2026 年第二届“中控杯”智能制造挑战赛

工控信息安全攻防演练赛题说明

赛道二：工控实战

赛题 4：工控信息安全攻防演练

一、赛题概述

在工业智能化与数字化转型加速推进的当下，工业控制系统已深度融入能源、交通、制造等国家关键基础设施领域，成为社会运转的核心支撑。然而，随着工业互联网的快速发展，传统封闭的工控环境逐渐开放，面临前所未有的信息安全挑战。从“震网”病毒对物理设施的精确破坏，到勒索软件导致的全厂停产，再到针对电网、供水系统的网络攻击，这些事件警示我们：工控信息安全已超越传统网络安全范畴，直接关系到生产安全、经济命脉、社会稳定乃至国家安全。在此背景下，探索工控系统的新型安全威胁、设计适应高实时性与复杂环境的安全防护方案、培养既懂工业运营又通安全技术的复合型人才，已成为产业升级与国家战略的迫切需求。本赛题旨在引导大学生直面这一重大现实课题，激励创新思维，为守护国家关键基础设施安全贡献智慧与解决方案。

本赛项以培养既懂工业运营又通安全技术的复合型人才为总体目标，引导参赛者直面工控系统面临的新型安全威胁，探索设计适应高实时性与复杂环境的安全防护方案。竞赛采用初赛与决赛两阶段递进形式：初赛依托网络靶场平台，采用线上夺旗赛（CTF）模式，围绕流量分析、组态分析、固件分析、密码学、Web 安全五大技术方向，在虚拟工控环境中完成解题与 Flag 提交；决赛采用线下“攻防对抗”模式，基于工控安全竞赛平台与实物实训台，由两支队伍分别担

任攻击方与防守方，针对实训台的 PLC 与 HMI 设备开展实战攻防，综合考核信息获取、后门植入、漏洞排查、防护修复等实操能力，最终通过攻击与防守报告、裁判评分确定成绩。

二、比赛平台

（一）网络靶场平台

网络靶场平台是面向网络安全人才培养、攻防演练、竞赛评估的一体化仿真训练系统。具体平台部署要求如下：

1. 平台功能：作为面向网络安全人才培养、攻防演练、竞赛评估的一体化仿真训练系统，需通过虚拟化技术、网络仿真技术和云计算技术的深度融合，构建高逼真、可重构、大规模的网络攻击防御演练环境；支持从拓扑设计、环境部署、导调控制到结果评估的全流程管理，可满足 CTF 竞赛、攻防演练等场景需求。

2. 平台架构：采用模块化架构设计，具备强大的资源管理能力和灵活的扩展能力；支持虚拟设备与物理设备的混合部署，可构建包含数千节点的复杂网络拓扑；内置丰富的虚拟机镜像库和网络模板库，支持 KVM、Docker 等多种虚拟化技术，能够快速部署各类工控攻防演练场景。

3. 管理功能：提供完善的导调控制系统，支持实时监控、任务调度、Flag 管理、录屏回放等功能，有效提升演练管理的精细化和智能化水平；具备自动判分、成绩统计、排名生成等功能，满足初赛客观题的评判需求。

4. 部署要求：可提前开放测试权限，供参赛队伍熟悉平台操作。

图 1 网络靶场平台图

（二）实训台

实训台主要用于决赛实物实操环节，构建小型完整的工业控制系统，具体配置如下：

核心配置：配置具有行业典型性的 HMI、工业交换机、PLC、安全防护与审计监测设备，以及小型电机、信号灯等执行机构；配备 1 台计算机作为实训工作站。

三、赛事实施流程

本次赛事分为初赛、决赛两个阶段，初赛前计划开展赛前培训。

（一）初赛阶段

1. 比赛时间：预计在 2026 年 5 月中下旬，具体日程以赛事通知为准。赛事主办方将通过大赛官网发布赛前培训、参赛细则等相关信息。

2. 比赛形式：采用线上夺旗赛（CTF）模式，依托网络靶场平台开展，参赛队伍在虚拟工控环境中进行攻防演练，全程线上完成解题。

3. 参赛要求：参赛队伍需在规定时间内登录网络靶场平台，使用主办方提

供的账号密码进入靶场平台；严格遵守竞赛规则，不得实施与竞赛无关的攻击行为，不得泄露赛题内容、Flag 等相关信息。

4. 比赛内容：赛题设计严格围绕五大技术方向，所有题目均依托网络靶场环境设计，每个技术方向的题目均与工控场景深度结合，具体如下：

（1）流量分析类：赛题提供工控流量数据包（包含正常流量与异常流量），同时新增 AI 相关流量内容，如 AI 模型推理指令、训练数据上传报文等。参赛队伍需通过流量捕获工具，分析流量中的异常数据（如协议篡改、恶意指令、数据泄露），提取隐藏的 Flag；

（2）组态分析类：靶场赛题提供组态文件，组态文件中包含设备联动逻辑、参数配置等核心内容，且隐藏 Flag（可藏于组态联动逻辑的注释、参数配置的加密字段等处）；参赛队伍需通过打开组态文件，分析组态逻辑、核查参数配置、排查组态漏洞（如组态权限漏洞、逻辑错误、参数泄露），提取隐藏的 Flag；

（3）固件分析类：提供相关固件，参赛队伍需通过靶场提供的固件解析工具，完成固件解压、根文件系统提取、代码反编译等操作，挖掘固件中的隐藏漏洞，Flag 直接藏于固件内部（可隐藏在固件的配置文件注释、漏洞函数参数、隐藏分区数据中），选手需通过固件深度分析提取 Flag；

（4）密码学类：结合工控场景的数据加密需求，在靶场的工控数据传输环节（如传感器数据上传、设备指令下发）设置加密数据，参赛队伍需通过靶场提供的加密数据样本，分析加密算法，破解加密数据，获取隐藏的 Flag；

（5）Web 安全类：在靶场虚拟工控上位机中搭建 Web 管理界面并植入 Web 漏洞，参赛队伍利用漏洞获取后台权限，查看或修改工控系统配置并提取基础 Flag；靶场同时提供基于语义检索模型的 AI 交互 Web 界面，界面内置

敏感词黑名单限制，选手需构造合法检索关键词绕过过滤，通过模型语义匹配直接获取隐藏在文档库中的最终 Flag。

5. 任务要求：参赛队伍需基于网络靶场给定的虚拟工控环境，围绕“流量分析、组态分析、固件分析、密码学、Web 安全”五大技术方向，在规定比赛时长内完成所有解题操作，提交的 Flag 由网络靶场平台自动校验、实时判分。

6. 流程细节：

（1）赛前 30 分钟：参赛队伍登录网络靶场平台，核对账号权限，检查虚拟环境是否正常，熟悉赛题列表（仅显示题目名称、技术方向）。

（2）比赛期间：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：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。

（二）决赛阶段

1. 比赛时间：2026 年 8 月中下旬，具体日程以赛事通知为准。

2. 比赛形式：采用“攻防对抗”的模式，基于工控安全竞赛平台，在统一竞赛环境下组织参赛队伍开展现场解题与综合能力比拼；融合虚拟仿真与实物设备，兼顾理论分析与实操能力。

3. 参赛要求：晋级决赛的队伍需按时抵达指定比赛现场，凭参赛凭证入场；严格遵守现场竞赛规则，服从工作人员、裁判的管理；不得携带与竞赛无关的电子设备、资料，不得作弊、串通答题。

4. 比赛内容：竞赛核心目标是针对实物设备平台部署的 PLC 设备与 HMI

设备，两者关联存储关键信息（含 Flag、生产参数、设备配置、程序逻辑等）。每轮对抗中，两支队伍分工明确，分别担任攻击方与防守方。攻击方需在规定时间内通过网络接入竞赛环境，重点针对 PLC 与 HMI 设备开展攻击操作，防守方对自身环境内的 PLC、HMI 设备及配套网络开展全面排查与防护，抵御攻击方的攻击。

5. 流程细节：

（1）赛前准备：现场核对各参赛队伍信息，通过现场抽签确定各队伍第一阶段第一轮的初始攻防身份（攻击方/防守方）；身份确认无误后，各队伍通过抽签确定本阶段对抗对手，对手配对结果同步公示。确认无误后，检查虚拟环境连通性、工具运行状态，熟悉目标区域 PLC 设备的基本信息，完成赛前准备确认。

（2）第一阶段：初始攻防对抗

1. 攻防开展：身份确定后，攻击方与防守方同时进入自身操作区域，在规定时间内开展对抗，攻击方针对防守方环境进行攻击操作，防守方针对自身环境进行防守操作；两队全程分别记录攻击、防守步骤及相关细节。

2. 报告提交：本轮攻防结束后，攻击方提交攻击报告（含操作步骤、漏洞利用方法、信息获取结果、后门植入细节等），防守方提交防守报告（含防守过程、攻击痕迹、后门排查结果、防护措施等），逾期未提交视为自动放弃本轮评分。

3. 身份互换：第一轮攻防结束后，进入中场休息环节，两队需在休息期间上交对应角色的报告；休息结束后，两队互换攻防身份，工作人员快速检查竞赛环境，准备进入第二轮攻防。

4. 第二轮攻防开展：身份互换后，攻击方针对防守方的环境开展攻击操作，

防守方针对自身环境开展防守操作，时长与第一轮一致，两队继续做好全程记录。

5. 报告补充提交：本轮结束后，两队分别补充提交对应角色的报告，逾期未提交视为自动放弃本轮评分。

6. 裁判评分：裁判组结合攻击方的攻击有效性（信息获取完整性、后门隐蔽性、操作规范性）、防守方的防守有效性（后门排查准确率、漏洞修复效果、防护合理性），分别对两队进行第一阶段的评分。

（3）第二阶段准备

第一阶段攻防结束后，所有参赛队伍再次进行现场抽签，重新确定第二阶段对抗的对手，对手配对结果当场公示。需明确：各队伍第二阶段第一轮的初始攻防身份，为其第一阶段第一轮的初始身份的互换（即第一阶段第一轮为攻击方的队伍，第二阶段第一轮为防守方；第一阶段第一轮为防守方的队伍，第二阶段第一轮为攻击方）。身份无需再次抽签，仅确认对手后，各队伍熟悉自身新身份的职责、操作要求，检查工具运行状态，准备进入第二阶段攻防对抗。

（4）第二阶段：互换身份攻防对抗

流程与第一阶段完全一致，具体如下：

1. 对手与身份确认：根据第二阶段抽签结果，各队伍确认本轮对抗对手及初始攻防身份，结果当场公示。

2. 第一轮攻防开展：初始攻击方针对初始防守方环境开展攻击操作，初始防守方针对自身环境开展防守操作，全程做好记录。

3. 中场休息与报告上交：第一轮攻防结束后，进入中场休息环节，两队需在休息期间，上交第一轮对应角色的报告；休息结束后，两队互换攻防身份，工作人员检查环境后，新攻击方与新防守方开展第二轮攻防对抗，全程做好记录。

4. 报告补充提交：本轮结束后，两队分别补充提交对应角色的报告，内容要求与第一轮一致。

5. 裁判评分：裁判组按照与第一阶段相同的标准，结合两队两次攻防表现，分别对两队进行本阶段性评分。

四、评比制度

本次赛事分为初赛、决赛两个评比环节，评比标准、晋级规则明确，确保公平、公正、公开，具体如下：

（一）初赛评比

1. 评分标准：采用纯客观题评分模式，由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. 晋级规则：依据初赛总成绩排名，筛选进入决赛的团队，所有参赛队伍均可获得参赛荣誉证书。

3. 异议处理：初赛成绩公示后，参赛队伍若对成绩有异议，可在公示期内（不少于 2 天）向主办单位提交异议申请，提供相关证明材料；主办单位组织工作人员核查，3 个工作日内给出核查结果并反馈。

（二）决赛评比

1. 评分标准：

（1）每轮比赛都有固定分值。

（2）攻击方完成对应任务，如获取 Flag 或成功植入后门等，即可获得对应分值。

（3）防守方防守失败，使攻击方成功突破防守、获取目标，防守方予以扣

分。

（4）若防守方成功溯源到攻击方攻击路径及植入的后门，提交对应报告，确认无误后，在原扣分基础上，返还该任务分值的 50%。

2. 排名规则：决赛总得分 = 第一阶段攻防得分 + 第二阶段攻防得分，按总得分从高到低排名；若总得分相同，以各阶段成功提交 Flag 的时间先后为序，提交时间越早者排名越靠前。

3. 奖项设置：决赛最终成绩按综合总分排序，确定各奖项。

五、竞赛规则

1. 参赛队伍需严格遵守赛事相关规定，服从主办单位、裁判组及工作人员的管理，不得擅自离场、违规操作。

2. 比赛过程中，不得实施与竞赛无关的攻击行为（如攻击赛事平台服务器、其他参赛队伍的虚拟环境、公共网络等），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。

3. 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。

4. 参赛队伍需妥善保管自身参赛账号、密码，不得转借他人使用，若因账号泄露导致的成绩异常，由参赛队伍自行承担责任。

5. 比赛期间，若出现平台、设备、网络等异常情况，参赛队伍需及时向工作人员、裁判反馈，不得擅自重启设备、修改平台配置，否则视为违规。

6. 赛题内容、Flag 等相关信息属于赛事机密，参赛队伍不得在比赛期间及比赛结束后擅自泄露，违者将追究相关责任。