烽台科技 FENGTAI TECHNOLOGY

桂林电子科技大学

工控 CTF 技能挑战赛

一、赛事简介

以提高工业信息安全防护水平，培养专业技术人才为目标；

桂林电子科技大学致力于打造集思广益的技术交流平台为广大学员提供展示精湛技能、相互切磋技艺的平台；

以赛促教、以赛促培、以赛促评、以赛促建，进一步壮大工业网络安全技术技能队伍，推动经济社会发展。

二、组织架构

2.1 组织机构

（一）指导单位

桂林电子科技大学-计算机与信息安全学院

（二）主办单位

桂林电子科技大学-计算机与信息安全学院、烽台科技（北京）有限公司

（三）承办单位

桂林电子科技大学-计算机与信息安全学院、烽台科技（北京）有限公司

（四）技术支持单位

烽台科技（北京）有限公司

2.2 赛事组织

（一）指导委员会

大赛设立指导委员会，拟邀请梁海老师，姚罡老师等，指导委员会负责指导

赛事活动，审议赛规赛制等。

（二）裁判组

裁判组设组长 1 名，推荐桂林电子科技大学姚罡老师担任。成员推荐烽台科技（北京）有限公司王龑、安成。主要负责大赛赛题研判、规则确认、比赛结果裁定等工作。

（三）协调组

协调组负责大赛全面组织协调工作。主要负责确定大赛定位、办赛原则和组织形式；审定大赛整体方案和实施方案；确定大赛顶层设计制度安排；指导赛事活动组织；审定大赛最终成绩。

协调组由桂林电子科技大学梁海老师、吴祥欢、左浩帆、何首其、于林杰、吴晓娜同学成员组成。

（四）秘书处

秘书处是大赛常设机构，负责大赛组委会日常事务，代表组委会发布正式通知。秘书处设在桂林电子科技大学“工控安全联合实验室”。

三、竞赛模式

3.1 竞赛介绍

本次桂林电子科技大学 工控CTF 技能挑战赛 分为初赛（体验赛）、复赛（晋级赛）、决赛（挑战赛）三个阶段，其中初赛、复赛为线上赛，决赛为线下赛。

3.2 赛程安排

本次活动采用线上报名+线下确认的方式进行参赛。

3.2.1 大赛报名

报名时间	2022.3.30 08:00——2022.4.6 17:00 止
报名方式及渠道	线上报名——官方获取挑战赛邀请函
线下报名确认时间	2022.4.7-4.8 17:00-20:00/天
确认地址	工控安全联合实验室（花江校区花江慧谷四创中心基地 2 栋 104 室）
确认内容	1、核对姓名、专业、电话报名信息 2、提交参赛选手的艺名（彰显个性，积极向上，不得包含不当词汇） 3、提交本人身份证号码（作为唯一认证信息） 4、提交个人简历一份（电子版） 5、组织建群 6、以上信息确认无误后，领取参赛须知和赛程安排

3.2.2 线上初赛

初赛（体验赛）时间	2022.4.9（周六） 8:00-12:00
比赛方式	线上赛，采用统一技术平台进行接入
竞赛题型	初级赛题 3 道、中级赛题 5 道、高级赛题 2 道
竞赛内容	包含但不限于：工控协议分析、工控梯形图、工控软件编程、工控固件分析、工控软件逆向及工控网络渗透测试等。
竞赛结果	初赛成绩排名以分数为主，相同分数以提交答案时间作为排名依据，最终取前 50 名进入复赛。

3.2.3 线上复赛

复赛（晋级赛）时间	2022.4.9（周六） 14:00-18:00
比赛方式	线上赛，采用统一技术平台进行接入
竞赛题型	初级赛题 3 道、中级赛题 5 道、高级赛题 2 道
竞赛内容	包含但不限于：工控协议分析、工控梯形图、工控软件编程、工控固件分析、工控软件逆向及工控网络渗透测试等。
竞赛结果	初赛成绩排名以分数为主，相同分数以提交答案时间作为排名依据，最终取前 20 名进入决赛。

3.2.4 线下决赛

决赛（挑战赛）时间	2022.4.10（周日） 10:00-15:00【08:30-16:30 为整体时间】
比赛方式	线下赛，统一技术平台进行接入 工控安全联合实验室（花江校区花江慧谷四创中心基地 2 栋 104 室）
竞赛内容	赛选手需通过现场提供的网络连接到工控网络环境中，通过发现网站门户系统漏洞、SCADA 系统漏洞或上位机漏洞，抢占关键通信节点，发现控制系统风险隐患，从而进一步攻击 PLC 控制器，实现场景攻击点效果。
竞赛结果	决赛成绩排名以分数为主，相同分数以提交答案时间作为排名依据。 一等奖 2 名，二等奖 3 名，三等奖 5 名

四、竞赛说明

4.1 命题规范

按照工业互联网工程技术人员相关技术应用和职业技能要求，把握产业发展、技术趋势和行业需求；以强化职业技能和技术应用要求，考察工业互联网安全的测评、评估、运维、保障等核心技术技能等为依据作为命题标准。

竞赛内容以企业生产实际环境、工业互联网安全技术应用发展为主，重点考察参赛选手在工业互联网网络、设备、控制、平台、应用、数据等方面的安全测试、评估、运维和保障的能力。

4.2 规则说明

4.2.1 线上初赛规则

挑战赛——初赛（体验赛）题目采用动态积分方式。每道赛题初始积分为：初级难度 50 积分、中级难度 100 积分、高级难度 150 积分，在比赛期间内提交正确的 Flag 及可得分。每道题目最先答对的前三名，会分别得到该题目总分的 30%、20%、10%的分数加成。

参赛选手需在比赛结束前需通过赛事平台上传《工控/CTF 挑战赛（体验赛）解题报告》，比赛结束后由裁判组根据各参赛选手上传的报告进行分值评定，最

终经裁判组逐一确认后，方可记录各队伍比赛成绩，未上传解题报告者则成绩作废。

4.2.2 线上复赛规则

挑战赛——复赛（晋级赛）题目采用动态积分方式。每道赛题初始积分为：初级难度 100 积分、中级难度 150 积分、高级难度 300 积分，在比赛期间内提交正确的 Flag 及可得分。每道题目最先答对的前三名，会分别得到该题目总分的 30%、20%、10%的分数加成。

参赛选手需在比赛结束前需通过赛事平台上传《工控/CTF 挑战赛（晋级赛）解题报告》，比赛结束后由裁判组根据各参赛选手上传的报告进行分值评定，最终经裁判组逐一确认后，方可记录各队伍比赛成绩，未上传解题报告者则成绩作废。

4.2.3 线下决赛规则

挑战赛——决赛计分方式分为三块：flag 分、攻击效果分、writeup 分等。

- **Flag 分**

(1) 每套仿真业务场景设置了 3 个场景内置 flag，需参赛选手采用相应的技术手段才能获取到内置 flag（每个 flag 为 100 分）。

(2) 参赛选手拿到上述 flag 得分点后方可进入仿真业务场景，参赛选手进入仿真业务场景需在 SCADA 界面中植入参赛选手的名称（成功植入不得分，名称可被删除）。

- **攻击效果分**

参赛选手攻破场景上位机系统后在 SCADA 画面成功植入参赛选手的名称且成功攻击该场景触发效果，则攻击选手加 200 分。

- **Writeup 分**

(1) writeup 分值根据参赛选手上传内容进行评定。

(2) writeup 分值分为三种评分等级：

一般质量=题目分值*30%（题目分值即当前攻击点分值）。

中等质量=题目分值*60%（题目分值即当前攻击点分值）。

高等质量=题目分值*90%（题目分值即当前攻击点分值）。

(3) writeup 质量评定标准：

一般质量=思路清晰、可顺利解答。

中等质量=思路清晰、采用脚本、复现难度、顺利解答。

高等质量=思路清晰、采用脚本、复现难度、多种思路、可顺利解答。

比赛结束时将各参赛选手 flag 提交分数、攻击效果分值、writeup 分值进行累加，作为各参赛选手的最终成绩。

4.3 注意事项

(1) 比赛过程中参赛选手需使用合法的用户名密码登录比赛平台，若发现人与账号不匹配账号外借等情况，视情况严重程度，将进行警告，严重者则取消参赛资格等处罚措施。

(2) 参赛选手应自觉维护赛场秩序，需遵循裁判及工作人员的安排，遵守操作规程，不得违章操作，干扰其他参赛选手比赛等行为，严格遵守比赛规则。如有疑问请举手示意。

(3) 参赛选手须尊重评审专家和工作人员，服从评判和管理。如对比赛平台有疑问，可通过举手寻求工作人员示意请求解答。禁止参赛选手之间相互询问，违者取消比赛资格。

(4) 比赛过程中严禁参赛选手向赛事服务器、参赛选手主机等设施发起任何可能影响比赛正常运行的渗透或恶意操作，视情况严重程度，将进行警告或取消参赛资格等处罚措施。

(5) 比赛期间，禁止参赛选手在互联网上（例如：QQ 群微信技术交流论坛等）发布传播竞赛真题进行求助，若大赛组委会在网络巡检中发现该类情况，则直接取消该选手的参赛资格。

(6) 禁止删除、修改、隐藏、重命名场景内置 flag，一旦发现该情况后，则对参赛选手进行扣分惩罚，每发现一次则扣除 200 积分。

(7) 禁止攻击用户防火墙及网关设备，一旦发现该情况，则对参赛选手进行断网惩罚，惩罚时间为 30 分钟。

(8) 参赛选手在比赛期间需遵循专家及工作人员的安排，遵守竞赛纪律，切勿喧

哗，如有疑问请举手示意，不得对他人进行语言或人身攻击。禁止参赛选手之间相互询问，违者取消比赛资格。

(9) 违反上述规定者，大赛组委会将视情况给予口头警告、断网、扣分、取消参赛资格等处罚。

五、竞赛筹备

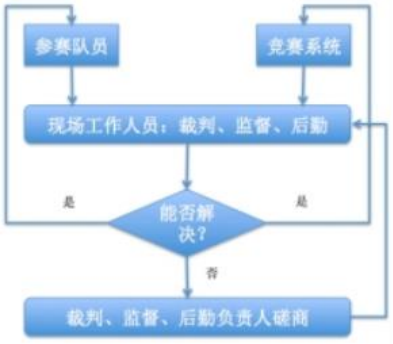
5.1 赛事流程设定

工控/CTF 挑战赛		
日期	时间	内容
4 月 9 日（周六）	08:00-12:00	工控/CTF 挑战赛—初赛（体验赛）
	12:30-13:00	晋级名单公布
	14:00-16:00	工控/CTF 挑战赛—复赛（晋级赛）
	16:30-17:00	决赛名单公布
4 月 10 日（周日）	08:30-09:30	工控安全联合实验室现场签到
	09:30-10:00	梁海老师致词，宣读比赛规则
	10:00-15:00	工控/CTF 挑战赛—决赛
		12:00-13:00 用餐时间（比赛不间断）
	15:30-16:30	成绩公布、颁奖

5.2 现场应急流程

现场的问题源主要来自于两个方面：参赛人员和竞赛系统。无论遇到什么问题（涉及到竞赛内容以外），现场工作人员：裁判、监督、后勤应第一时间获取问题进行解答，如果无法解答，需要反馈给各自单位的负责人（组委会成员）进行紧急磋商，解决问题。

应急响应的流程图如下：



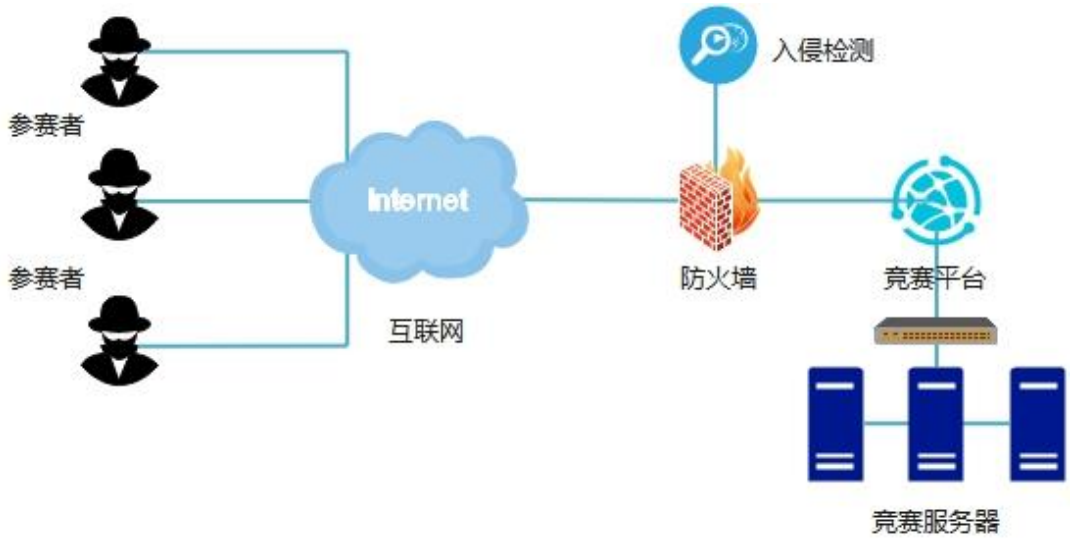
5.3 竞赛结果

活动后为获奖选手颁发获奖证书及奖励				
序号	奖项	数量	获奖证书	奖励
1	一等奖	2	各 1 个	各 1000 元
2	二等奖	3	各 1 个	各 500 元
3	三等奖	5	各 1 个	各 300 元

六、竞赛实施

6.1 线上初、复赛

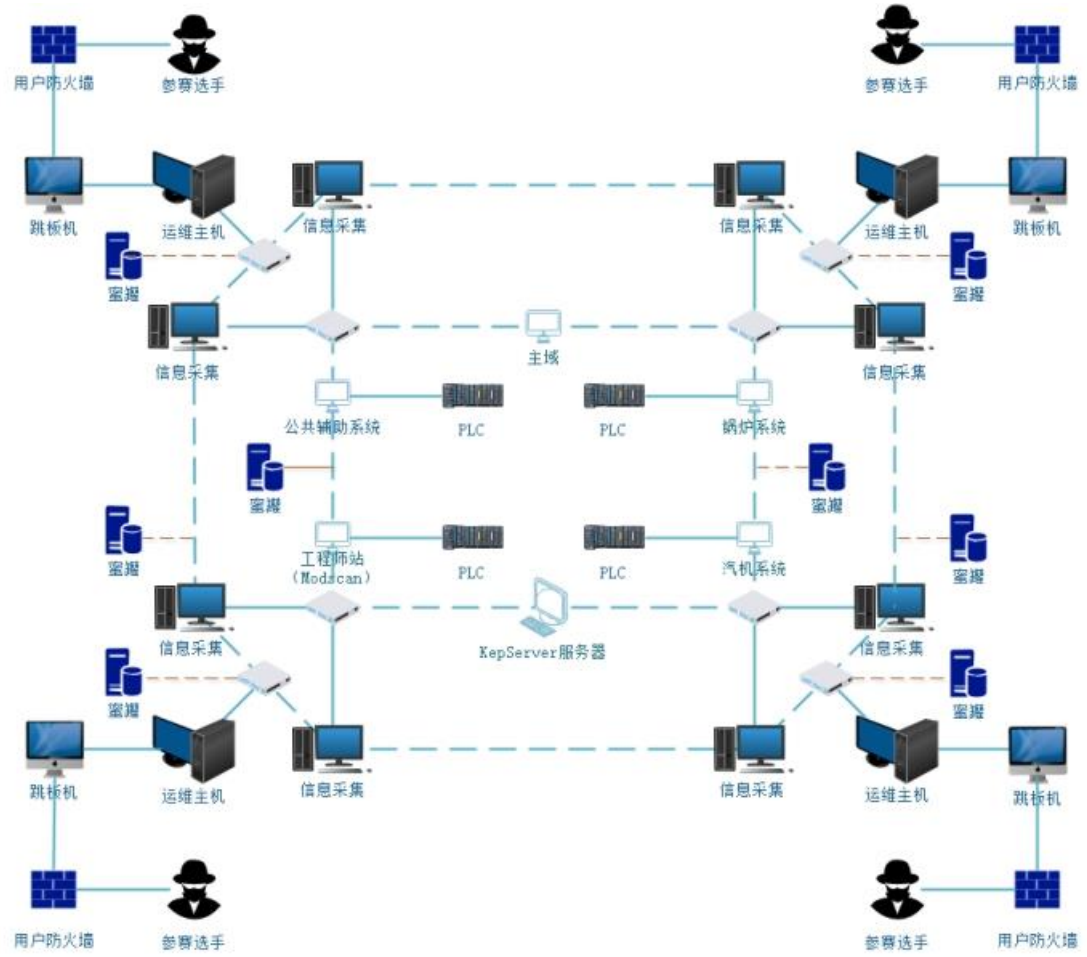
参赛选手通过互联网接入比赛平台，采用线上答题的方式进行。比赛管理系统完成比赛过程中各个环节的管理，包括赛题开放管理、FLAG 提交及正确性判断、得分管理、比赛进程展示等。赛事期间赛事保障人员监控比赛平台运行状况，及时处理突发情况。



线上赛用户接入图（示意）

6.2 线下决赛

用户环境的网络拓扑图如下，每个参赛队伍均在独立的 VLAN 中进行访问操作（具体拓扑根据现场实际环境进行定制设计）。



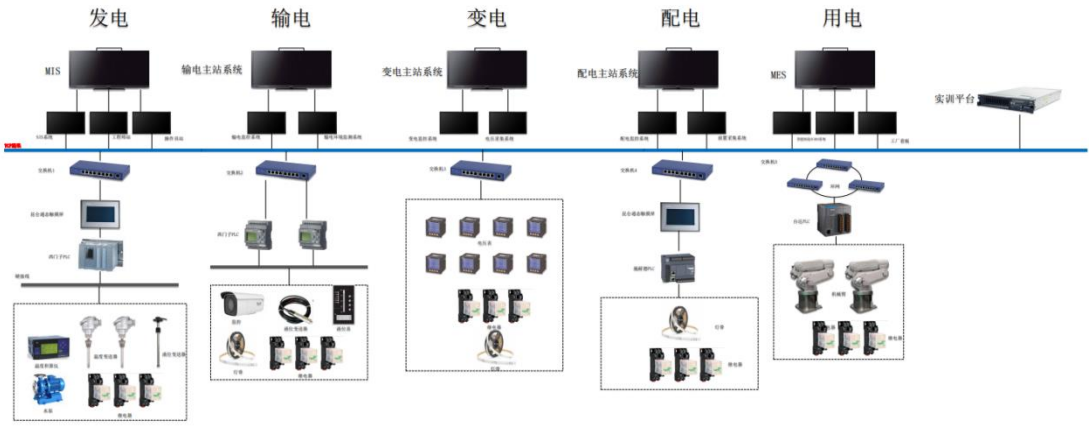
线下赛用户接入图（示意）

七、附录

7.1 场景介绍

本次挑战赛竞赛场景题目依托桂林电子科技大学“工控安全联合实验室”的发电、输电、变电、配电、用电等电力行业全流程的仿真验证场景开展。场景包含但不限于 MAC1100、Mic800、S7-200 SMART、和利时 LE、三菱 FX5U-32M、S7-1200、浙大中控 GCU331、台达 AS、步科 K204ET-16DT、ABB PM862K02、西门子 AS 410

SMART、 AB Controllogix、施耐德 M340、S7-300、西门子 1500、西门子 PLC300、三菱 FX31、OPC、KepServer、等软硬件设备。



（一）发电场景介绍

此场景模拟火力发电工艺，系统由火力发电工程实物装置，仪表、机泵，PLC 控制器及工作站组成。实物装置设备的尺寸将真实火电工程设备按比例缩小的总原则设计，仪表、手操阀及机泵根据安装环境及电气功能要求进行选择，采集装置中压力、温度、液位等实际状 态下数值，现场阀门、泵的操作状态信号上传至控制器，并接收由控制器发送的控制指令。

（二）输电场景

电网输配电系统是“发、输、变、配、用”五大环节重要组成部分，其作用是分配和汇集作用。输配电系统的稳定和安全是电网输送的关键环节，因此对输配电系统进行监控和安全防护具有十分重要的意义。是电力企业降低运行风险、提高生产率、增加安全经济效益的有效途径之一，控制系统采用在发电系统中常用的西门子系列，上位机采用力控制电力版组态软件，与工艺相结合，实现一个典型的配电控制系统。通过组合继电器的逻辑控制。

（三）变电场景

此场景采用变电站工艺进行仿真，高度还原了变电站控制系统。通过电压变换（220VAC→110VAC→36VAC→10VAC→2VAC），模拟高压变低压全过程，变压后通过配电场景进行分配用电线路，供用户使用。共设计 4 组变压器，模拟 220KV 变电站、110KV 变电站、36KV 变电站、10KV 变电站以及低压变压系统。

（四）配电场景

实验展板由显示器、交换机、指示灯、断路器、三遥信号模拟装置等设备组成。被测设备可置于台面下方的柜体中，并使用安全标识示意。配电接口通过展板背后的配电端子排进行连接，当需接入设备时，可通过预留的接口在设备之间进行切换，便于设备的测试。网络接口则通过背板后面的网络接口排进行连接，并预留一定数量的接口，方便扩展。

（五）用电场景

用电场景采用工厂用电进行模拟，主要以智能制造场景进行展示，模拟汽车焊接工序，将采用两套 6 轴工业级机器人模拟焊接工艺。通过电表对用电系统进行用电计量。

7.2 场景攻击效果

工控/CTF 挑战赛决赛——工控场景攻击效果				
场景	攻击点编号	攻击点	攻击效果	
发电	A-1	攻击 BV102 电动阀，使其停止	锅炉安全阀门出口处有水流出	锅炉液位上升至 80%
	A-2	攻击仿真工艺输水泵 P130，使其停止	/	锅炉液位上升到至 60%
输电	B-1	1#输电线路	输电线路由红变绿，不停闪烁	
	B-2	2#输电线路	PLC 停止工作	
变电	C-1	上位机电压值	电压值显示异常	
	C-2	变电站输电线路	输电线路状态灯由绿变红	
配电	D-1	配电柜遭受攻击	配电柜报警灯异常报警	
	D-2	配用电输电系统遭受攻击	输电杆塔灯光异常	
用电	E-1	攻击机器臂激光焊枪，使机器臂激光灯熄灭	激光指示消失	
	E-2	攻击 SCADA 系统运行画面，篡改控制运行状态，使机械臂停止运行	停止运行	运行指示为停止状态

7.3 决赛场景资源介绍

下图展示的场景都是基于真实业务环境来制作，高度还原日常一线业务中的安全问题及配置策略，将日常业务与竞赛场景结合，实现更加贴近真实环境的网络攻防。

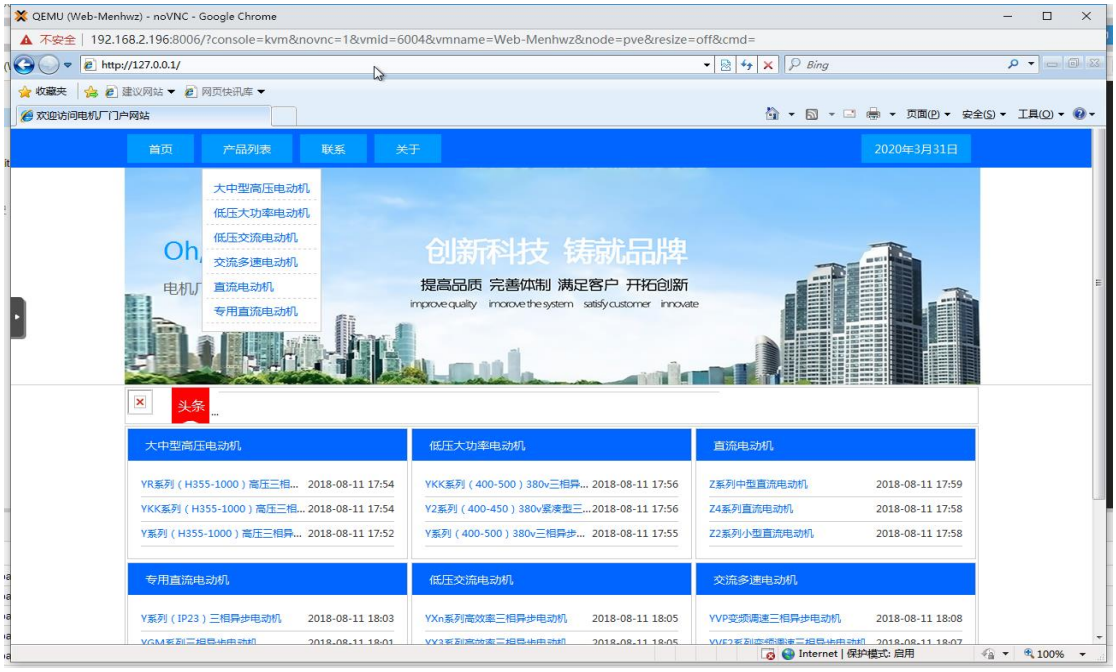


图 1 某工电机厂门户网站（场景）

图 2 某火电厂 SCADA 画面（场景）

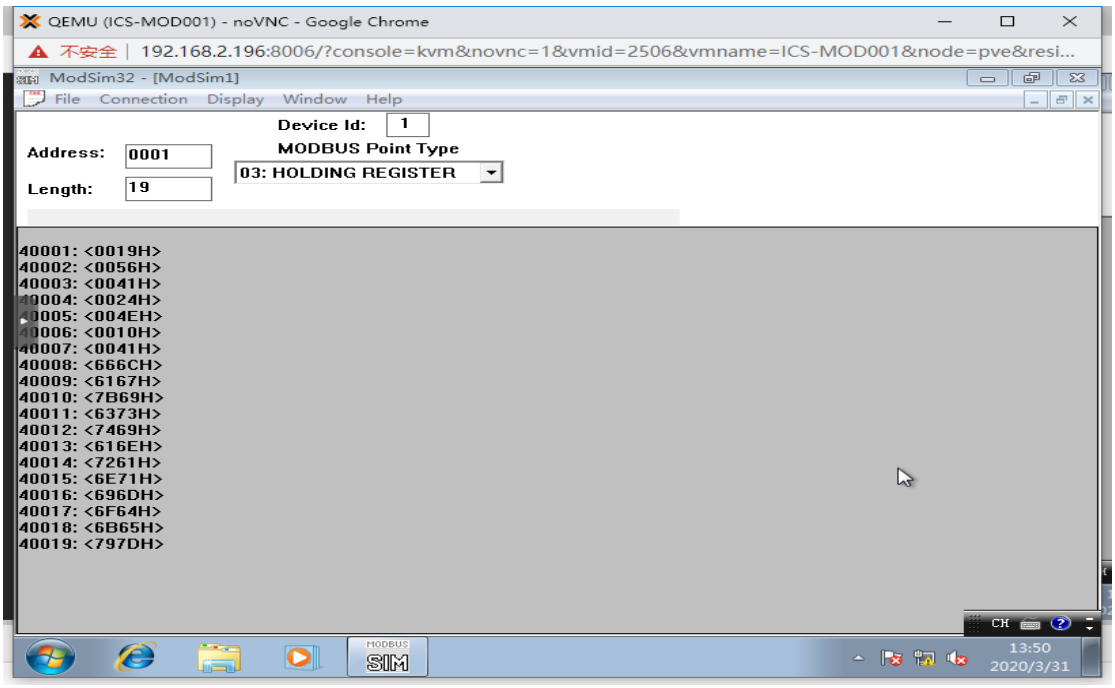

QEMU (ICS-MOD001) - noVNC - Google Chrome
不安全 | 192.168.2.196:8006/?console=kvm&novnc=1&vmid=2506&vmname=ICS-MOD001&node=pve&resi...
ModSim32 - [ModSim1]
File Connection Display Window Help
Device Id: 1
Address: 0001
MODBUS Point Type
Length: 19
03: HOLDING REGISTER
40001: <0019H>
40002: <0056H>
40003: <0041H>
40004: <0024H>
40005: <004EH>
40006: <0010H>
40007: <0041H>
40008: <666CH>
40009: <6167H>
40010: <7B69H>
40011: <6373H>
40012: <7469H>
40013: <616EH>
40014: <7261H>
40015: <6E71H>
40016: <696DH>
40017: <6F64H>
40018: <6B65H>
40019: <797DH>
MODBUS SIM
13:50
2020/3/31

图 3 某仿真 PLC（场景）