附件：

**2018年全国职业院校技能大赛**

**赛项申报书**

赛项名称：工业互联网安全技术与应用

赛项类别：常规赛项■ 行业特色赛项□

赛项组别：中职组□ 高职组■

涉及的专业大类/类：电子信息大类

方案设计专家组组长：

手机号码：

方案申报单位（盖章）：[工业和信息化职业教育教学指导委员会](http://www.baidu.com/link?url=ZPgIpMUfROHyCZHRsjlX1rIq6Tdu0sGkqSECAfGdNrP5pFKOUxEF0QozHgGtpBZYjOPgJ9Uu0HdJQwo9feyqVT4KeTxs3Te-7HXWdlvLCybrZ8RUe_pbrf0t506oM4na)

方案申报负责人：

方案申报单位联络人：

联络人手机号码：

电子邮箱：

通讯地址：

邮政编码：

申报日期：2017年8月28日

**2018年全国职业院校技能大赛**

**赛项申报方案**

**一、赛项名称**

（一）赛项名称

工业互联网安全技术与应用

（二）压题彩照

（三）赛项归属产业类型

信息产业，信息服务业

（四）赛项归属专业大类/类

61 电子信息大类

610119 物联网应用技术

610211 信息安全与管理

**二、赛项申报专家组**

**三、赛项目的**

2015年5月，国务院发布《中国制造2025》文件明确提出促进**工业互联网**、云计算、大数据在企业研发设计、生产制造、经营管理、销售服务等全流程和全产业链的综合集成应用。加快开展**物联网技术**研发和应用示范，培育智能监测、远程诊断管理、全产业链追溯等**工业互联网新应用**。加强智能制造工业控制系统**网络安全**保障能力建设，健全综合保障体系。

当前工业互联网的安全形势非常严峻，2016年，全球发生了多起工业控制领域重大事件，3月，美国纽约鲍曼水坝的一个小型防洪控制系统遭受攻击；8月，卡巴斯基安全实验室揭露了针对工业控制行业的“食尸鬼”网络攻击活动，该攻击主要对中东和其他国家的工业企业发起定向网络入侵；12月，乌克兰电网再一次经历了供电故障，据分析本次故障缘起恶意程序“黑暗势力”的变种。

我国工业控制系统规模巨大，安全漏洞、恶意探测等均给我国工业控制系统带来一定的安全隐患。截至 2016 年年底，CNVD 共收录工业控制漏洞 1036 条，其中2016 年收录173 个，较 2015 年增长 38.4%。工业控制系统主要存在缓冲区溢出、缺乏访问控制机制、弱口令、目录遍历等漏洞风险。同时，通过联网工业控制设备探测和工业控制协议流量监测，2016年 CNCERT/CC 共发现 我国联网工业控制设备2504 个，协议主要涉及 S7Comm、Modbus、SNMP、 EtherNetIP、Fox、FINS等，厂商主要为西门子、罗克韦尔、施耐德、欧姆龙 等。通过对网络流量分析发现，2016 年度 CNCERT/CC 累计监测到联网工业控制设备指纹探测事件 88 万余次，并发现来自境外 60 个国家的 1610 个 IP 地址对我国联网工业控制设备进行指纹探测。

随着物联网技术在工业互联网中的广泛应用，物联网设备安全也深深影响着智能制造工业企业的网络安全保障能力，2016年CNVD收录的IoT设备漏洞1117个，涉及Cisco、Huawei、Google、Moxa等厂商。2016年CNVD收录的IoT设备漏洞类型分别为权限绕过、拒绝服务、信息泄露、跨站、命令执行、缓冲区溢出、SQL注入、弱口令、设计缺陷等漏洞。2016年CNVD公开收录的1117个IoT设备漏洞中，影响设备的类型（以标签定义）包括网络摄像头、路由器、手机设备、防火墙、网关设备、交换机等。其中，网络摄像头、路由器、手机设备漏洞数量位列前三，分别占公开收录漏洞总数的10.1%、9.4%、4.7%。

为此，自去年以来，我国政府就采取了一系列重大举措，加大网络安全和信息化发展的力度。《国务院关于促进信息消费扩大内需的若干意见》强调，加强信息基础设施建设，加快信息产业优化升级，大力丰富信息消费内容，提高信息网络安全保障能力。十八届三中全会《决定》明确提出，要坚持积极利用、科学发展、依法管理、确保安全的方针，加大依法管理网络的力度，完善互联网管理领导体制。

2月27日，中央网络安全和信息化领导小组宣告成立，中共中央总书记、国家主席、中央军委主席习近平亲自担任组长，李克强、刘云山任副组长。此次举措既、表明了网络信息安全目前面临的形势任务复杂和所处地位的重要，也标志着中国已把信息化和网络信息安全列入了国家发展的最高战略方向之一。

针对高职“信息安全与管理”、“物联网应用技术”专业建设和发展的需求，通过引入工业互联网安全技术实际应用场景，该应用场景通过办公网络环境安全、物联网（IOT）设备安全与生产环境安全三个部分全面考察高职学生前沿的知识、技术技能、职业素养和团队协作能力。促进职业院校相关专业课程改革，推动院校、科研院所与企业联合培养符合国家需要的网络安全人才，促进相关专业与产业、职业岗位的对接。

**四、赛项设计原则**

（一）坚持公开、公平、公正；

遵从全国职业院校技能大赛一贯倡导的各项基本原则。

遵循大赛一贯坚持的公开、公正、公平原则、普惠性原则。

赛项的样题、赛题库公开、评分规则尽可能细致并通过规程公开、认真召开免费的赛项说明会详细介绍赛项规程，竞赛组织评判工作严格遵守《全国职业院校技能大赛制度汇编》各项要求。

组织邀请没有购买竞赛设备的参赛队免费集训。

（二）赛项关联职业岗位面广、人才需求量大、职业院校开设专业点多；

学生就业可以面向新一代信息技术产业、智能制造企业的信息安全工程师、网络管理工程师、物联网集成测试工程师等岗位需求，同时可以面向专注于工业互联网提供安全设备与服务的专业厂商。

职业院校广泛开设的计算机网络技术、物联网应用技术、信息安全与管理、计算机应用技术、移动互联应用技术等相关专业都能通过本赛项促进教学，并能促进符合国家智能制造战略发展需要的工业互联网急需高素质技术技能型人才培养。

（三）竞赛内容对应相关职业岗位或岗位群、体现专业核心能力与核心知识、涵盖丰富的专业知识与专业技能点；

信息安全与管理及物联网应用技术专业培养中，前者侧重于网络安全领域，后者侧重于物联网应用领域，物联网安全和工控安全也是网络安全的重要领域，但是在信息安全与管理专业建设中较少涉及，物联网安全对于物联网应用技术毕业生来说也是适应产业发展的必备技能，所以有拓展教学内容的必要。

该赛项聚焦工业互联网领域信息安全，突出考查选手办公网络环境安全、物联网（IOT）设备安全与生产环境安全三个方面的核心技能，同时也考核了信息安全与管理专业及物联网应用技术专业的基础技能，涵盖了上述两个专业的部分专业核心技能点。

竞赛内容涵盖了：渗透场景、防御场景案例、网络攻防基础、物联网应用技术基础；现场问题的分析、处理、团队组织及协作等多方面的专业知识与技能点。

通过本赛项的训练和比赛，选手未来可以胜任的工作岗位有：信息安全员、信息安全工程师、网络管理员、网络管理工程师、物联网集成测试工程师等岗位。

（四）竞赛平台成熟。根据行业特点，赛项选择相对先进、通用性强、社会保有量高的设备与软件。

竞赛平台硬件方面，采用可靠、高性能、高并发、高可用性部署，保障设备可靠、安全、通用。

软件方面，采用设计先进，并基于主流云计算技术提供竞赛支持，展示界面设计人性化并兼具观赏性，便于观众参观与理解。

**“工业互联网安全技术与应用竞赛”平台软件系统的组成：**

1.竞赛管理系统

竞赛管理系统可以设置参赛学员、参赛单位、竞赛管理、试卷管理等功能。竞赛管理可以制定竞赛任务。竞赛管理可以根据演练过程与结果进行成绩的采集、判定与成绩的综合评估。竞赛管理系统能够监控竞赛过程。

2.竞赛展示系统

竞赛展示系统以巨幕的形式向用户展示演练作战的情况，用户可以看到所有的作战队伍的作战情况。在竞赛过程中，态势展示系统必须显示当前时间、距离竞赛结束的时间以及距离当前阶段结束的时间。渗透阶段中，用户能够根据图形化界面，动态的看到每个队伍的答题目标，并能直观的显示每个队伍的答题数量，同时能够看到每个赛题的名称。

3. 竞赛场景设计系统

场景设计系统中，用户可以根据自己的需求，调用已有的靶场靶机生成竞赛网络环境，也可以自己创建属于自己的靶机。竞赛场景设计系统针对所有用户开放靶场接口，用户可以通过接口创建、上传靶机到靶场中，也可以根据已有的靶机复用并修改，生成自己的靶机。通过已有或者新建立的靶机，用户可以生成网络环境，应用到竞赛试题中。

4. 分析评估系统

分析评估系统能够分析每个参赛团队在每个阶段中的实时得分、提交时间、答对与答错的题目数量，并能够以图形化的形式展示整个竞赛的成绩，包括总体排名的柱状图，柱状图中包括每个队伍的每个阶段的得分，包括每个队伍得分时间现状图。团队统计以图形化展示统计，包括图形化展示各个阶段的得分占比，对错的得分占比，整体竞赛的得分走势图.

在2016-2017年期间，该竞赛平台中国信息安全测评中心举办的信息安全铁人三项赛中，曾经过22场近百所院校参赛的赛事的实践检验，成熟可靠。

**五、赛项方案的特色与创新点**

（一）**通用性**。竞赛网络结构设计，基于典型制造业企业网络结构设计，融合办公网络环境、物联网（IOT）设备与生产环境等网络部分。

（二）**引领性**。通过参与本赛项，院校老师了解了工业互联网安全产业发展、岗位需求和知识技能要求。在工信行指委的领导下，赛项设计专家组参与开发工业互联网安全相关课程课程标准。通过赛项教学资源转化计划的实施，从课程、师资、教材、实训等方面促进职业院校相关专业建设。

（三）**科学性**。本赛项成通过产业、企业和院校专家多次研讨，并对国家电网、神华集团、中国石油、南方电网、等大批甲方企业以及启明星辰、绿盟科技、匡恩网络等乙方企业进行**岗位调研**，通过智联招聘、51job等招聘网站进行**岗位分析**，设计本赛项。本赛项知识与技能点同企业网络安全工作岗位和业务充分对接，培养工业互联网领域等应用型安全人才。

（四）**普惠性**。赛前公布涵盖赛项知识技能点的实训资源，通过微信、QQ等沟通平台进行互动，提供在线问答服务，通过“工业互联网安全技术与应用”竞赛考试系统组织2次模拟竞赛。于开赛2个月前在大赛网络信息发布平台上公开全部赛题。

（五）**先进性。**工业互联网系统中涉及的物联网系统、工业控制系统均属于近些年被广泛关注的系统，国家还没有出台相关系统的政策要求及防护标准。通过本赛项工业互联网安全方案的实施，充分体现了工业互联网安全技术与应用竞赛的先进性。

竞赛过程中采用“工业互联网安全技术与应用”竞赛考试系统，渗透题目由系统自动统计评分，通过场外大屏，可实时跟踪监控答题进度。安全防护题目需要由裁判手工评分部分，明确每项得分点并公开，保证公平公正。

比赛后公布竞赛试题，公布用于竞赛的试卷的评分标准和参考答案。

**六、竞赛内容简介（须附英文对照简介）**

“工业互联网安全技术与应用”项目竞赛设计遵循《2018年全国职业院校技能大赛制度汇编》的总体指导思想及原则。

随着物联网技术在工业互联网中的广泛应用，物联网设备安全深深影响着智能制造工业企业的网络安全保障能力。竞赛设计适应国家产业结构调整与社会发展需要，展示信息时代高技能人才培养的特点，聚焦工业领域信息安全需求，与相关企业紧密合作，以实际项目为基础，针对计算机网络专业学生实践能力欠缺的短板，以赛促教，以赛促学，以赛促建。

本赛项重点考察高职学生在学习完相关竞技知识理论时，能融合多种信息安全技术手段，对互联网出口安全漏洞、内网系统安全漏洞、工业控制网络系统安全漏洞进行评估，并要求学生对工业互联网络安全防护加固，适合高职学生的综合实践能力培养。同时，赛项考核点包含办公网络环境安全、物联网（IOT）设备安全、生产环境安全等方面的漏洞挖掘、利用以及防护技能，能够促进高职院校“信息安全与管理”、“物联网应用技术”两个专业多门课程建设及教学改革，促进学生专业核心技能和职业核心能力的同步提高，提升毕业生就业水平。

【英文版】

With the wide application of Internet of things technology in industrial Internet, the security of Internet of things devices has a profound impact on the network security capability of intelligent manufacturing enterprises. The design of competition should adapt to the management of national industries' structure and the need of social development, to present the characteristic of talented people trained in information age, to focus on information security requirements in industry; and the competition also needs to collaborate with enterprises closely, which are based on the real projects, aim at the computer networks major students ‘shortcoming in practice. Because of the competition, we could promote teachers’ teaching, students’ learning and construction of major.

The competition focuses on higher vocational students after learning related competitive theory, combines various information security technology. The assessment of the export of Internet security vulnerabilities, inner network system security vulnerabilities, and industrial control network system security vulnerability are all needed, so as the reinforce of industrial Internet security protection. The competition can train for vocational students comprehensive practical ability. At the same time, the examination includes vulnerability mining and protection skills about office network security, Networking (IOT) equipment safety, production environment security and so on. The competition can also promote higher vocational colleges’ course construction and teaching reform in the major “information security and management "," Internet application technology ", promote students to improve synchronization professional skill and occupation of core competence, enhance the level of employment of graduates.

**七、竞赛方式（含组队要求、是否邀请境外代表队参赛）**

（一）竞赛以团队赛方式进行，每队由3名选手（设场上队长1名）和1-2名指导教师组成。指导老师须为本校专职或兼职教师。要求参赛队中队员必须来自同一所学校，不得跨校组队。同一学校相同报名参赛队不超过1支。组队成员能力建议3名选手均覆盖web安全技术，其中一名队员侧重于内网渗透、一名队员侧重于工控安全、第三名队员侧重物联网安全。

（二）参赛选手必须是2018年度在籍的高等职业院校学生，性别和年级不限。往届全国职业院校技能大赛同类赛项中获得一等奖的选手，不得参加同一项目组别的赛项。

（三）在全国职业院校技能大赛组委会与赛项执委会的指导下，在赛区组委会与执委会的领导下，由工业和信息化职业教育教学指导委员会牵头成立2018年全国职业院校工业互联网安全技术与应用赛项执委会，下设本赛项专家组、裁判组、督导组、仲裁组等工作机构。

（四）参加竞赛各代表队的抽签顺序和竞赛场次，将在领队会议上现场抽签确定。每名选手竞赛的赛位号，在进入赛场进行检录时由抽签确定。抽签工作由裁判长主持，赛务组负责组织实施，竞赛督导人员现场监督。

（五）2018年邀请国际团队参赛，同时欢迎国内团队到场观摩。

**八、竞赛时间安排与流程**

（一）时间安排

时间安排：6个小时

|  |  |
| --- | --- |
| **竞赛前一天** | **（1）赛前准备** |
| 8：00-14：30 | 参赛队报到 |
| 14︰30-15︰30 | 召开领队与指导教师赛项说明会、答疑 |
| 15︰30-17︰00 | 参赛选手熟悉赛场 |
| **竞赛当天** | **（2）（3）（4）** |
| **7：50-9：00** | **（2）检录入场** |
| 7:50-8:10 | 参赛选手到指定地点集合检录，抽取抽签顺序号、一次加密 |
| 8︰10-8︰30 | 选手抽工位号、二次加密、工具检验 |
| 8︰30-8︰40 | 选手进入工位，进行设备、工具、资料检查并签字确认 |
| 8︰40-8︰50 | 分发比赛任务书、指导老师进场 |
| 8：50-9：00 | 现场裁判讲解比赛注意事项、宣布比赛开始 |
| **9︰00-15︰00** | **（3）竞赛时间** |
| 9︰00-13︰00 | 选手完成工作任务 |
| 10︰00-11︰30 | 观众观摩赛场 |
| **15：00-17：00** | **（4）成绩评定** |
| 15：00-15：10 | 参赛队离场 |
| 15：00-17：00 | 赛项申诉与仲裁 |
| 15：00-18：00 | 裁判进行竞赛成绩评定，成绩复核确认、录入上报 |
| 21︰30-23︰30 | 竞赛成绩登记与解密 |
| **竞赛日后一天** | **（5）闭幕式** |
| 9：00-9：30 | 赛项点评 |
| 9：30-10：30 | 公布成绩、颁奖 |

（二）竞赛流程

参赛队报到

领队会

熟悉赛场

检录、一次加密

二次加密

宣布比赛开始

比赛操作

宣布比赛结束

评分

成绩复核确认

成绩录入上报

闭幕式公布成绩

仲裁申请

赛项仲裁委复议回复

二次申诉

赛区仲裁委复议回复

**九、竞赛试题**

**2018年全国职业院校技能大赛**

**高职组“工业互联网安全技术与应用”**

**竞赛任务书（样题）**

**题目: “工业互联网安全技术与应用”的设计与实现**

**【选手须知】：**

1. 任务书通过在线“工业互联网安全技术与应用”竞赛考试系统和书面文档共同发布，内容完全一致，电子文档共 3 页，如出现任务书缺页、字迹不清、同考试系统不一致等问题，请及时向裁判示意，并进行任务书的更换。

2. 参赛团队应在 6 小时内完成任务书规定内容；选手在竞赛过程中涉及到渗透与防护任务。渗透所获得的题目答案，须实时提交至“工业互联网安全技术与应用”竞赛系统，系统自动评分。防护任务需要选手做防护同时，通过配置文档截图保存，并最后提交至“工业互联网安全技术与应用”竞赛系统。由裁判手动评分。

3. 选手提交的试卷用工位号标识，不得写上姓名或与身份有关的信息，否则成绩无效。

4. 比赛过程中由于人为原因造成设备或软件损坏，不予更换。

**【项目背景】**

某大型制造型企业，积极响应国家《智能制造2015》战略，已完成了工业物联网在企业研发设计、生产制造、经营管理、销售服务等全流程和全产业链的综合集成应用，也完成了物联网（IOT）技术在工业互联网中的研发和应用示范，组成了覆盖办公网络、物联网（IOT）设备、生产环境的工业互联网智能制造网络系统。

当完成公司工业互联网智能制造网络系统的构建之后，伴随而来的网络安全问题也日益凸显，传统应用漏洞（web应用、安全产品、操作系统、数据库、网络设备）不断有新的漏洞涌现威胁，同时物联网智能设备、移动互联终端设备、工业控制网络等存在的漏洞造成的威胁日益增多，伴随着工业控制系统接入Internet所造成的生产网络安全事故也呈明显的增加趋势。

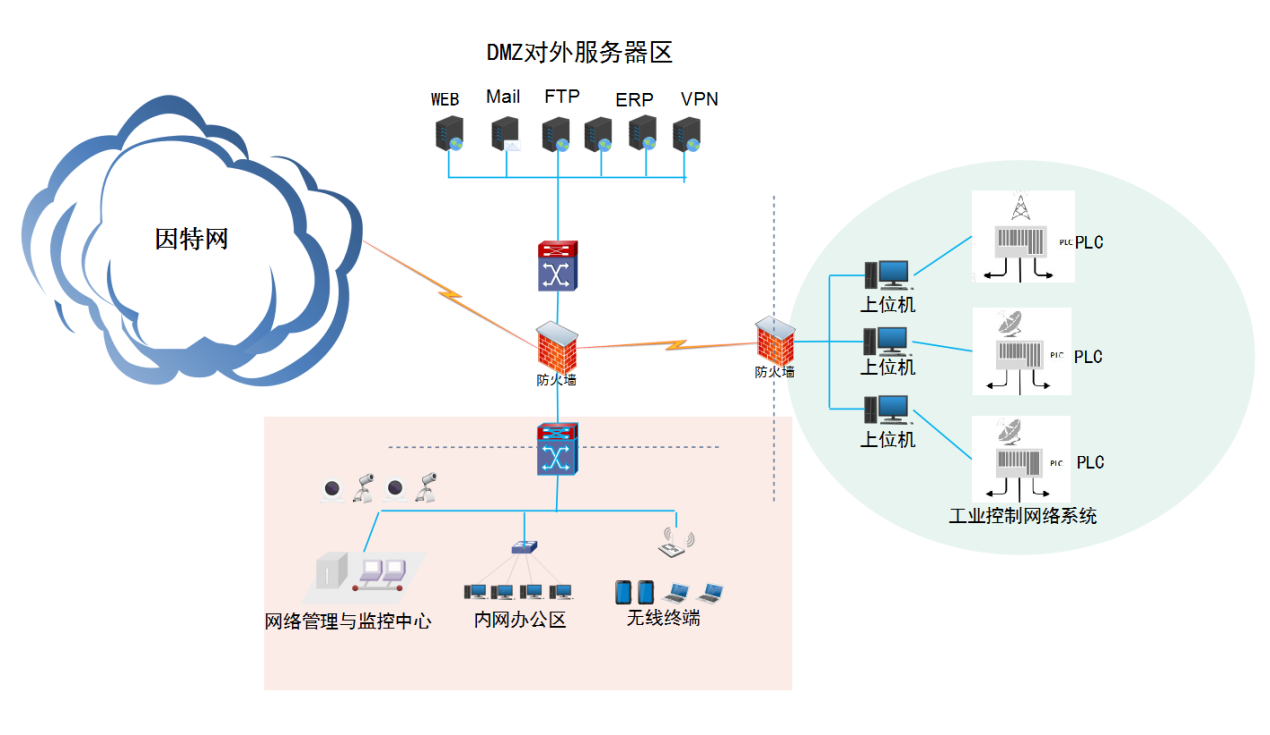
工业互联网的安全威胁远比传统互联网时代造成的影响更大，全球范围影响的案例如“Stuxnet——震网病毒”给伊朗的核设施带来了毁灭性的打击，因此基于工业互联网的漏洞渗透挖掘与防护，就显得尤为重要。本次任务将在典型的某企业工业互联网模拟场景中，由参赛学员完成从渗透到防护的工作任务。

某企业工业互联网模拟场景网络架构设计如下：

1.办公网络环境，通过防火墙链接互联网，同时设置dmz区域，发布对Internet提供的服务。通过无线扩展，增加了移动终端的连接途径。

2.物联网（IOT）设备，部署了智能门禁、网络监控、网络投影、网络视频终端等物联网与监控系统。

3.生产环境，通过工业防火墙，连接生产工业控制系统网络。工控系统涉及上位机、PLC、传感器等。



工业互联网络设计图

需要根据上图的网络架构设计，分析现有工业互联网络存在的安全威胁，找出系统的漏洞，针对漏洞所能达到的效果进行评估，同时对漏洞进行加固，以防止安全事件的发生。

**【项目任务】**

**任务一、互联网出口的安全漏洞发现与评估**

任务1.1 扫描网络的Internet出口及服务，评估网络出口及服务的端口情况及漏洞信息。

任务1.2 通过网络对外的服务漏洞的利用，获得dmz区服务器的控制权。

**任务二、内网系统安全漏洞发现与评估**

任务2.1 扫描并发现内网的其他服务器服务与漏洞信息，并通过漏洞利用评估漏洞的威胁。

任务2.2 扫描并发现内网IOT类设备的安全漏洞，并通过漏洞利用评估漏洞的威胁。

**任务三、工业控制网络系统安全漏洞发现与评估**

任务3.1 扫描并发现工业控制网络连接上位机，并通过漏洞利用评估漏洞的威胁。

任务3.2 扫描并发现工控系统设备，如PLC的漏洞信息，并通过漏洞利用评估漏洞的威胁。

**任务四、工业互联网络安全防护加固。**

任务4.1 分析网络Internet出口及服务存在的脆弱性，并进行安全加固，并书写加固配置手册。

任务4.2 分析内网的服务与应用漏洞，进行修复加固，并书写加固配置手册。

任务4.3 分析内网的IOT类设备漏洞，进行修复加固，并书写加固配置手册。

任务4.4 分析工业控制网络系统漏洞，进行修复加固，并书写加固配置手册。

1. **评分标准制定原则、评分方法、评分细则**

（一）考核内容

本赛项考核内容主要涉及办公网络环境安全、物联网（IOT）设备安全、生产环境安全等方面的漏洞挖掘、利用以及防护技能。其中：

1.办公网络环境安全涉及：web应用、操作系统、数据库、网络设备等。

2.物联网（IOT）设备安全：网络摄像头、无线AP、无线终端、以及其他相关联的物联网络设备。

3.生产环境安全涉及：工业网络协议安全、HMI上位机安全、固件漏洞、PLC漏洞等安全问题。

竞赛内容结合工业互联网各组成部分，从Internet入口安全渗透、内网渗透、生产网络渗透以及防护组成。通过渗透过程中的漏洞挖掘，评估工业互联网存在的脆弱性以及安全威胁。通过安全加固操作，实现对工业互联网的安全防护。题目模拟典型工业互联网的网络架构，通过完整的渗透以及加固过程，让学生实现宏观到细节的对工业互联网安全技术与应用的深入理解。

**竞赛内容分类表：**

|  |  |
| --- | --- |
| **类别** | **内容** |
| 互联网出口的安全漏洞发现与评估 | 1.web系统漏洞挖掘与评估；  2.web系统渗透与提权。 |
| 内网系统安全漏洞发现与评估 | 1.内网代理技术应用；  2.内网渗透技术；  3.物联网设备漏洞挖掘与利用技术。 |
| 工业控制网络系统安全漏洞发现与评估 | 1.工业控制网络系统结构；  2.工控上位机的漏洞发现与利用；  3.PLC漏洞发现与利用；  4.工业防火墙技术。 |
| 工业互联网络安全防护加固 | 1.web应用加固；  2.内网主机安全加固；  3.物联网设备安全加固；  4.工控系统安全加固。 |

（二）评分标准制定原则

根据《2018年全国职业院校技能大赛成绩管理办法》的相关要求，遵循成绩管理基本流程，通过检录、一次加密、二次加密、竞赛成绩评定、解密、成绩公布等流程，规范成绩管理。

竞赛评分严格按照公平、公正、公开的原则，评分标准注重考查参赛选手以下各方面的能力和水平。

1.web系统渗透与防护技能；

2.内网渗透与防护技能；

3.物联网系统渗透与防护技能；

4.工控系统渗透与防护技能。

（三）评分方法

组织分工:

1.本竞赛参与赛项成绩管理的组织机构包括裁判组、监督组和仲裁组，受赛项执委会领导。裁判组设置裁判20人，包括裁判长1名，裁判19名。

2．监督组对裁判组的工作进行全程监督，并对竞赛成绩抽检复核。

3.仲裁组负责接受由参赛队领队提出的对裁判结果的申诉，组织复议并及时反馈复议结果。

4.竞赛将制定裁判遴选管理办法、赛事保密细则和预案、命题管理办法等制度，保证竞赛的公平公正。赞助企业、参赛院校不安排人员进入裁判团队。

评分方法:

1.本赛项的评分方法分为：机考评分、结果评分。

2.本赛项考核环节：工业互联网安全技术与应用赛项渗透部分采用机考评分，防护加固部分采用结果评分。

3.机考评分。机考评分占比60%,参赛队根据分配到的考试系统帐号登录系统，完成竞赛渗透部分内容，由系统自动判分。

4.结果评分：结果评分主要体现在工业互联网安全加固防护部分。结果评分占比40%，参赛选手通过渗透过程中发现的安全漏洞，进行安全加固，并通过截图等手段编写安全加固手册。加固手册提交到竞赛系统，由评分裁判依据赛项评价标准进行评价评分。

5.每个裁判小组汇总本组所有的评分表，计算成绩，本组裁判成员签字确认。成绩汇总表备案以供核查，最终的成绩由裁判长及监督人员进行审核、签字确认，上报大赛组委会。

6.赛项结束后，大赛组委会负责公布最终竞赛成绩。

（四）评分细则

评分标准:总分100分

|  |  |  |
| --- | --- | --- |
| **考核环节** | **考核知识点和技能点** | **分值** |
| **1.互联网出口的安全漏洞发现与评估** | 扫描企业对外web服务器，获取web注入漏洞，通过注入，获取后台管理员账户信息。 | 2 |
| 通过web后台，寻找上传漏洞，成功上传一句户木马，可以通过webshell读取flag信息。 | 2 |
| 通过系统漏洞分析，上传提权工具，获得高权限，发现c盘根目录提示flag。 | 2 |
| 通过上传shell，实现代理连接。从外网绕过防火墙连接到web服务器的3389端口。 | 5 |
| 2. **内网系统安全漏洞发现与评估** | 通过代理技术，扫描发现内网ftp服务器，并获取敏感信息。 | 3 |
| 通过扫描技术，发现内网网管服务器，并获得网关服务器IP及端口信息。 | 5 |
| 通过“永恒之蓝”漏洞攻击，获取网管服务器权限及敏感文件。 | 5 |
| 通过扫描发现网络摄像头，通过摄像头CNVD-2017-01037漏洞，获取摄像头管理员信息。 | 8 |
| 通过扫描发现AP，（友讯集团(D-Link)新产品“云路由”）固件系统中存在漏洞，攻破路由器后台，获取ap管理员权限，控制无线AP。 | 8 |
| 3. **工业控制网络系统安全漏洞发现与评估** | 通过扫描，发现上位机IP地址。 | 2 |
| 发现SIMATIC WinCC存在文件包含漏洞。通过未经身份验证的攻击，发送数据包到SIMATIC WinCC可提取任意文件，获取敏感信息。 | 8 |
| 通过提示，获知PLC为(Siemens SIMATIC S7 PLC) ,该系统在实现上存在密码泄露漏洞，攻击者可利用此漏洞获取设备密码凭证，通过离线破解，获取密码信息。 | 10 |
| 4. **工业互联网络安全防护加固。** | 加固web服务器SQL注入漏洞。 | 3 |
| 加固web服务器webshell上传漏洞。 | 4 |
| 升级web服务器操作系统，加固提权漏洞。 | 4 |
| 设置ftp默认账号和复杂口令。 | 3 |
| 网管服务器，关闭445端口，或升级系统，打补丁。 | 4 |
| 升级网络摄像头固件，修复信息泄露漏洞。 | 5 |
| 升级路由器固件，修复未授权获取敏感信息漏洞。 | 5 |
| 升级SIMATIC WinCC软件，修复文件包含漏洞。 | 6 |
| 升级PLC系统，防止认证凭证泄露。 | 6 |

**十一、奖项设置**

竞赛设参赛选手团体奖，以赛项实际参赛队总数为基数，一等奖占比10%，二等奖占比20%，三等奖占比30%，小数点后四舍五入。

获得一、二、三等奖的团体赛参赛选手，授予相应荣誉证书。

获得一等奖的参赛队指导教师获“优秀指导教师奖”，授予荣誉证书。

大赛所有荣誉证书、奖杯由大赛组委会统一制作颁发。

**十二、技术规范**

工业互联网安全技术与应用按照《普通高等学校高等职业教育（专科）专业目录（2015年）》的电子信息大类（61）、物联网应用技术（610119）、信息安全与管理（610211）等专业的教学要求和职业技术标准、参照信息安全国家技术标准以及国内外电子信息行业技术标准。

|  |  |  |
| --- | --- | --- |
| **序号** | **标准号** | **中文标准名称** |
| 1 | GB 17859-1999 | 《计算机信息系统安全保护等级划分准则》 |
| 2 | GB/T 20271-2006 | 《信息安全技术信息系统通用安全技术要求》 |
| 3 | GB/T 20270-2006 | 《信息安全技术网络基础安全技术要求》 |
| 4 | GB/T 20272-2006 | 《信息安全技术操作系统安全技术要求》 |
| 6 | GA/T 671-2006 | 《信息安全技术终端计算机系统安全等级技术要求》 |
| 7 | GB/T 20269-2006 | 《信息安全技术信息系统安全管理要求》 |
| 8 | GB21671-2008 | 基于以太网技术的局域网系统验收测评规范 |
| 9 | LD/T81.1-2006 | 职业技能实训和鉴定设备技术规范 |

**竞赛现场环境标准:**

1．竞赛现场设置竞赛区、裁判区、服务区、技术支持区。

2．竞赛区为参赛队提供标准竞赛设备；竞赛区的每个比赛工位上标明编号；每个比赛间配置若干工作台，用于摆放计算机和其它调试操作，工作台上面摆放制作工具等。

3.裁判区配置计算机等统计工具，配置投影仪及大屏幕，用于放映竞赛实时的通关进程；配置摄像机，记录各参赛队的比赛全过程。

4.服务区提供医疗等服务保障。

5.技术支持区为参赛选手提供公用焊接等竞赛相关设备。

6.竞赛现场各个工作区配备单相220V/3A以上交流电源。

**十三、建议使用的比赛器材、技术平台和场地要求**

1. 建议使用的比赛器材和技术平台

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **数量** | **参考型号** | **备注** |
| 1 | 攻防演练系统 | 1 | 西普教育攻防演练系统；时代恒运实战比赛系统 | 每台可支持5个参赛队共用，根据参赛队数量按比例增加 |
| 2 | 工控安全攻防演练系统 | 1 | 西普教育工控安全攻防演练系统；时代恒运靶场实战系统 | 所有参赛组共用一台设备，各小组分配相同权限，皆在此平台进行比赛 |
| 3 | PC | 3 | 笔记本或台式机 | 每小组三台操作PC，用于比赛 |

**攻防演练系统具体参数：**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **产品名称** | **技术指标需求** | **单位** | **数量** |
| 安全实验演练 | 基础云平台 | 一、功能要求：  ★支持对安全实验演练主控设备的占用率监控，包括CPU核数、CPU使用率、内存总数、内存使用数、硬盘总大小、硬盘使用大小等信息；  ★支持对系统用户总数、使用用户数、课程总数、课程使用数、拓扑总数、拓扑使用数、虚拟机母本数、正在运行的虚拟机数等信息进行监控；  系统B/S架构访问，无需安装客户端软件；  ★系统支持竞赛模式和练习模式；  支持管理员、参赛队员和观众三种角色的使用与验证，同时对并发用户数量的控制。支持对管理员、参赛队员和观众进行账号管理，要求新增帐号默认有初始密码；  ★系统支持主流的虚拟主机操作系统类型，并且不限制用户上传操作系统的类型，要求至少包含Windows、Linux操作系统类型；  ★教师用户可以创建新的教学课程与教学实验，并且不限制数量；  ★内置DHCP服务，可以设置多个地址池，能够为竞赛中的资源分配IP地址，包括：网段、掩码位、适用模块等  ★长宽高20cm\*30cm\*20cm的便携式手提箱；  二、硬件规格要求:  CPU：E3-1230v5；  内存：32G；  硬盘：SSD 1T\*1；  ≥4个千兆网口，≥2个USB口，≥1个RJ-45串口； | 台 | 1 |
| 交换机 | 24个10/100/1000Base-T，4个复用SFP千兆端口（Combo）；  支持4个万兆SFP+；  16K MAC地址容量；  支持MAC地址自动学习和老化；  支持4K个VLAN；  支持Guest VLAN、Voice VLAN；  支持基于MAC/协议/IP子网/策略/端口的VLAN；  支持RRPP环型拓扑和RRPP多实例；  静态路由、RIPv1/2、RIPng、OSPF、OSPFv3、ECMP、ISIS、ISISv6、BGP、BGP4+、VRRP、VRRP6；  支持ND（Neighbor Discovery）；  支持基于源IPv6 地址、目的IPv6 地址、四层端口、协议类型等ACL；  支持 PIM DM、PIM SM、PIM SSM；  支持IGMP v1/v2/v3 Snooping和快速离开机制；  支持捆绑端口的组播负载分担，支持可控组播，支持基于端口的组播流量统计；  支持对端口入方向、出方向进行速率限制；  支持L2（Layer 2）~L4（Layer 4）包过滤功能，提供基于源MAC地址、目的MAC地址、源IP地址、目的IP地址、TCP/UDP协议源/目的端口号、协议、VLAN的包过滤功能；  用户分级管理和口令保护；  支持防止DOS、ARP攻击功能、ICMP防攻击；  支持IP、MAC、端口、VLAN的组合绑定；  支持作为SVF client零配置即插即用；  智能iStack堆叠；  支持虚拟电缆检测(Virtual Cable Test)；  VBST基于VLAN生成树协议（和PVST/PVST+/RPVST 互通）；  LNP 链路类型协商协议（和DTP相似功能）；  VCMP VLAN集中管理协议（和VTP相似功能）； | 台 | 1 |
| 平台管理系统 | 支持单兵作战和团队作战；  ★支持竞赛模式和练习模式两种答题方式；  支持实现自动进行竞赛与手动进行竞赛两种模式，自动开启竞赛支持设置竞赛开始时间、结束时间以及每个竞赛阶段的开始时间和结束时间，到点自动开始该阶段的比赛；能够同时进行多场竞赛（为证明此功能的真实性必须包含此功能，必要时提供现场演示）；  ★支持自定义竞赛内容，包括：竞赛名称、是否开启观众席、竞赛公告、竞赛试卷、竞赛时间、竞赛工具、竞赛团队等内容，要求竞赛列表必须包含竞赛名称、试卷名称、分值、模式、竞赛工具、参与队伍、状态、管理、操作；  ★支持用户添加竞赛、练习试卷信息，包含：试卷标题、备注信息、基础考核题、CTF夺旗题、综合渗透题、攻防对抗题、防守分值、攻击分值上限、防守分值不设下限、攻击分值不设下限等；  竞赛管理，支持开始竞赛、暂停竞赛、停止竞赛三种操作方式；  支持自由选择竞赛公告、竞赛试卷、竞赛时间、竞赛工具、竞赛团队；  支持练习场景生成，要求可以自由选择练习公告、练习试卷、练习工具、练习团队；  支持竞赛场景或练习场景过程中，用户可以自由选择题目类型与题目数量，并自动计算总体分值；  ★可以设置FLAG推送的时间,要求以分钟为单位；  在竞赛过程中，支持开启、关闭、重启竞赛靶机环境；  ★支持四种竞赛阶段：基础考核阶段、CTF夺旗阶段、综合渗透阶段、攻防对抗阶段，四种竞赛阶段可以随意组合；  基础考核阶段，要求答案可以反复提交，提交后页面显示提交的答案结果；  CTF夺旗阶段考核支持题目对错判断，参赛选手填入答案后能够自动判断答案的正确性，同时答题页面需要展现题目信息、分值、已提交的答案、题目连接等；  综合渗透阶段要求赛题可以反复提交，答题页面要求显示题目描述、分值、已提交的正确答案、题目连接、提交的答案是否正确等信息；  ★攻防对抗阶段能够显示防守机的用户名、密码、地址等信息，能够显示获得的flag数量与攻陷的队伍数量，能够显示防守机当前轮数被攻击的成功的情况与整个阶段所有被攻击成功的队伍数量（为证明此功能的真实性，必要时提供现场演示）；  竞赛支持针对不同用户发布不同的公告信息，包括学生公告、观众公告，必须支持实时弹出公告功能，支持向指定参赛队伍发送公告；  支持用户以选择文件形式、拖拽形式上传自己的镜像，上传过程中实时显示镜像上传进度百分比，上传后系统自动纪录镜像的状态、大小等信息，要求镜像上传后自动获取镜像编号、镜像名称、镜像容量、镜像分类等信息；  用户端支持对系统镜像资源的查询功能，基础镜像库和用户上传的镜像库分类管理，查询条件要求支持镜像名称的关键字查询方式；  ★支持用户创建母本虚机功能，创建方式要求支持安装母本虚机、上传母本虚机、复用母本虚机三种形式；  ★安装母本虚机，支持设置虚拟资源，包括：母本名称、分类、内存大小、CPU个数、网卡数量、光驱数量、硬盘大小、硬盘数量等信息，进入安装虚机页面后可以在页面上添加虚机描述信息、加载光驱、设置网卡IP、子网掩码等信息，方便用户对虚机进行管理；  ★上传母本虚机，支持设置虚拟资源，包括：母本名称、内存大小、CPU个数、网卡数量、光驱数量、硬盘大小、硬盘数量等信息，要求上传母本虚机时可以实时显示上传进度百分比，上传的母本虚机需要支持qcow2格式；  ★复用母本虚机，支持设置虚拟资源，包括：母本名称、复用的虚机、分类、内存大小、CPU个数、网卡数量、光驱数量、硬盘大小、硬盘数量等信息；  支持每个虚拟机内配置对应实验所需要的实验环境，包含操作系统环境、实验配套工具等，要求虚拟机通过WEB浏览器页面的形式进行实验；  用户端支持对母本虚机的查询功能，基础母本库和用户的母本库分类管理，查询条件要求支持母本虚机名称的关键字查询方式；  支持对基础母本库、私有母本库的查询功能，要求基础母本库的查询条件包含：母本名称、母本分类、CPU、硬盘、内容等，私有母本库查询条件包含：母本名称、分类、CPU、硬盘、内容、创建人，私有母本库支持删除、批量删除；  ★用户可以通过安装、上传、复用等形式制作靶场中的靶机，制作靶机的过程中，用户可以设置所使用的镜像、操作系统类型、内存大小、CPU个数、网卡数量、光驱数量、硬盘大小、硬盘数量等信息（为证明此功能的真实性，所提供测试报告中的测试项目必须包含此功能，必要时提供现场演示）；  ★上传靶机过程中，用户可以选择自行制作的靶机，要求靶机支持qcow2格式； | 套 | 1 |
| 关卡资源库 | ★包含基础考核题目数量不少于100道题，CTF夺旗题目数量不少于40道题，综合渗透题目数量不少于10道题，攻防对抗题目数量不少于6道题；  基础考核题必须包含基本编码、MySQL数据库安全、SQL注入利用、信息隐藏、XSS与编码、MSSQL数据库安全、MD5算法、缓冲区溢出之shellcode提取、缓冲区溢出之ActiveX漏洞的fuzzing和利用、移动应用的安全防护、逆向工程、密码破解、SQL注入、源码分析、欺骗技术、缓冲区溢出、溢出攻击安全防护、编码解析、Windows操作系统主机安全防护、Linux/Unix操作系统主机安全防护、DNS系统的安全防护、扫描与探测、DOS及DDOS类攻击的安全防护、网络层攻击的安全防护、提权攻击的安全防护、数据保护、主机恶意代码防护、网络单元信息的收集、暴力破解、Web入侵安全防护、安全设备与工具、系统压缩文件密码破解、代码审计等内容，提供必须的题目环境及服务；  CTF夺旗题目必须包含基本编码、MySQL数据库安全、SQL注入利用、信息隐藏、XSS与编码、MSSQL数据库安全、MD5算法、缓冲区溢出之shellcode提取、缓冲区溢出之ActiveX漏洞的fuzzing和利用、逆向工程、密码破解、SQL注入、源码分析、欺骗技术、缓冲区溢出、编程语言、编码解析、系统压缩文件密码破解、代码审计等内容，提供必须的题目环境及服务  综合渗透题目必须包含mailpress RCE漏洞、弱口令漏洞、权限提升、列目录漏洞、爆破密码、自定义页面上传木马、信息收集、Web入侵安全防护、主机入侵与防护、数据库安全、溢出攻击、提权攻击与防护、后门技术、基本编码、MySQL数据库安全、SQL注入利用、信息隐藏、XSS与编码、MSSQL数据库安全、MD5算法、缓冲区溢出之shellcode提取、缓冲区溢出之ActiveX漏洞的fuzzing利用、密码破解、SQL注入、源码分析、欺骗技术、缓冲区溢出、编码解析、系统压缩文件密码破解、代码审计、等漏洞内容，提供必须的题目环境及服务  攻防对抗必须包含任意文件读取漏洞、注入上传漏洞、任意权限getshell、后台任意目录上传和执行、弱密码爆破、宽字节配合万能密钥、mailpress RCE漏洞、弱口令漏洞、权限提升、列目录漏洞、爆破密码、自定义页面上传木马、基本编码、数据库安全、溢出攻击、信息隐藏、XSS与编码、MD5算法、密码破解、主机入侵与防护、SQL注入、源码分析、欺骗技术、组件安全、提权攻击与防护、编码解析、后门技术与防护、代码审计等漏洞，提供必须的题目环境及服务； | 套 | 1 |

**工控安全攻防演练系统具体参数：**

|  |  |
| --- | --- |
| 产品配置（包括配置、标准及技术指标等详细内容） | ★实验箱集成施耐德PLC-TM218、威纶通HMI触摸屏-MT8070iP/MT8070iH5，支持MODBUS TCP工业通讯方式，构建成小型工业控制系统，具备展示工业控制系统架构拓扑和特点，又可完成自动化控制系统实验，满足对工业控制系统学习、实践需求。。  ★结合行业背景，工控案例集成了信号灯控制、交通灯控制、流水灯控制、模拟量控制、电机控制、汽车装配、石化流程、智能制造、钢铁转炉、变电站。  ★以实际工控系统系统为攻防目标，配套PC端攻击程序和成熟的工控网络安全监测产品，可进行ARP欺骗、ARP攻击、数据篡改指令、汽车装配线指令注入攻击实验，石化流程指令篡改攻击，智能制造攻击，钢铁转炉生产流程攻击实验，变电站攻击实验。  ★配合智能保护模块，可以进行数据篡改防护、汽车装配线指令注入攻击防护实验，石化流程指令篡改防护，智能制造攻击防护，钢铁转炉生产流程攻击防护，变电站攻击防护实验。  ★监测审计产品可提供网络监测和流量与协议审计，抓取工控协议数据包，并对数据包进行深入解析。  ★提供工控系统网络安全教材，内容涵盖工业控制理论、工控网络结构、工控网络漏洞、工业网络安全协议、工控网络安全防御和典型行业安全案例分析，提供配套的实验课件、实验手册，形成了工控网络安全教学体系。  ★监测审计产品硬件配置：CPU处理性能 2 GHz 3MB Cache；内存：16GB DDR3；存储：日志存储16GB；以太网口数量2个10/100/1000Mbps；Console管理口1个RJ45； 1个 USB2.0接口  ★免费1年升级服务。  ★监测审计产品具有以下功能：  白名单  监测审计产品支持白名单，有智能学习功能，自动学习生成白名单，形成白名单规则进行部署，通过白名单规则匹配判断工控协议数据包是否异常，得出允许、告警等结果，白名单包括多种工控协议和传统协议白名单。  实时网络监测  对工控网络中的数据、事件行为进行实时监测、实时告警，帮助用户实时掌握工控网络运行状况。  网络安全审计  对工控网络中存在的所有活动提供协议审计、流量审计、行为审计，生成完整记录便于事件追溯。  防御策略建议  根据监测结果，提供防御策略建议，帮助用户构建适用的专属工控网络安全防御体系。  可视化网络拓扑  提供直观清晰的网络拓扑图并集成网络告警信息，是用户在了解网络拓扑的同时获知网络告警分布，轻松掌握网络状况。  网络行为可视化  以静态的网络拓扑管理工具，配合动态的流量行为分析，关联网络告警分布，以最直接最详细的呈现方式，帮助用户了解自身网络。  流量异常监测  对流量的流入流出的异常情况进行监测，实时以图的形式展现出来，直观方便观察数控流量情况，在监测到流量突然变大后进行告警。  实时事件导出功能  事件信息，支持第三方平台syslog实时导出功能。  ★智能保护产品硬件配置：CPU处理性能 2 GHz 3MB Cache；内存：16GB DDR3；存储：日志存储16GB；以太网口数量2个10/100/1000Mbps；Console管理口具备1个RJ45； 1个 USB2.0接口  ★智能保护产品具有以下功能：  工业协议智能解析与防护  智能保护平台针对工控系统的防御系统设计，能快速识别系统中的非法操作、异常事件以及外部攻击并及时告警和阻断非法数据包。  多种保护防御机制  智能保护平台通过白名单、黑名单、IP/MAC地址绑定方式，对APT网络攻击、异常行为和非法数据包等多种威胁进行多方式保护，对发现的威胁进行告警和阻断，保护工业控制网络安全，有效的提高网络的安全性。  持续专业的安全漏洞服务  持续的提供专业的安全漏洞服务，为各种工控行业提供有针对性的、可行的防护方案和建议。通过及时的升级，智能保护平台就能有效的防止日益严重APT高级持久性威胁。  实时事件导出功能  事件信息，支持第三方平台syslog实时导出功能。 |

**工控安全攻防演练系统软、硬件配置**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **元器件** | **型号** | **数量** | **品牌** |
| 1 | PLC控制器 | TM218LDAE40DRPHN | 1 | 施耐德 |
| 2 | PLC接口扩展模块 | TM2DOCKN | 1 | 施耐德 |
| 3 | PLC模拟量模块 | TM2AMM3HT(2AI,1AO) | 1 | 施耐德 |
| 4 | 触摸屏 | MT8070IH5，DC24V | 1 | 威纶通 |
| 5 | 继电器含座 | RJ2S-CL-D24 | 2 | 和泉 |
| 6 | 交换机 | BL-SG108M，带镜像口功能 | 1 | 必联 |
| 7 | 开关电源 | DR-60-24 | 1 | 台湾明纬 |
| 8 | 指示灯 | LA42(B)DJ/024R | 1 | 上海天逸 |
| 9 | 指示灯 | LA42(B)DJ/024Y | 1 | 上海天逸 |
| 10 | 指示灯 | LA42(B)DJ/024G | 1 | 上海天逸 |
| 11 | 蜂鸣器 | LA42(B)FMJ024 | 1 | 上海天逸 |
| 12 | 直流电机 | 24v（0-200转速） | 1 | 中兴电机 |
| 13 | 调带器 | 控制电机 | 1 | 中兴电机 |
| 14 | 直流电压表 | BT3603R 0-10VDC，电源24VDC | 1 | 聚英 |
| 15 | 电位器 | 单圈B10K | 2 | W.L |
| 16 | 波段开关 | BRT | 1 | BRT |
| 17 | 220V开关带保险插座 | 10A | 1 | Jec |
| 18 | 导线、网线、箱体、安装架 |  | 1套 | 定制 |
| 19 | 监测审计 | KEC教育版 | 1 | 匡恩网络 |
| 20 | 智能保护 | KEA教育版 | 1 | 匡恩网络 |
| 21 | PLC编程软件 | Somachine v4.1 | 1 | 施耐德 |
| 22 | 触摸屏组态软件 | EB8000 | 1 | 威纶通 |
| 23 | 攻击软件 | 基于Python | 1 | 定制 |
| 24 | SCADA项目文件 | 基于WINCC | 1 | 定制 |
| 25 | 触摸屏组态项目文件 | 基于EB8000 | 1 | 定制 |
| 26 | PLC项目文件 | 基于Somachine v4.1 | 1 | 定制 |

**十四、安全保障**

根据《全国职业院校技能大赛安全管理规定》的有关要求，制以下具体的安全管理措施并严格执行。

(一) 成立安全保障工作组，负责本赛项筹备和比赛期间的各项安全工作，赛项执委会主任和安全保障工作组组长均为第一责任人；

(二) 制定安全管理的相应规范、流程和突发事件应急预案，保证比赛筹备和实施工作全过程的安全；

(三) 确保比赛内容涉及的器材、设备符合国家有关安全规定；

(四) 赛项执委会在赛前对本赛项全体裁判员、工作人员、指导老师、参赛选手进行安全培训；

(五) 赛项执委会制定专门方案保证比赛命题、赛题保管、发放、回收和评判过程的安全；

(六) 赛项执委会在赛前组织专人对比赛现场、住宿场所和交通保障进行考察，并对安全工作提出明确要求。赛场的布置，赛场内的器材、设备，应符合国家有关安全规定，组织模拟测试，排除安全隐患；

(七) 赛场周围设立警戒线，防止无关人员进入，发生意外事件。比赛现场内参照相关职业岗位的要求为选手提供必要的劳动保护和医务服务；

(八) 承办院校应提供保障应急预案实施的条件，明确制度和预案，并配备急救人员与设施；

(九) 赛项执委会会同承办院校制定开放赛场和体验区的人员疏导方案。赛场环境中存在人员密集、车流人流交错的区域，除了设置齐全的指示标志外，增加引导人员，并开辟备用通道；

(十) 大赛期间，赛项承办院校须在赛场设置医疗医护工作站；在管理的关键岗位，增加力量，建立安全管理日志。比赛期间安排的住宿地应具有宾馆、住宿经营许可资质，保证住宿、卫生、饮食安全等；

(十一) 比赛期间发生意外事故时，发现者应第一时间报告赛项执委会，同时采取措施，避免事态扩大。赛项执委会应立即启动预案予以解决并向赛区执委会报告。

**十五、经费概算**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **费用类别** | **项目** | **金额**  **（万元）** | **备注** | |
| 赛项研讨论证、赛题开发及培训预算 | 竞赛方案研讨论证会议组织 | 5 | 研讨会专家的用餐、论证费等 | |
| 竞赛试题开发 | 10 | 专家封闭开发住宿、用餐等 | |
| 印刷费 | 2 | 大赛通知、赛程、竞赛文档、赛题等 | |
| 培训费 | 1 | 裁判员培训费用 | |
| 专家 | 3 | 包括命题、评审、裁判等环节的专家费用 | |
| 赛项组织预算 | 场地布置 | 8 | 根据比赛要求布置场地、布线、主席台搭建等 | |
| 设备运输、安装、调试 | 6 | 比赛设备运输及安装等 | |
| 现场技术支持 | 3 | 竞赛现场支持 | |
| 赛项宣传费用 | 5 | 赛场环境设计与制作、宣传材料制作，平面媒体、网站宣传维护等 | |
| 服装费 | 4 | 选手、指导老师、裁判、监考、工作人员、志愿服装费 | |
| 获奖奖励 | 4 | 获奖人员奖励、奖品和纪念品等 | |
| 餐费、交通费 | 6 | 领导、专家、选手在津食、交通费用、工作人员餐费 | |
| 预留资金 | 3 | 处理赛事突发事件 | |
| 总计 | | 60 | |  |

**十六、比赛组织与管理**

经大赛执委会批准，成立赛项执行委员会、赛项专家组，落实赛项承办院校

(一) 赛项执委会：全面负责本赛项的筹备与实施工作，接受大赛执委会领导，接受赛项所在分赛区执委会的协调和指导。赛项执委会的主要职责包括：领导、协调赛项专家组和赛项承办院校开展本赛项的组织工作，管理赛项经费，选荐赛项专家组人员及赛项裁判与仲裁人员等；

(二) 赛项专家组：在赛项执委会领导下开展工作，负责本赛项技术文件编撰、赛题设计、赛场设计、设备拟定、赛事咨询、技术评点、赛事成果转化、赛项裁判人员培训、赛项说明会组织等竞赛技术工作；同时负责赛项展示体验及宣传方案设计；

(三) 承办院校：在赛项执委会领导下，负责承办赛项的具体保障实施工作，主要职责包括：按照赛项技术方案要求落实比赛场地及基础设施，赛项宣传，组织开展各项赛期活动，参赛人员接待，生活服务，比赛过程文件存档等工作，赛务人员及服务志愿者的组织，赛场秩序维持及安全保障，赛后搜集整理大赛影像文字资料上报大赛执委会等。赛项承办院校按照赛项预算执行各项支出。承办院校人员不得参与所承办赛项的赛题设计和裁判工作；

(四) 现场裁判、仲裁、监督组：开赛前一周，在裁判员库、仲裁员库、监督员库中随机抽取组成。裁判组负责赛前检查及赛场鉴定、现场执裁和评审比赛结果等工作；仲裁组负责受理各参赛队的书面申诉、对受理的申诉进行深入调查，做出客观、公正的集体仲裁；监督组对指定赛区、赛项执委会的竞赛筹备与组织工作实施全程现场监督，包括赛项竞赛场地和设施的部署、选手抽签、裁判培训、竞赛组织、成绩评判及汇总、成绩发布、申诉仲裁、成绩复核等；

(五) 协办企业：提供竞赛现场设备并设置技术保障组，为竞赛设备、软件与竞赛设施提供保障服务。

**十七、教学资源转化建设方案**

为了更好的将信息安全技术应用于工业互联网，推动工业互联网的蓬勃发展，本竞赛项目组将通过技能竞赛助力于院校的专业建设、教材编写、教学资源、师资队伍、校企合作、国际合作等方面，在赛后持续开展实施大赛成果转化方案：

(一) 专业建设。根据行业发展情况修订“信息安全与管理”、“物联网技术应用”专业课程库，确定课程库中每门课程编写课程标准，为学校建设“信息安全与管理”及“物联网技术应用”专业提供课程指导；在“信息安全与管理”、“物联网技术应用”专业课程库基础上，按职业教育专业建设标准流程，为“信息安全与管理”、“物联网技术应用”专业在工业互联网安全等方向上，分别提出新的专业建设方案、课程体系和教学计划；

(二) 教材编写。在2018年赛项组织期间，计划联合优秀院校，编写《物联网安全导论》、《物联网安全技术及应用》、《工业控制系统安全技术及应用》等三本教材，并计划于2019年底出版发行，供开设“信息安全与管理”、“物联网技术应用”等专业的学校使用；2018年赛项结束后半年内，在“工业互联网安全技术与应用”赛项各省赛、国赛所用试题的基础上，编写《工业互联网安全技术与应用赛题汇编》，为各学校做大赛准备、学校“工业互联网安全技术与应用”技能考试提供有效的支撑；

(三) 教学资源。2018年赛项结束后半年内，提供《工业互联网安全技术与应用综合实训》实训指导书、课件和操作视频，提供《工业互联网安全技术与应用大赛试题汇编》讲解视频，在应用层面上为学校教学提供丰富的教学资源。

(四) 组织推广。赛后持续召开工业互联网安全技术与应用大赛成果专题研讨交流会。在研讨会上，由获得作为示范推广的指导教师或学生介绍大赛成果，包括本赛项资料文本、音视频、图片成果等，围绕着工业互联网安全技术与应用大赛成果交流学习的体会，分组展开研讨，提出进一步深入研究的做法、建议。使大赛成果深入人心，使大赛成果在院校得以有效推广应用。

(五) 师资队伍。赛后持续借助工业互联网安全技术培训的有效方式推广成果。由院校与企业共育相关专业师资，借助师资培训的机会，推广大赛的成果；促进相关课程的人才培养模式创新。

(六) 校企合作。加强与行业企业合作，让大赛成果走近行业。注重大赛成果向行业转化，把大赛成果与行业应用紧密对接，转化为可在实际工程案例中实施的实际工业互联网安全应用项目，产生直接的经济效应和社会效应。

(七) 国际合作。让大赛成果走出国门，接受更大的挑战。推荐优秀的大赛成果参与国际性的比赛，切实推动我国工业互联网安全领域的国际性发展。

**十八、筹备工作进度时间表**

依据大赛组委会安排，项目在核定后在两个月时间之内，组织行业、企业专家和院校代表完成竞赛规程的完善修订工作，筹备工作时间进度表如下。

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **筹备阶段** | **内　容** | **时间安排** |
| 1、 | 项目筹备 | 组建赛项专家组、赛项技术工作团队，开展赛项准备和筹备工作，确定竞赛设备技术标准和规范 | 2017年3月~2018年7月 |
| 2 | 申报、立项 | 赛项设计专家研讨会，完成赛项申报方案 | 2017年8月 |
| 确定赛项 | 2017年10月 |
| 成立赛项执委会、领导小组和相应的工作组 |
| 3 | 赛前准备 | 赛项专家会议3-5轮次会议，确定赛项规程、样题、赛项技术方案、赛场方案、体验环节设计方案、开放方案、宣传方案、教学资源转化方案、赛事安全规章、突发事件应急预案等 | 2017年11月～2018年 1 月 |
| 确定分赛区及承办校 | 2018年1月 |
| 公开样题，召开全国赛项说明会 | 2018年2月 |
| 命题专家组会议，赛题开发、确定竞赛题库 | 2018年1月～2月 |
| 赛项预报名及报名完成 | 2018年2月～4月 |
| 4 | 比赛阶段 | 比赛设备安装、调试，赛场布置、同期技术展示、体验和活动现场布置；赛项指南印刷、选手服装制作 | 2018年5月～6月 |
| 专家组题库审核，确定评分标准及抽题 |
| 成立裁判组、仲裁组、监督组；培训并验收赛场 |
| 正式比赛、同期技术展示、体验和活动举办；竞赛成绩提交、竞赛过程文档提交、教学资源转化成果与赛项总结 |
| 5 | 项目总结 | 竞赛项目总结 | 2018年7月～8月 |
| 6 | 资源转化 | 围绕本竞赛项目的相关教学成果研讨会及展示等相关活动 | 2018年10月～12月 |

**十九、裁判人员建议**

根据《全国职业院校技能大赛专家和裁判工作管理办法》，由高校、行业企业专家共同组成裁判组，赛项合作企业不得参与评分。裁判员从裁判库中抽取，要求：身体健康，年龄一般在60周岁以下，具有良好的职业道德，坚持原则，作风正派，认真负责，廉洁公正，从事电子信息类、计算机类、信息安全类等专业工作或教学5年以上。竞赛期间，赛项裁判组设裁判组组长1名，检录及一次加密裁判1名，现场裁判7人，评分裁判10人，裁判总人数20人。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **专业技术方向** | **知识能力要求** | **执裁、教学、工作经历** | **专业技术职称**  **（职业资格等级）** | **人数** |
| 1裁判长 | 信息安全、网络安全、计算机网络、计算机应用方向 | 熟悉网络基础以及windows和linux操作系统，熟悉网络安全、物联网安全、工控安全类别和主要攻防手段 | 5年以上信息安全、计算机专业教学经历、至少3次电子信息类赛项执裁经验 | 教授、研究院级高级工程师 | 1 |
| 2现场裁判 | 信息安全、网络安全、计算机网络、计算机应用方向 | 熟悉网络基础以及windows和linux操作系统，熟悉系统加固及安全评估流程，熟悉网络安全、物联网安全、工控安全主要类别和主要攻防手段，熟练调试主流网络设备 | 5年以上信息安全、计算机专业课程教学经历 | 工程师、高级工程师、副教授、教授 | 7 |
| 3评分裁判 | 信息安全、网络安全、计算机网络、计算机应用方向 | 5年以上信息安全、计算机专业课程教学经历 | 工程师、高级工程师、副教授、教授 | 10 |
| 4加密裁判 | 信息安全、网络安全、计算机网络、计算机应用方向 | 3年以上信息安全、计算机专业课程教学经历 | 工程师、高级工程师、副教授、教授 | 2 |
| **裁判总人数** | 20 | | | | |

**二十、其他**

专职联络人员

手机号码

邮箱

专职联络人员具有强烈的工作责任感和良好的保密意识。