

“中控杯”智能制造挑战赛组委会

组委会函字〔2026〕10号

赛题4“工控信息安全攻防演练”

决赛赛题发布及决赛通知

一、决赛基本信息

参赛对象：初赛晋级的参赛队伍

决赛地址：杭州白马湖国际会展中心

决赛报到：所有参赛选手须于2026年8月18日16:00前至杭州白马湖建国饭店完成报到，未按时完成报到的会影响参赛资格审核。

决赛时间：2026年8月19日-2026年8月20日

决赛形式：夺旗赛+攻防对抗

决赛平台：决赛现场通知

二、赛题说明

本次决赛赛题聚焦工业控制系统漏洞挖掘，围绕“工控信息安全攻防演练”开展综合竞技。组委会依托工控软硬件仿真靶场环境，搭建贴合电力、石化、供水等主流流程工业的工控网络场景，覆盖PLC、HMI、工业以太网、工控组态系统等核心工业设备与网络架构。参赛队伍需基于工控设备运行机制、工业网络通信协议、工控系统漏洞机理及安全防护规范，自主完成资产测绘、漏洞挖掘、点位篡改、设备加固、安全应急处置等全流程实战操作。

（一）比赛形式

本次决赛整体赛程分为第一阶段工控夺旗赛（8月19日下午）、第二阶段攻防排位赛（8月20日一整天）两大考核环节，全赛程聚焦工业控制系统安全攻防场景。

1. 工控夺旗赛：依托工控网络靶场，采用夺旗CTF模式，所有参赛队伍在决赛现场通过电脑远程登录工控网络靶场平台，完成题目解题、Flag提交操作；依据夺旗赛总成绩排名，选取前4支队伍晋级攻防排位赛。

2. 攻防排位赛：基于实训台竞技，采用实物PLC、HMI工控设备搭建对抗环境；4支晋级队伍互为攻防双方，同步开展现场实操、漏洞挖掘、系统加固、应急处置综合比拼，兼顾理论分析、组态调试、实物设备实操能力。

（二）比赛内容

1. 工控夺旗赛：深度贴合工业现场场景，设置工控实物类赛题，选手通过工控网络靶场平台的虚拟机远程访问实物PLC完成答题，题型包含资产识别、点位读写、PLC组态逻辑分析等；每个队伍成功提交对应Flag即可获得题目分值，工控夺旗赛以队伍总积分作为排名依据。

2. 攻防排位赛：每支队伍独立部署一套实物PLC+HMI成套工控平台，搭载模拟生产工艺参数、设备配置文件、控制程序逻辑等核心考核信息；不设置固定Flag标识，依托资产识别、设备操控、工艺干预等实战任务进行综合计分。赛事采用排位赛机制：

- (1) 赛前抽签确定两组对阵队伍，开展首轮的两场攻防对抗；
- (2) 两场对抗结束后进入下一轮竞赛，获胜队伍晋级冠亚军争夺战，未晋级队伍进入三、四名争夺战；
- (3) 每场攻防对抗期间，每支队伍同时承担攻击、防守双重职责：一方面保障己方工控设备持续稳定运行、参数不被篡改、业务流程不间断；另一方面挖掘对手 PLC/HMI、仿真系统漏洞，通过完成资产识别、点位篡改、设备控制等攻防任务获取对应任务分值。



(三) 评分指标

决赛考核评分指标如下，具体评分细则待后续发布。

1. 工控夺旗赛评分标准：

采用纯客观题评分模式，由工控网络靶场平台自动判分；每道题对应固定分值，提交正确 flag 后自动加分，错题不扣分，得分实时累计，最终以总得分作为评比依据。

2. 攻防排位赛评分标准：

(1) 每场攻防对抗赛设置固定总分，裁判严格依据赛前公示评分细则量化打分。

(2) 攻击得分：攻击方成功完成指定攻击目标（如成功利用漏洞、植入后门、修改关键控制变量、设备操控等）可获得相应任务分值；

(3) 防守得分：因攻击成功导致 PLC 停止运行、HMI 异常、关键控制变量被篡改、工业网络通信中断等情况的，按照评分细则扣减相应防守分值；成功发现攻击行为、识别攻击路径、定位攻击源、排查并清除后门、完成系统恢复，或有效利用工业审计日志完成攻击溯源并提交完整分析报告，经裁判组确认后，奖励分值为对应防守扣分值的 50%。

(4) 参赛队伍须保障 PLC 与 HMI 通信正常、不干扰模拟生产正常业务；严禁擅自关闭业务端口、通过白名单全盘拦截合法业务流量，违规一经查实按评分细则予以扣分。

(5) 每场比赛以各队伍综合得分确定比赛胜负。

三、 决赛流程

(一) 准备阶段

1. 上位机组态软件发放

大赛组委会将于 8 月 1 日提供上位机软件下载地址，同步提供配套使用教程及相关学习资料，供各参赛队伍熟练掌握软件操作方法、熟悉上位机操控流程，完成赛前适配准备工作。

（二）现场决赛阶段

2. 选手入场

8 月 19 日所有参赛选手，在规定时间内根据会场指示牌到达决赛会场（杭州白马湖国际会展中心），并按照工作人员指引，到指定位置落座。每个参赛选手需自备一台笔记本电脑。

3. 身份核验

所有参赛选手均需携带报到时发放的参赛证件、身份证。组委会巡查员将在赛前对参赛选手身份进行核验，参赛选手身份与报名身份不一致的将不允许参赛。

4. 工控夺旗赛

1) 赛前准备（30 分钟）：参赛队伍登录工控网络靶场平台，核对账号密码，基础流程、答题操作规范与初赛完全一致。

2) 比赛期间（3 小时）：平台实时监控参赛队伍操作行为，记录操作日志；实时统计各队伍得分，自动更新排名；参赛队伍可随时提交 flag，提交正确后自动加分，错题不扣分。

3) 赛后期间：平台关闭 flag 提交通道，自动生成最终得分排名；工作人员核查操作日志，排查作弊行为，确认排名有效性；裁判组复核成绩后公示前 4 支晋级攻防排位赛名单。

5. 攻防排位赛

1) 赛前准备（30 分钟）：按赛程安排组织 4 支队伍统一抽签确定对阵顺序；各队伍进入专属竞赛区域，核对电脑、实物 PLC/HMI、内网网络环境；工作人员完成设备、网络、靶标环境初始化检查，确认无异常后裁判宣布本轮比赛正式开始。

2) 首轮第一场攻防对抗（1 小时）：比赛开始后，对阵双方同时承担攻击与防守职责。各队伍需要实时监控己方 PLC、HMI 工控设备，及时修补漏洞、调整防护策略、处置入侵、修复篡改数据，保障系统稳定运行。同时在合规范围内挖掘对方漏洞，开展漏洞利用、数据窃取、逻辑篡改等攻击操作。比赛过程中，各队伍应完整记录攻击、防守过程及相关操作细节。

3) 中场休整阶段（1 小时）：首轮第一场对抗结束后，同步完成三项工作：参赛队伍须提交攻防报告。报告内容包括但不限于攻击过程、漏洞利用方法、攻击效果、防护策略、防火墙配置调整、工业审计日志分析、攻击事件处置等。未按规定时间提交报告的，视为主动放弃本轮报告评分；裁判组同步审阅队伍提交的攻防报告，并核对本场比赛设备运行数据、攻防操作记录；工作人员统一完成竞赛环境复位，全面恢复初始竞赛状态，保障下一场比赛顺利进行。

4) 首轮第二场攻防对抗（1 小时）：休整 1 小时结束后，开启首轮第二组队伍的攻防对抗赛，比赛规则、操作要求、计分标准与首轮第一场完全一致。

5) 第二轮排位赛：首轮两场对抗全部结束、成绩核算完毕后，按照既定规则晋级的队伍，依次开展冠亚军争夺战、三四名争夺战，单场对抗时长、赛前准备、报告提交、环境恢复流程均沿用上述统一时长标准。

四、排名规则

前四名由攻防排位赛评定，其余队伍最终排名与奖项均以夺旗赛成绩评定。

五、公正竞赛说明

参赛队伍须严格遵守以下规定，违规者将取消参赛资格或竞赛成绩：

1. 比赛过程中，不得实施与竞赛无关的攻击行为，不得恶意破坏平台、设备及赛题内容，违者直接取消竞赛资格。
2. 禁止作弊行为，包括但不限于：串通答题、共享赛题答案及 flag、使用非法工具解题、伪造答题成果等，一经发现，取消参赛队伍的成绩及参赛资格，情节严重的纳入赛事黑名单。
3. 其他未明确但明显影响公平性的行为：由组委会评议后裁定。

六、结果及争议处置

1. 结果公布

在 2026 年 8 月 20 日比赛结束后，大赛组委会完成评分统计并公布各赛队的排名。

2. 异议反馈

若对排名或评分有异议，须在 2026 年 8 月 20 日 18:00 前向大赛组委会提交反馈。逾期不再受理。

3. 答复方式

相关异议反馈由大赛组委会商议后予以答复。

预祝各参赛队伍取得优异成绩！

“中控杯”智能制造挑战赛组委会

2026 年 7 月 20 日

发文专用章

