CAICT 中国信通院

2020全国行业职业技能竞赛——全国工业互联网安全技术技能大赛技术方案

2020年9月

大赛目的

为深入实施工业互联网创新发展战略，大力培育高素质网络安全技术技能人才队伍，加快推进工业互联网安全保障体系建设，弘扬精益求精的工匠精神，工业和信息化部、人力资源社会保障部、中华全国总工会、共青团中央决定共同举办“2020年全国工业互联网安全技术技能大赛”。

1、通过职业技能大赛的形式，检验考察我国工业互联网安全职业人员与相关专业在校学生在工业互联网安全测试、评估、防护和场景实操等方面的技能水平，为工业互联网安全行业企业、系统集成商和应用企业储备急需的岗位人才和后备人才，选拔培养高水平、高技能工业互联网安全队伍。

2、引领促进工业互联网安全技术创新和融合应用，强化工业互联网安全领域自主安全能力，汇聚培育一批本土工业互联网安全龙头企业和产品服务供应商；

3、促进工业互联网安全职业技能标准建设，引导工业互联网安全专业教育、技能培训和职业建设，促进人才培养和产业对接模式的改革创新，建设完善工业互联网安全人才培育体系；

4、综合展现参赛队伍的专业风采，汇聚展示工业互联网安全政策、技术、产业发展成果，持续建设完善工业互联网安全产业生态。

目录

1

大赛赛程及说明

1.1 命题原则

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，坚持四个命题原则：

1、聚焦当前工业互联网跨行业、跨领域融合和新技术应用的发展趋势；

2、立足工业互联网安全领域高技能人才选拔和工程技术人员培养的长期目标；

3、强化职业技能和技术应用要求，考察工业互联网安全的测试、评估、运维、保障等核心技术技能；

4、重点突出岗位专业技能培养、行业场景实操和新技术应用创新等高素质、综合能力选拔，突出技术创新、技能考核和工匠精神要求。

1.2 竞赛内容

（一）竞赛内容：

竞赛由理论知识考试和技能操作考核两部分组成。其中，理论知识占 20%，技能操作占 80%。竞赛内容紧密结合企业生产实际场景和工业互联网安全技术应用发展状况，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、保障以及完成指定任务的理论和技术水平。

具体赛程及要求由大赛组委会办公室另行通知。

1.3 竞赛分组及报名

（二）竞赛分组

竞赛分为职工组、教师组和学生组，各组别均为三人团体赛。

1.职工组：具有工业互联网安全技术应用相关工作经历的企业在职人员。

2.教师组：具有工业互联网安全技术应用相关工作经历的高等院校、职业学校（含技工院校，下同）在职人员。

3.学生组：高等院校、职业学校相关专业全日制在籍学生。

（三）报名条件

1.思想品德优秀；

2.具备较高的工业互联网安全技术技能水平；

3.学习能力较强，身体素质好；

4.具备较好的心理素质和较强的应变能力；

5.已获得“中华技能大奖”“全国技术能手”荣誉及在2019年国家级一类大赛获得前 5名（双人赛项前3名、三人赛项前2名）、国家级二类竞赛获得前3名（双人赛项前2名、三人赛项第1名）且为职工身份的人员，不得以选手身份参赛。

1.4 竞赛方式

（四）竞赛方式及名额

大赛分选拔赛（预选赛）和决赛两个阶段。

- 预选赛和决赛在大赛组委会领导下，由大赛组委会办公室具体组织实施。

- 选拔赛由省（区、市）及新疆生产建设兵团工业和信息化主管部门、人力资源社会保障厅（局）、工会、团委以及地方通信管理局等相关单位联合组织实施。举办选拔赛的省（区、市）及新疆生产建设兵团选派7支队伍（职工组3支，教师组2支，学生组2支）参加决赛。不具备举办选拔赛条件的省（区、市）及新疆生产建设兵团可组织参赛队伍参加预选赛。此外，本次大赛拟邀请部分国有重要骨干企业独立举办选拔赛，举办选拔赛的企业可选派2支队伍参加决赛，不具备举办选拔赛条件的企业可组织参赛队伍参加预选赛。

- 选拔赛由各省相关部门及各相关企业自愿组织举办。所有参赛队伍可自主选择参加选拔赛或官方统一预选赛，也可同时参加。

2

比赛内容及规则

1. 预选赛

大赛预选赛为线上平台竞赛，采用大赛统一技术平台进行比赛，全程赛时8小时，竞赛内容分为理论和实操两部分，预选赛成绩中理论考试占20%，实际操作占80%。

- ✓参赛队伍为不超过3人的比赛团队，每队可另设一名领队，领队不参加比赛。参赛队员均须为无违法犯罪记录的中华人民共和国合法公民，并进行实名注册。
- ✓大赛报名采取官方网站线上报名形式，线上报名9月5日10:00开始，10月10日17:00截止。
- ✓参赛队伍组队并报名成功后，参加比赛直到竞赛结束期间，不得更换或增加队员。
- ✓预选赛将从职工组选拔40支队伍、教师组选拔20支队伍、学生组选拔20支队伍，共80支队伍进入决赛。

1.1 预选赛——理论考试

- 比赛时间：10月24日
- 比赛内容：

理论考试采用单选、多选、判断的答题方式，主要考核参赛选手对网络安全及工业互联网安全相关政策法规、基础知识的掌握情况以及技术应用水平。考点范围涉及政策法规、工业互联网、安全防护、安全运维、移动安全、网络安全、数据库安全、云安全、密码学等方面。

- 比赛形式

每个竞赛团队限定队长账号答题，打开试卷作答并提交答案。

每个竞赛团队抽取试卷和题目不同，题目由竞赛平台按照30%变动比例自动生成。

每道题根据难度不同设置答题时限，超时后答题自动提交，不计分，跳转下一题。

理论考试总时长90分钟，超过90分钟后自动交卷，理论考试结束后平台自动判分。

1.1 预选赛——理论考试

- 计分方式：

每个竞赛团队理论题共100题，满分500分。单选题40道，每题5分，多选题20道，每题10分，判断题40道，每题2.5分。答对获得相应分数，答错不扣分。考试时间结束之前可以随时在线交卷，交卷后无法修改答案。

队伍理论题得分=答题者得分/500*100% （保留小数点后2位）

- 注意事项：

断网、掉线、关闭页面、退出平台登陆等事件不影响计时。

请保持网络畅通，并在考试期间认真答题。

1.1 预选赛——理论考试

理论题样题示例：

1、关于工业互联网工控协议Modbus协议的安全缺陷，哪一项是错误的（）

A、没有认证机制　B、没有终端加密　C、没有数据加密　D、没有消息检验

答案：B

2、以下哪项属于设计阶段风险评估应着重考虑的内容（ ）

A、设计方案是否符合业务建设规划，并得到最高管理者的认可
B、设计方案是否采取了一定的手段来应对业务可能的故障
C、设计方案是否考虑可能随着其他业务接入而产生的风险
D、业务性能是否满足用户需求，并考虑到峰值的影响，是否在技术上考虑了满足业务性能要求的方法

答案：ABCD

1.1 预选赛——场景实操

- 比赛时间：10月24日 9:00--17:00
- 比赛内容：以工业互联网场景为答题环境，通过夺旗解题方式，考核选手在工业互联网安全领域知识和技能应用水平，重点涉及人工智能、区块链、5G、密码破解、渗透测试、工控设备漏洞、工控设备协议分析、云安全、溯源分析等方面。
- 比赛方式：
- 以团队为单位的夺旗赛模式，赛题以工业互联网场景为环境，预设典型安全漏洞，并在环境内置一个以“flag”开头的特殊字符串（通称“flag”）作为答案。
- 在比赛时间内，所有参赛团队成员都可以反复提交答案（flag），只以第一次正确提交flag为正确解出题目。此后再重复提交不得分。

1.1 预选赛——场景实操

- 计分方式：
- 每道题根据题目设置500分的初始分值，根据正确解题的战队数量分数发生动态衰减。赛题分值衰减会同步影响所有已经解出题目的队伍得分。
- 队伍场景实操得分=比赛时间内队伍成员得分之和/本场比赛团队最高得分*100%（保留两位小数）
- 注意事项：
- i. 比赛时，答题页面左上角会显示每队唯一的战队标识（战队token），任何情况下，请妥善保护好战队token、容器地址等战队唯一标识信息，一经泄露会被判定为作弊。
- ii. 比赛结束后，所有参赛队伍需通过平台提交解题思路文档（通称“WRITEUP”，简称“WP”）。不提交WP、WP不完整、WP与战队解题事实不符以及WP和其他战队雷同的情况，都会被视为作弊。
- iii. 比赛期间请注意查看是否收到大赛裁判组电话（以官网或平台公告号码为准），无特殊原因不接、漏接、或无法通话都将被视为作弊。

1.1 预选赛——场景实操

比赛涉及知识内容：

工业控制系统安全	DCS、PLC等工控设备漏洞利用
	上位机软件、实时数据库等的漏洞利用
	工业协议分析
	工控程序设计
	工控程序逆向
工业互联网平台安全	平台数据泄露而被恶意利用
	平台各组件（docker、K8S等）漏洞利用
	平台与底层设备通信安全
智能终端设备安全	摄像头漏洞利用及协议分析
	数采网关漏洞利用及协议分析
	路由器、打印机等设备的漏洞利用及协议分析
	终端设备漏洞挖掘
人工智能安全	AI算法自身的漏洞分析利用
	利用AI算法自动漏洞挖掘
	AI图像识别训练
	AI学习框架组件漏洞、引入第三方依赖库带来的漏洞分析利用

1.1 预选赛——场景实操

比赛涉及知识内容：

区块链	日食攻击（eclipse attack）利用
	The DAO漏洞分析利用
	Parity多重签名钱包合约漏洞分析利用
	以太坊短地址漏洞分析利用
	以太坊编程语言Solidity漏洞分析利用
5G	算法模型分析
	仿5G协议应用程序分析
其他相关知识点	渗透测试：多以web形式，以工业场景为背景，如能源管理系统、WEB SCADA系统等。
	密码学
	……

1.1 预选赛——场景实操

场景实操题样题示例：

PLC固件分析

考点：考察参赛选手利用逆向技术对工业程序进行分析并提取有用信息的能力

解题步骤：

（1）利用固件分析工具获取固件所使用的操作系统信息；

（2）利用反汇编工具获取后门账号信息及程序中所使用的加密算法；

（3）运行解密算法获取登陆密码。

```
root@ubuntu:/home/        /Desktop# binwalk chall.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
901           0x385           Zlib compressed data, default compression
```

```
ROM:00205B30 aPasswordS:     .string "-----> Password: %s <-----\n"
ROM:00205B30                                         # DATA XREF: sub_299F0+1E4↑o
ROM:00205B30                                         # sub_299F0+1E8↑o
ROM:00205B30                 .byte 0
ROM:00205B4C aN0tnsab4ckd0or:.string "N0tNsAb4ckD0or0r" # DATA XREF: sub_299F0+208↑o
ROM:00205B4C                                         # sub_299F0+20C↑o
ROM:00205B4C                 .byte 0
ROM:00205B5D                 .byte 0, 0, 0
ROM:00205B60 aYbz99sbrd:     .string "ybz99SbRd"     # DATA XREF: sub_299F0+210↑o
ROM:00205B60                                         # sub_299F0+214↑o
ROM:00205B60                 .byte 0
ROM:00205B6A                 .short 0
ROM:00205B6C                 .long 0, 0, 0, 0, 0, 0
ROM:00205B84 dword_205B84:   .long 0, 0, 0, 0, 0, 0, 0, 0 # DATA XREF: sub_29F1C+204↑o
ROM:00205B84                                         # sub_29F1C+208↑o ...
ROM:00205B84                 .byte 0x53 # S
ROM:00205B85 aEe9cb9y99:     .string "ee9cb9y99"
ROM:00205B85                 .byte 0
ROM:00205B8F                 .byte 0
ROM:00205BB0 aNoe_root_task: .string "NOE_Root_Task" # DATA XREF: sub_299F0+328↑o
ROM:00205BB0                                         # sub_299F0+32C↑o
```

```
    char *out                                   /* encrypted string */
    )
    {
    int           ix;
    unsigned long  magic      = 31695317;
    unsigned long  passwdInt = 0;

if (strlen (in) < 8 || strlen (in) > 40)
    {
errnoSet (S_loginLib_INVALID_PASSWORD);
    return (ERROR);
    }

for (ix = 0; ix < strlen(in); ix++)          /* sum the string */
    passwdInt += (in[ix]) * (ix+1) ^ (ix+1);

sprintf (out, "%u", (long) (passwdInt * magic)); /* convert interger
                                                    to string */
/* make encrypted passwd printable */

for (ix = 0; ix < strlen (out); ix++)
    {
    if (out[ix] < '0')
        out[ix] = out[ix] + '1';     /* arbitrary */

    if (out[ix] < 'A')
        out[ix] = out[ix] + 'A';     /* arbitrary */

    if (out[ix] < '9')
        out[ix] = out[ix] + '8';     /* arbitrary */
    }

return (OK);
```

```
password:1G0AT42ET5 to hash:cQwwddSRxS
password:Q6kL8A2Y52 to hash:cQwwddSRxS
password:CHd88CCN35 to hash:cQwwddSRxS
password:BZ4APB45W3 to hash:cQwwddSRxS
password:3CAkq501F1 to hash:cQwwddSRxS
password:IYMeD5F01D to hash:cQwwddSRxS
password:5FHHGX041I to hash:cQwwddSRxS
password:eGay244D76 to hash:cQwwddSRxS
password:TbGUTU0329 to hash:cQwwddSRxS
password:PmG8ICBM51 to hash:cQwwddSRxS
password:01nA5GCR32 to hash:cQwwddSRxS
```

2. 选拔赛

选拔赛分为地方选拔赛和国有骨干企业选拔赛。计划举办选拔赛的单位需于9月25日前向大赛组委会办公室报备选拔赛举办意愿及相关信息，10月15日前向大赛组委会办公室提交组织方案、报名名单，10月23日前完成赛事组织工作并提交比赛结果和决赛晋级名单。

选拔赛具体要求及晋级名额详见《2020年全国工业互联网安全技术技能大赛选拔赛组织方式及报送规则》。

3. 决赛

决赛采用理论考试+场景实操赛制模式，职工组、教师组、学生组分组同时进行。参赛选手首先参加理论考试，随后是实操环节。实操环节的比赛环境包括靶场平台和多个工业场景。每个参赛队拥有一套独立的靶场环境，参赛队根据在靶场环境中攻破考点的情况得分，累积到一定分数后，即可获得一次工业场景选择权，随后便可在工业场景中进行渗透。决赛详细规则将在官网另行发布。

场景示例： 工业机器人5G物联网智能生产线场景

- 该产线根据实际工程场景，由三台工业机器人和配套的工业流水线为基础模型，通过现场数据采集模块将各个机器人的运行数据进行采集利用5G传输模块通过互联网传输到各个数据接收终端。
- 其中包括负责分析机器人现场工作运行情况的机器人群管控监控系统负责产品生产管理的MES系统负责订单管理财务核算的ERP系统整个系统采用云服务器的方式与现场生产线实时进行数据交互，通过机器人的数据分析精确的计算和分析实际生产运行的情况，形成一套完整的制造业智能化生产线的最小系统，实现了物联网情境下的设备与信息的深度融合。

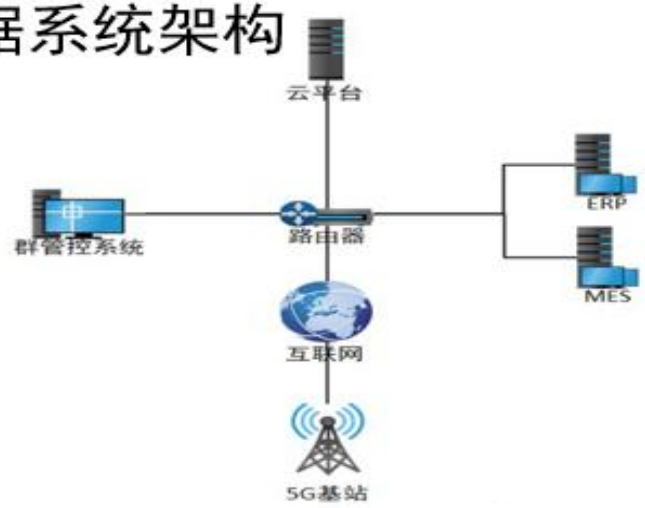
3. 决赛

场景实例：工业机器人5G物联网智能生产线场景

数据分析

接单评估
订单交期
生产计划
采购计划
作业计划
产能挖掘

数据系统架构



交互屏幕显示

人脸识别权限系统

伺服生产流水线

3. 决赛

场景内容：

- 该产线根据实际工程场景，由三台工业机器人和配套的工业流水线为基础模型，通过现场数据采集模块将各个机器人的运行数据进行采集利用5G传输模块通过互联网传输到各个数据接收终端。系统包括负责分析机器人现场工作运行情况的机器人群管控监控系统、负责产品生产管理的MES系统、负责登录执行操作的人脸识别系统等。整个系统采用云端与现场生产线实时进行数据交互的方式，通过机器人的数据分析精确的计算和分析实际生产运行的情况，实现了物联网情境下的设备与信息的深度融合。

赛题内容：

- 赛题内容主要涉及云计算服务器漏洞、主机人脸识别系统漏洞、工控设备（PLC）协议分析、工控设备（PLC）漏洞利用、工控设备（PLC）程序控制等。

3

大赛赛项保障

3.1 评分标准和原则

依据参赛选手完成的情况实施综合评定。

评定依据全国工业互联网安全技术技能大赛技术方案中明确的技术规范，按照技能大赛技术裁判组制定的考核标准进行评分，全面评价参赛选手职业能力的要求，本着“科学严谨、公正公平、可操作性强、突出工匠精神”的原则制定评分标准。

3.2 运维保障

- 线上赛-烽火台反作弊系统
- 为保证比赛的公平性，CTF团队竞技平台采用烽火台反作弊系统，主要作用是监控比赛过程中的异常行为，譬如ip频繁变化、答题时间异常、Flag集中提交、相同Flag等信息，并向裁判和系统管理员发起警报，同时记录异常日志，为参赛选手提供一个公平、公正的比赛环境。

- 线下赛-现场运维保障
- 1.比赛过程中的全部操作均提供日志纪录，通过日志纪录可以进行比赛过程追溯；

2.比赛过程中将有现场监审组成员针对比赛平台的运行情况进行监管管理，确保平台运行和操作符合“公正”、“公平”、“公开”的比赛精神；

3.比赛过程中比赛后台及后台相关操作将进行全程视频录制，相关视频记录由大赛工作组统一管理。

3.3 申诉与仲裁

比赛过程中存在两种判罚行为

（一）平台自动判罚：烽火台反作弊系统的反作弊算法及机制已经过组委会专家及裁判组审计，根据监控比赛过程中的异常行为，进行自动判罚，此类判罚以平台判罚为准，不接受申诉。

（二）在比赛过程中或比赛结束后，若出现有失公正或有关人员违规等现象，代表队队长可在比赛结束后2小时之内向大赛工作组提出正式的书面申诉，大赛工作组在接到申请后的2小时内反馈受理，并以大赛工作组的仲裁结果为最终结果。

CAICT 中国信通院

国家高端专业智库 产业创新发展平台

谢谢！