上海市级虚拟仿真实验教学课程（原虚拟仿真实验教学项目）申报表

学校名称	上海电力大学
实验教学项目名称	电力 SCADA 系统网络攻击防御
所属课程名称	工业控制系统安全
所属专业代码	080904K
实验教学项目负责人姓名	王勇
有效链接网址	http://pt.thingeasy.cn/experiment/detail/751.html

上海市教育委员会制

二〇二〇年十月

填写说明和要求

1. 以 Word 文档格式，如实填写各项。

2. 表格文本中的中外文名词第一次出现时，要写清全称和缩写，再次出现时可以使用缩写。

3. 所属专业代码，依据《普通高等学校本科专业目录（2012 年）》填写 6 位代码。

4. 不宜大范围公开或部分群体不宜观看的内容，请特别说明。

5. 表格各栏目可根据内容进行调整。

1.实验教学项目教学服务团队情况

1-1 实验教学项目负责人情况					
姓　名	王勇	性别	男	出生年月	1973-2
学　历	博士	学位	博士	电　　话	65514261
专业技术职务	教授	行政职务	无	手　　机	13371896817
院　系	计算机科学与技术学院，信息安全系			电子邮箱	wy616@126.com
地　址	上海市浦东新区沪城环路1851号			邮　　编	201303

教学研究情况：主持的教学研究课题（含课题名称、来源、年限，不超过5项）；作为第一署名人在国内外公开发行的刊物上发表的教学研究论文（含题目、刊物名称、时间，不超过10项）；获得的教学表彰/奖励（不超过5项）。

1）主持的教学研究课题（含课题名称、来源、年限，不超过5项）；

（1）“信息安全专业一流教学团队”，上海市高水平地方建设大学专项项目，2019

（2）“智能电网信息安全创新人才培养方法研究”，上海电力学院，重点教改，2018

（3）《工业控制系统安全》，上海电力学院，慕课建设，2017.

（4）《工业控制系统安全》，上海电力学院，骨干课程建设 ,2015

（5）《信息安全专业网络创新教育培养模式研究》，上海电力学院，重点教改，2014

2）作为第一署名人在国内外公开发行的刊物上发表的教学研究论文

[1] 王勇,高志远,刘金永,王相,李双飞,邵猷海,翟昊,刘蔚.电力控制系统信息安全实验平台设计[J].自动化博览,2018,35(S2):84-87.

[2] 王勇,周林.电力特色信息安全专业创新人才培养模式研究[J].中国电力教育,2014(09):24-25+27.

[3] 王勇,段存升,罗静,洪月好.计算机病毒免疫系统的仿真试验教学[J].实验室研究与探索,2006(02):192-193+271.

3）获得的教学表彰/奖励（不超过5项）

(1) 2021年工业互联网安全大赛上海选拔赛，学生组，一等奖，指导教师

(2) 2021年上海电力大学，优秀本科毕业设计，曹可凡，指导教师

(3) 2019年上海电力学院，优秀本科毕业设计，沈鹏飞，指导教师

(4) 2018年上海电力学院，优秀本科毕业设计，汪心桐，指导教师

(5) 2017年上海电力学院，优秀毕业毕业设计，潘玺廷，指导教师

学术研究情况：近五年来承担的学术研究课题（含课题名称、来源、年限、本人所起作用，不超过 5 项）；在国内外公开发行刊物上发表的学术论文（含题目、刊物名称、署名次序与时间，不超过 5 项）；获得的学术研究表彰/奖励（含奖项名称、授予单位、署名次序、时间，不超过 5 项）

1）近五年来承担的学术研究课题（含课题名称、来源、年限、本人所起作用，不超过 5 项）；

(1) “电力 SCADA 系统假数据注入攻击的关系图谱检测方法研究”，上海市自然科学基金，20ZR1455900，2020/7-2023/6，在研，主持

(2) “数据库服务中数据的隐私保护及可控关键技术研究”，国家自然科学基金委员会，61772327，2017-01 至 2020-12,63 万，结题，参加

(3) “面向智能电网互动用电信息质量的数据安全关键技术研究”，上海市科委地方能力建设项目，15110500700，2015/10-2018/10，100 万，已结题，参加。

(4) “电网信息安全监测装置的研制与应用”，上海电力大学智能电网产学项目，2017/05- 2019/5，35 万，已结题，主持。

(5) “电力 SCADA 系统中病毒入侵检测关键技术研究与应用”，上海浦江学者创新基金，16PJ1433100，，2016/07-2018/07，20 万，已结题，主持。

2）在国内外公开发行刊物上发表的学术论文（含题目、刊物名称、署名次序与时间，不超过 5 项）；

[1] **王勇** ；王相；刘丽丽；刘金永；武津园；李双飞；配电网 IEC60870-5-104 协议的 抗中间人攻击算法，信息安全学报（CCF B 类），2019，4(6)：56-66.

[2] **Yang Y.**, Liu J., Zhang Y., An Analysis of the Implications of China’s Urbanization Policy for Economic Growth and Energy Consumption. Journal of Cleaner Production Vol. 161 (2017) 1251-1262. [2]Wang, Yong; Xu, Zhaoyan; Zhang, Jialong; Xu, Lei; Wang, Haopei; Gu,Guofei ;SRID: State relation based intrusion detection for false data injection attacks in SCADA , Computer Security - ESORICS 2014 - 19th European Symposium on Research in Computer Security （CCF B 类），Wroclaw, Poland, 2014-09-07 至 2014-09-11.

[3] 国家标准,信息安全技术工业控制系统网络审计产品安全技术要求，GB/T 37941-2019，全国信息安全标准化技术委员会，2019-08-30. 参与

[4] 国家标准，工业控制系统专用防火墙技术要求，GB/T 37933-2019，全国信息安全标准化技术委员会,2019-8-30. 参与

[5] 国家标准，工业控制系统的信息物理融合异常检测系统技术要求，国标计划：20190643-T-604，全国自动化系统与集成标准化技术委员会,2021-1-7.

1-2 实验教学项目教学服务团队情况

1-2-1 团队主要成员（含负责人，5 人以内）

序号	姓名	所在单位	专业技术职务	行政职务	承担任务	备注
1	王勇	上海电力大学	教授	无	主讲	
2	周林	上海电力大学	副教授	系主任	综合实践	
3	陈思远	上海电力大学	讲师	无	综合实践	
4						
5						

1-2-2 团队其他成员

序号	姓名	所在单位	专业技术职务	行政职务	承担任务	备注
1		奇安信科技集团股份有限公司	工程师	无	技术指导	
2	郭乃网	国网上海市电力公电力科学研究院	工程师	国网大数据安全中心副主任	技术指导	
…						

项目团队总人数：5（人）高校人员数量：3（人）企业人员数量：2（人

注：1.教学服务团队成员所在单位需如实填写，可与负责人不在同一单位。

2.教学服务团队须有在线教学服务人员和技术支持人员，请在备注中说明。

2. 实验教学项目描述

2-1 名称

电力 SCADA 系统网络攻击防御

2-2 实验目的

电力系统面临严峻的网络攻击风险，2010 年伊朗核电站的震网 Stuxnet 病毒导致离心机故障，2017 年出现的乌克兰电力系统的 BlackEnergy 病毒对变电站系统攻击，导致大面积停电事故。2019 年南美洲多国发生大停电事故，美大停电事故被怀疑是网络攻击导致。

我国电力 SCADA 系统面临巨大的网络攻击风险，但是无法对真实变电站发生攻击测试，因此需要建立模拟环境，连接网络，了解网络攻击对变电站系统发生的影响。

（1）了解变电站的的实物结构；

（2）掌握变电站 SCADA 监控室的操作，了解变电站 SCADA 系统的的操作过程；

（3）掌握变电站系统攻击的核心原理，通过网络攻击手段，获得变电站 SCADA 系统上位机的控制权，或者通过截获或者篡改变电站的通信数据，影响变电站的异常动作，从而破坏变电站的正常运行，引发变电站事故。

（4）掌握针对该种类型攻击的防御措施，促进学生对变电站攻击手段的理解，提高防御攻击的技能。

2-3 实验课时

（1）实验所属课程所占课时：16

（2）该实验项目所占课时：　2

2-4 实验原理（简要阐述实验原理，并说明核心要素的仿真度）

知识点：共__4___个

2-4-1 简要阐述实验原理

（1）了解变电站的的实物结构，包括：110KV 变电站组织工作原理（主变压器，10KV 高压区，110KV 设备区），变电站 SCADA 系统的部署两大部分（变压器，隔离开关，电压互感器，电流互感器，六氟化硫隔离开关，避雷器，母线排）

（2）掌握变电站 SCADA 监控室的操作（变电站巡检报告，了解变电站安全的检测点），了解变电站 SCADA 系统的的操作过程（分类信息：110KV 接线图，1 号主变，2 号主变，开关状态）；

（3）掌握变电站系统攻击的核心原理，通过多种网络攻击手段，获得变电站 SCADA 系统上位机的控制权，或者通过截获或者篡改变电站的通信数据，影响变电站的异常动作，从而破坏变电站的正常运行，引发变电站事故，查看变电站的虚拟仿真的刀闸是否打开。

（4）掌握针对该种类型攻击的防御措施，监控网络攻击是否能够导致变电站刀闸打开，提高防御攻击的技能。

该仿真试验的核心因素，不仅实现了变电站设备级仿真，而且**仿真系统提供了 IP 地址与端口号，与 SCADA 软件系统连接，能够实现网络攻击效果的真实展示**。

2-4-2 核心要素仿真度

本次试验的总体思想：了解变电站的核心设备，了解变电站系统的核心通信设备，掌握变电站 SCADA 系统主站的操作步骤，学生通过网络连接到仿真系统，通过网络攻击导致变电站刀闸开启，通过防御手段防御攻击行为，维护变电站 SCADA 系统安全。

其核心要素包括，变电站系统设备仿真，变电 SCADA 监控主站系统仿真，变电站网络攻击导致的刀闸打开仿真。

（1）变电站的实物结构仿真

学生很不方便了解变电结构，学校需求提前变电站提出认知实践申请，得到批准后，带领学生到变电参观，需要站住线外观看，认知实践收到时间和地点的制约。虚拟仿真解决了这个困难问题，学生可以直接通过虚拟仿真系统，，了解变电站设备的物理结构，解决了这个实际困难问题。110KV 变电站组织工作原理（主变压器，110KV 设备区，10KV 高压区）如图 1 所示。

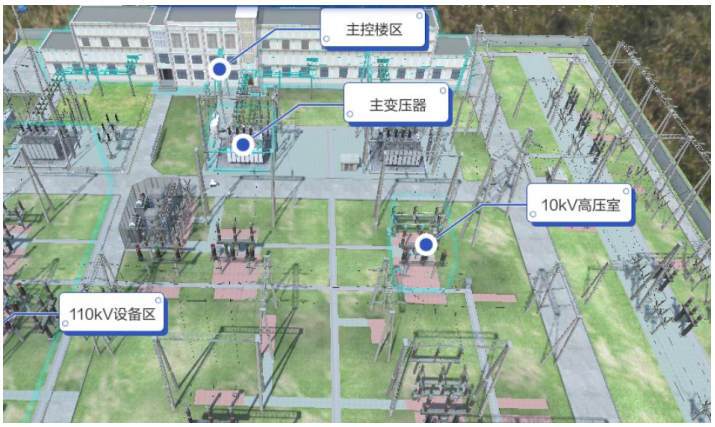

图 1. 变电站系统鸟瞰图

变电站 SCADA 系统的部署两大部分（变压器，隔离开关，电压互感器，电流互感器，六氟化硫隔离开关，避雷器，母线排），如图 2 所示。

图 2. 变电站系统中变压器的巡检仿真

（2）变电站 SCADA 监控室的操作仿真

巡检结束后，到变电站监控室填写巡检报告，包括变压器，隔离开关，断路器的巡检结果。如图 3 所示：

图 3. 变电站监控室填写巡检报告

操作变电站监控系统，查看主站接线图，分类信息：110KV 接线图，1 号主变，2 号主变，开关状态，如图 4 所示：

图 4. 变电站 SCADA 系统操作仿真

这种变电站 SCADA 系统的操作是在对变电站巡检之后，对整个变电站系统有了感性认识，更加容易理解主变压器，隔离开关，数据传输的过程，对于信息安全专业的学生，在没有电气工程相关知识的背景下，快速理解了变电站通信的过程原理，提高了掌握知识的效率。

（3）变电站网络攻击防御仿真

电站系统攻击的核心原理，通过多种网络攻击手段，获得变电站 SCADA 系统上位机的控制权，因此**变电站虚拟仿真系统提供了与变电站 SCADA 系统软件的网络接口**，如图 5 所示：

图 5. 变电站仿真系统连接 SCADA 系统

虚拟仿真系统从电力 SCADA 系统中读取数据，刀闸根据状态和远程控制命令，可以启动关闭和开启状态。如图 6 所示：

图 6. 变电站刀闸根据 SCADA 控制命令合上刀闸

或者通过截获或者篡改变电站的通信数据，影响变电站的异常动作，从而破坏变电站的正常运行，引发变电站事故，查看变电站的虚拟仿真的刀闸是否打开。

本虚拟仿真系统，提供与了变电站 SCADA 系统的 IP 链接，实现了虚拟系统可以采集网络系统中的数据，让仿真系统可以根据网络参数的改变，转变系统状态信息和控制命令，实现刀闸的开启与闭合。

学生根据网络攻击工具，采取多种攻防手段对网络扫描，启动刀闸，改变

状态，通过漏洞扫描，渗透测试、中间人攻击，漏洞利用等方式获得变电站系统的上位机的控制权，从而破坏变电站的正常运行。或者通过截获或者篡改变电站的通信数据，影响变电站的异常动作，引发变电站事故。针对网络攻击，可以采用多种防御方法进行防御，主要采用的技术手段包括 VLAN 网络分区，访问控制，SnortIDS，数据篡改攻击检测，控制命令攻击检测等， 学生在做试验过程中，采用红蓝战队的形式，红队防御，蓝队攻击，对抗性非常强，激发了学生的兴趣。并且也展示了变电站 SCADA 系统的网络攻击效果。为工业信息安全技能训练提供了靶场，培养了技能型人才。

2-5 实验仪器设备（装置或软件等）

服务器：变电站 SCADA 系统攻防虚拟仿真平台

http://pt.thingeasy.cn/experiment/detail/751.html

学生机：安装 Kingview SCADA 3.7

网络攻击工机集（Kali）

网络防御工具集（Snort, Python）

Vmware 虚拟机（Ubuntu, Win7）

2-6 实验材料（或预设参数等）

1）设置数据库服务端主机，将主机 ip 改为 192.168.1.106，然后运行力控和 kingview 程序。

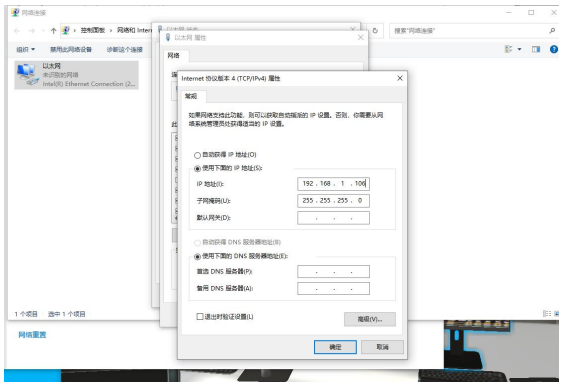

图 7 IP 地址设定

2）接着打开 Dbcommservice

图 8 Dbcommservice 服务

3）再在同网段下的任意一台主机中（IP：192.168.1.188）打开 DbCommService 文件夹。

4）打开 DbCommServiceTest_c_sharp 应用程序。

5）然后打开力控软件将 IP 改为 DbCommServicetest 所加载的数据库所在主机的 IP 地址，端口号为 2006，然后点击连接实时数据库。

图 9 DbCommServicetest 参数设定

5）打开力控 V7.2 并直接运行 OPC 接口工程文件。

6）然后打开 3D 模拟软件，输入力控端主机 IP 地址:192.168.1.188 和端口号：2006。

图 9 连接 3D 仿真软件

7）然后点击开始连接，3D 模拟软件成功连上 SCADA 系统。

图 10 虚拟仿真系统连接数据库成功

8）通过更改 DbCommService 目录下的 config 文件的 ip 地址可以使得力控数据库端与服务端相连。

2-7 实验教学方法（举例说明采用的教学方法的使用目的、实施过程与实施效果）

1) 采用的教学方法的使用目的

电力系统面临严峻的网络攻击风险，伊朗核电站的震网 Stuxnet 病毒导致离心机故障，乌克兰电力系统的 BlackEnergy 病毒对变电站系统攻击，导致大面积停电事故。2 南美洲多国发生大停电事故，美大停电事故被怀疑是网络攻击导致。我国电力 SCADA 系统面临巨大的网络攻击风险，但是无法对真实变电站发生攻击测试，因此需要建立模拟环境，连接网络，了解网络攻击对变电站系统发生的影响。

（1）了解变电站的的实物结构；

（2）掌握变电站 SCADA 监控室的操作，了解变电站 SCADA 系统的的操作过程；

（3）掌握变电站系统攻击的核心原理，通过网络攻击手段，获得变电站 SCADA 系统上位机的控制权，或者通过截获或者篡改变电站的通信数据，影响变电站的异常动作，从而破坏变电站的正常运行，引发变电站事故。

（4）掌握针对该种类型攻击的防御措施，促进学生对变电站攻击手段的理解，提高防御攻击的技能。

2) 实施过程

根据 4 个试验目的，制定了 10 个试验步骤，每个步骤的估计时长和分数与评判标准如下：

表 1：实施步骤评判标准

步骤序号	步骤名称	估计用时（分钟）	评判分数	成绩类型
1	打开虚拟仿真实验平台	1	1	□操作成绩
2	了解变电站 SCADA 系统的部署	4	2	□操作成绩
3	了解变电站 SCADA 系统的部署--110KV 变电站组成工作原理	5	2	□操作成绩
4	了解变电站 SCADA 系统的部署--变电 SCADA 系统部署	5	5	□操作成绩
5	了解变电站 SCADA 监控与控制	5	5	□操作成绩
6	掌握变电站 SCADA 虚拟攻防--模拟机数据	5	5	□实验报告
7	掌握变电站虚拟攻防连接 SCADA 系统	5	5	□实验报告
8	掌握变电站 SCADA 虚拟攻防--在线数据	20	25	□实验报告
9	掌握网络攻击与防御	30	40	□实验报告
10	实现变电站 SCADA 虚拟攻防攻击效果展示	10	10	□教师评价报告

3) 实施效果

采用虚拟仿真的试验教学，让学生快速了解了变电站的 SCADA 的结构，掌握变电站 SCADA 监控室的操作，了解变电站 SCADA 系统的的操作过程；掌握变电站系统攻击的核心原理，通过网络攻击手段，获得变电站 SCADA 系统上位机的控制权，或者通过截获或者篡改变电站的通信数据，影响变电站的异常动作，从而破坏变电站的正常运行，引发变电站事故。掌握针对该种类型攻击的防御措施，促进学生对变电站攻击手段的理解，提高防御攻击的技能。达到了教学目的。

该系统先后对信息安全专业的《工业控制系统安全》4 个班级，2 届学生，工业信息安全竞赛团队培养，系统支撑了 2021 工业信息安全技能大赛，并且在 2021 年 2021 年工业互联网安全大赛上海区选拔赛学生组获得一等奖和二等奖。

2-8 实验方法与步骤要求（学生交互性操作步骤应不少于 10 步）

1）实验方法描述：

（1）了解变电站的的实物结构，包括：110KV 变电站组织工作原理（主变压器，10KV 高压区，110KV 设备区），变电站 SCADA 系统的部署两大部分（变压器，隔离开关，电压互感器，电流互感器，六氟化硫隔离开关，避雷器，母线排）

（2）掌握变电站 SCADA 监控室的操作（变电站巡检报告，了解变电站安全的检测点），了解变电站 SCADA 系统的的操作过程（分类信息：110KV 接线图，1 号主变，2 号主变，开关状态）；

（3）掌握变电站系统攻击的核心原理，通过多种网络攻击手段，获得变电站 SCADA 系统上位机的控制权，或者通过截获或者篡改变电站的通信数据，影响变电站的异常动作，从而破坏变电站的正常运行，引发变电站事故，查看变电站的虚拟仿真的刀闸是否打开。

（4）掌握针对该种类型攻击的防御措施，监控网络攻击是否能够导致变电站刀闸打开，提高防御攻击的技能。

2）学生交互性操作步骤说明：

(1)打开虚拟仿真实验平台

http://pt.thingeasy.cn/experiment/resource/751.html

进入电力 SCADA 系统网络攻击虚拟仿真系统

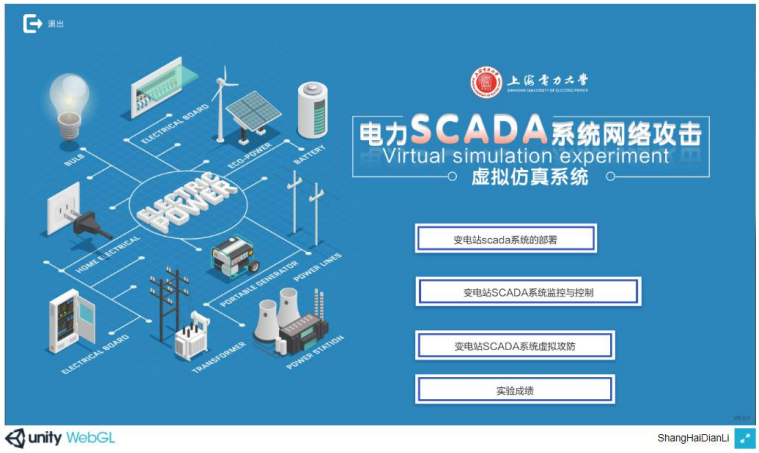

图 11. 电力 SCADA 系统网络攻击虚拟仿真系统

(2)学习变电站 SCADA 系统的部署

在变电站 SCADA 系统的部署的菜单下面有两个子菜单（110KV 变电站组成工作原理，变电 SCADA 系统部署）

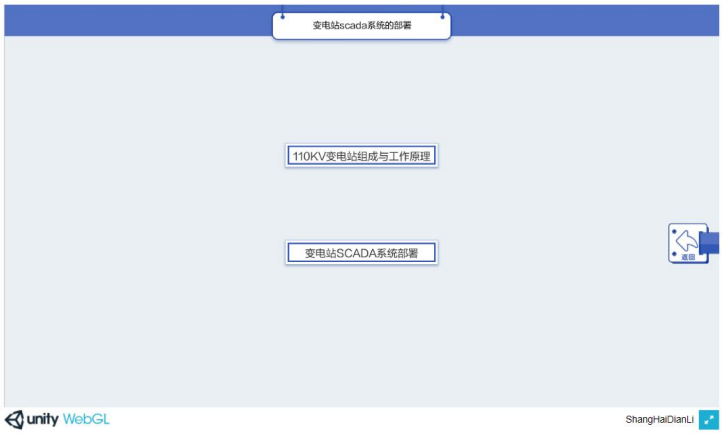

图 12. 变电站 SCADA 系统的部署的二级子菜单

（3）了解变电站 SCADA 系统的部署--110KV 变电站组成工作原理

110KV 变电站组织工作原理（主变压器，110KV 设备区，10KV 高压区）如图 13 所示。

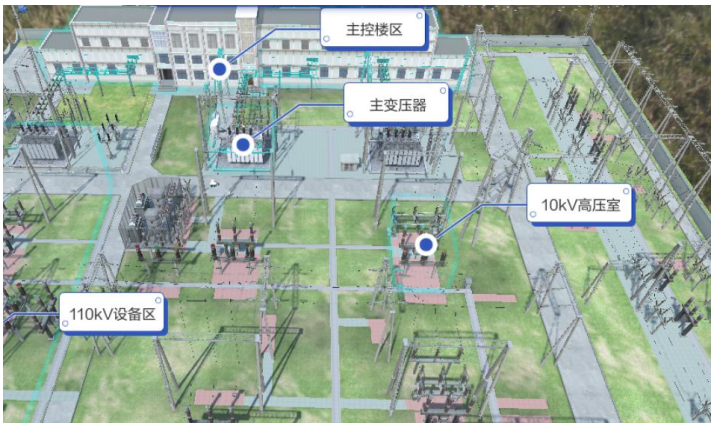

图 13. 变电站系统鸟瞰图

（4）了解站 SCADA 系统的部署--变电 SCADA 系统部署

变电站 SCADA 系统的部署两大部分（变压器，隔离开关，电压互感器，电流互感器，六氟化硫隔离开关，避雷器，母线排），如图 14 所示。

图 14. 变电站系统中变压器的巡检仿真

（5）了解变电站 SCADA 监控与控制

巡检结束后，到变电站监控室填写巡检报告，包括变压器，隔离开关，断路器的巡检结果。如图 15 所示：

图 15. 变电站监控设备的状态监控

点击监控室的监控，查看当前状态信息，记录到工作巡检报告。如图 16 所示

图 16. 变电站监控设备的状态信息巡检

根据巡检结果，输入到巡检报告中，如图 17 所示：

图 17. 变电站监控室填写巡检报告

（6）掌握变电站 SCADA 虚拟攻防--模拟机数据

点击进入变电站 SCADA 虚拟攻防--模拟机数据，如图 18 所示：

图 18. 变电站 SCADA 虚拟攻防--模拟机数据

系统会弹出 IP 地址和端口地址输入内容，如图 18 所示，

图 18. 变电站 SCADA 虚拟攻防的 IP 地址与端口号

（7）掌握变电站虚拟攻防连接 SCADA 系统

通过多种网络攻击手段，获得变电站 SCADA 系统上位机的控制权，因此**变电站虚拟仿真系统提供了与变电站 SCADA 系统软件的网络接口**然后点击开始连接，3D 模拟软件成功连上 SCADA 系统。

图 19 虚拟仿真系统连接数据库成功

（8）掌握变电站 SCADA 虚拟攻防--在线数据了解

操作变电站监控系统，查看主站接线图，分类信息：110KV 接线图，1 号主变，2 号主变，开关状态，如图 20 所示：

图 20. 变电站 SCADA 系统操作仿真

这种变电站 SCADA 系统的操作是在对变电站巡检之后，对整个变电站系统有了感性认识，更加容易理解主变压器，隔离开关，数据传输的过程，对于信息安全专业的学生，在没有电气工程相关知识的背景下，快速理解了变电站通信的过程原理，提高了掌握知识的效率。

（9）掌握网络攻击与防御

提供与了变电站 SCADA 系统的 IP 链接，实现了虚拟系统可以采集网络系统中的数据，让仿真系统可以根据网络参数的改变，转变系统状态信息和控制命令，实现刀闸的开启与闭合。

学生根据网络攻击工具，采取多种攻防手段对网络扫描，启动刀闸，改变状态，通过漏洞扫描，渗透测试、中间人攻击，漏洞利用等方式获得变电站系统的上位机的控制权，从而破坏变电站的正常运行。或者通过截获或者篡改变电站的通信数据，影响变电站的异常动作，引发变电站事故。主要的攻击手段如下表 1 所示：

表 1. 变电站 SCADA 系统的网络攻击

序号	类型	内容
1	网络扫描	1）扫描系统中所有的设备 IP 地址
		2）系统 Ip 地址开放的端口
2	数据修改	1）攻击电脑篡改变频器启停数据
		2）攻击电脑篡改刀闸状态信息
3	注入攻击	1）攻击电脑篡改电压
		2）攻击电脑篡改电流信息
4	缓冲区溢出攻击	1）对目标 kingview 主机的攻击

5	口令破解	1）取目标主机 Kingview 的管理员权限
6	拒绝服务攻击	1）采用 DDoS 攻击网络连接

针对网络攻击，可以采用多种防御方法进行防御，主要采用的技术手段包括 VLAN 网络分区，访问控制，SnortIDS，数据篡改攻击检测，控制命令攻击检测等，如表 2 所示：

表 2. 变电站 SCADA 系统的防御措施

序号	主要内容	主要内容
1	VLAN 网络分区	1) 试验箱系统与变频器系统划分一个网段
		2) 连接交流接触器，电灯一个网段
		3) 两个网段实现 VLAN
2	访问控制	1) 访问控制策略
		2) 防御未授权攻击
3	Snort IDS	1) 启动 Snort
		2）设置 Snort 规则
		1）能够检测到攻击行为
4	数字篡改攻击检测	1）电压数字篡改检测
		2）电流数字篡改检测
5	控制命令攻击检测	1）刀闸闭合检测
		2）刀闸打开

学生在做试验过程中，采用红蓝战队的形式，红队防御，蓝队攻击，对抗性非常强，激发了学生的兴趣。并且也展示了变电站 SCADA 系统的网络攻击效果。为工业信息安全技能训练提供了靶场，培养了技能型人才。

（10）实现变电站 SCADA 虚拟攻防攻击效果展示

电站系统攻击的核心原理，通过多种网络攻击手段，获得变电站 SCADA 系统上位机的控制权，因此**变电站虚拟仿真系统提供了与变电站 SCADA 系统软件的网络接口**，虚拟仿真系统从电力 SCADA 系统中读取数据，刀闸根据状态和远程控制命令，可以启动关闭和开启状态如图 21 所示：

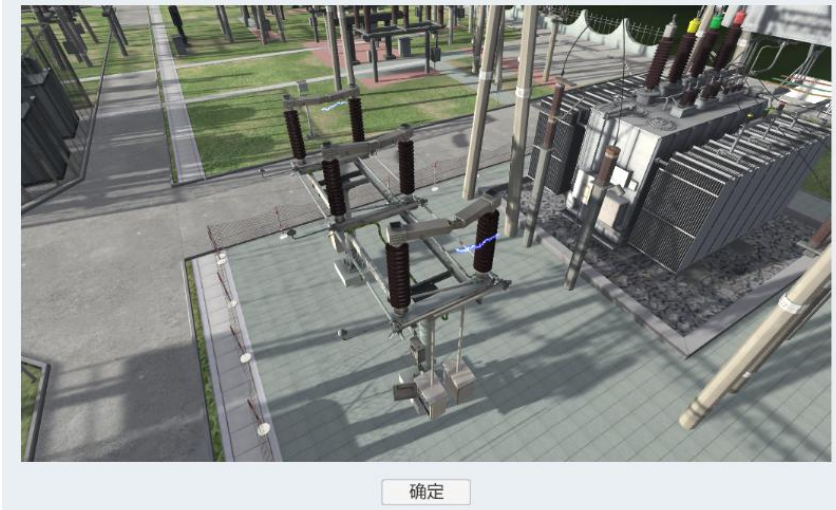

图 21. 变电站刀闸根据 SCADA 控制命令合上刀闸

或者通过截获或者篡改变电站的通信数据，影响变电站的异常动作，从而破坏变电站的正常运行，引发变电站事故，查看变电站的虚拟仿真的刀闸是否打开。

2-9 实验结果与结论要求

（1） 是否记录每步实验结果：☑是 ☐否

（2） 实验结果与结论要求：☑实验报告 ☐心得体会 其他

（3） 其他描述：

2-9 考核要求

将**实验预习、实验操作、实验结果、实验报告**“四位一体”全面考核和评价学生的学习成效。具体考核要求、评分细则和比例见表 1。

表 1 虚拟仿真实验考核要求以及评分细则表

考核要求	考核内容	评分细则
实验预习（15%）	预习考核（网上提交）	10
	口试（翻转课堂抽查提问）	5
实验操作（40%）	实验步骤是否清楚，数据记录是否准确	10
	仪器的操作方法是否正确、规范	20
	对实验现象的观察是否精心	10
实验结果（15%）	数据分析、处理是否正确	15
实验报告（30%）	实验目的、原理、实验操作步骤、实验数据记录与处理、实验结果和结论、注意事项、对实验的评价和建议等是否完整	20
	对实验结果的分析、讨论是否充分	10
总分（100%）		100

2-10 面向学生要求

（1） 专业与年级要求

例子：本实验项目主要面向信息安全专业，网络工程专业，计算机专业的学大四学生，要求学过计算机，信息安全，工业控制相关知识

（2） 基本知识和能力要求等

要求掌握 变电站系统攻击的核心原理就是要了解变电站二次系统的通信过程，电力二次系统的安全防护措施，通过网络攻击手段，利用已知漏洞或者未知漏洞，采用多种工具，多种攻击策略，获得变电站系统的上位机的控制权，从而破坏变电站的正常运行。或者通过截获或者篡改变电站的通信数据，影响变电站的异常动作，引发变电站事故。

2-12 实验项目应用及共享情况

（1） 本校上线时间 ：

（2） 已服务过的本校学生人数：

（3） 是否纳入到教学计划： ☑是 ☐否

(勾选“是”，请附所属课程教学大纲）

（4） 是否面向社会提供服务：☑是 ☐否

（5） 社会开放时间 ： ，已服务人数:

3. 实验教学项目相关网络及安全要求描述

3-1 有效链接网址 http://pt.thingeasy.cn/experiment/detail/751.html
3-2 网络条件要求 （1）说明客户端到服务器的带宽要求（需提供测试带宽服务） 需要 100M 以上带宽 （2）说明能够支持的同时在线人数（需提供在线排队提示服务） 最大能够提供 150 人同时在线访问
3-3 用户操作系统要求（如 Windows、Unix、IOS、Android 等） （1）计算机操作系统和版本要求：windows （2）其他计算终端操作系统和版本要求:windows （3）支持移动端：☑是 ☐否
3-4 用户非操作系统软件配置要求（如浏览器、特定软件等） (1) 需要特定插件 ☐是 ☑否 （勾选“是”，请填写）插件名称 插件容量 下载链接 （2）其他计算终端非操作系统软件配置要求（需说明是否可提供相关软件下载服务）
3-5 用户硬件配置要求（如主频、内存、显存、存储容量等） （1）计算机硬件配置要求 Windows 10, CPU i5 以上，8G 内存以上，最好 16G 内存 （2）其他计算终端硬件配置要求
3-6 用户特殊外置硬件要求（如可穿戴设备等） （1）计算机特殊外置硬件要求 （2）其他计算终端特殊外置硬件要求
3-7 网络安全 （1） 项目系统是否完成国家信息安全等级保护 ☐是 ☑否 （勾选“是”，请填写） 级

4. 实验教学项目技术架构及主要研发技术

<table>
<tr><th colspan="2">指标</th><th>内容</th></tr>
<tr><td colspan="2">系统架构图及简要说明</td><td></td></tr>
<tr><td rowspan="4">实验教学项目</td><td>开发技术</td><td>☐VR ☐AR ☐MR ☑3D 仿真 ☐二维动画
☐HTML5
其他____</td></tr>
<tr><td>开发工具</td><td>☑Unity3D ☐3D Studio Max
☐Maya☐ZBrush ☐ SketchUp
☐Adobe Flash☐Unreal Development Kit
☐Animate CC☐Blender ☐Visual Studio
☐其他____</td></tr>
<tr><td>运行环境</td><td>服务器
CPU _16_核、内存_128__GB、磁盘_1T__GB、
显存_16_ GB、GPU 型号__i5__
操作系统
☑Windows Server ☐Linux ☐其他 具体版本_____
数据库
☐Mysql ☐SQL Server ☐Oracle
其他____
备注说明___（需要其他硬件设备或服务器数量多于 1 台时请说明）_____</td></tr>
<tr><td>项目品质（如：单场景模型总面数、贴图分辨率、每帧渲染次数、动作反馈时间、显示刷新率、分辨率等）</td><td></td></tr>
</table>

5. 实验教学项目特色

（体现虚拟仿真实验教学项目建设的必要性及先进性、教学方式方法、评价体系及对传统教学的延伸与拓展等方面的特色情况介绍。）

（1）实验方案设计思路：制定一个虚实结合的仿真系统，可以支持网络攻防，攻击可以改变 3D 虚拟系统。

（2）教学方法创新：3D 虚拟仿真系统通过网络与数据库的链接，实现了变电站 SCADA 系统的网络攻防。

（3）评价体系创新：攻防的可视化展示

（4）对传统教学的延伸与拓展:虚拟与网络的链接

6. 实验教学项目持续建设服务计划

（本实验教学项目今后 5 年继续向高校和社会开放服务计划及预计服务人数）

（1）项目持续建设与服务计划：

继续完善虚拟化仿真系统，设计虚拟化组件，数字双胞胎，可以定制提供设备参数与网络的实对接，实现更大规模的在线数据仿真。

（2）面向高校的教学推广应用计划：

通过交流访问的机会，计划在上海交通大学网络空间安全学院合作，

（3）面向社会的推广应用计划：

支撑了 2021 工业信息安全技能大赛上海站的比赛，取得圆满成功，得到了国家工业信息发展研究中心的肯定。

7. 知识产权

软件著作权登记情况	
软件著作权登记情况	☐已登记　☐未登记
完成软件著作权登记的，需填写以下内容	
软件名称	

是否与项目名称一致	□是　　□否
著作权人	
权利范围	
登记号	

8. 诚信承诺

本人承诺：所申报的实验教学设计具有原创性，项目所属学校对本实验项目内容（包括但不限于实验软件、操作系统、教学视频、教学课件、辅助参考资料、实验操作手册、实验案例、测验试题、实验报告、答疑、网页宣传图片文字等组成本实验项目的一切资源）享有著作权，保证所申报的项目或其任何一部分均不会侵犯任何第三方的合法权益。

本人已认真填写、检查申报材料，保证内容真实、准确、有效。

实验教学项目负责人（签字）：

年　　月　　日

9. 附件材料清单

1. 政治审查意见（必须提供）

（本校党委须对项目团队成员情况进行审查，并对项目内容的政治导向进行把关，确保项目正确的政治方向、价值取向。须由学校党委盖章。无统一格式要求。）

2. 校外评价意见（可选提供）

（评价意见作为项目有关学术水平、项目质量、应用效果等某一方面的佐证性材料或补充材料，可由项目应用高校或社会应用机构等出具。评价意见须经相关单位盖章，以 1 份为宜，不得超过 2 份。无统一格式要求。）

10 申报学校承诺意见

本学校已按照申报要求对申报的虚拟仿真实验教学项目在校内进行公示，并审核实验教学项目的内容符合申报要求和注意事项、符合相关法律法规和教学纪律要求等。经评审评价，现择优申报。

本虚拟仿真实验教学项目如果被认定为“国家虚拟仿真实验教学项目”，学校将严格贯彻《教育部高等教育司关于加强国家虚拟仿真实验教学项目持续服务和管理有关工作的通知》（教高司函〔2018〕56 号）的要求，承诺将监督和保障该实验教学项目面向高校和社会开放，并提供教学服务不少于 5 年，支持和监督教学服务团队对实验教学项目进行持续改进完善和服务。

（其他需要说明的意见。）

主管校领导（签字）：

（学校公章）

年　　月　　日