工业网络靶场平台

综合测试评价报告

国家工业信息安全发展研究中心
检查评估所

2021年11月

版权声明

目　录

一、我国工业网络靶场应用现状分析

（一）工业网络靶场是工业信息安全研究重要基础设施之一

工业网络靶场的定义及内涵：工业网络靶场是主要基于虚拟化技术、大规模网络仿真技术、网络流量与用户行为模拟技术、数据采集与分析技术、工业仿真技术等技术进行开发，对工业网络、工业控制系统中的网络架构、系统设备、业务流程、工艺状态、运行环境和用户行为实现模拟仿真和复现，形成主要包含弹性云资源分配、可视化网络拓扑编排、工业软硬件仿真、数据采集与分析、应用服务及运行等核心功能的产品或系统；可实现业务松耦合、数据复用、底层共享，快速构建大规模高仿真工业控制系统，为工业控制系统领域技术研究、适配验证、开发测试、攻防对抗、应急演练、人才培养提供面向用户基础支撑环境。

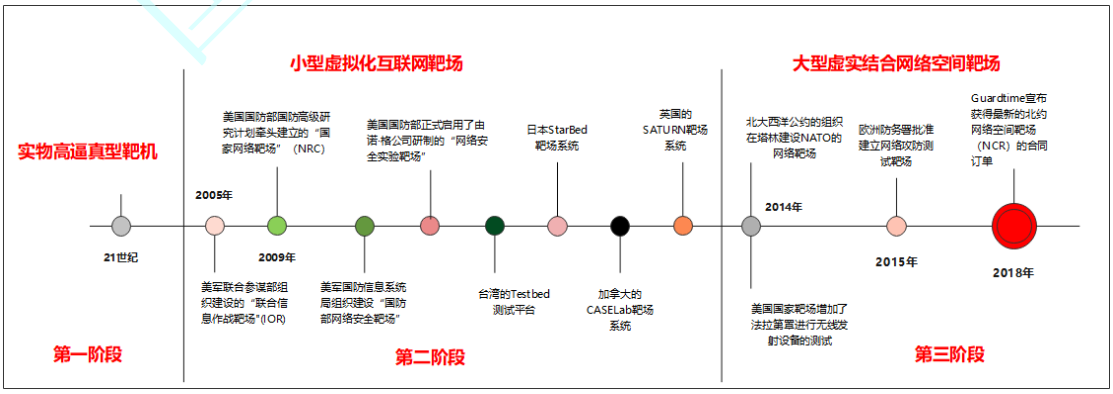
根据建设规模及用途，工业网络靶场主要分为：国家政府机构建设的军事国防类国家级示范靶场；地方政府及科研机构建设的基础设施类城市级靶场；工业企业及集团建设的教育培训或演练类企业级靶场。

工业网络靶场应用意义：（1）工业系统由隔离封闭转向开放互联，工控安全事件频发，工控系统面临的安全威胁日益突出，且攻击呈现出持续性和高隐蔽的特点；工业网络靶

场可解决真实工业系统无法直接进行网络安全研究且试错成本较高的关键问题。（2）信息技术与工业控制系统深度融合，我国大力推进大数据、云计算、人工智能、区块链等技术融入传统制造业；工业网络靶场通过快速构建能力为新技术、新场景应用有效性、适配性研究提供有效支撑。（3）综合性工业技术人才需求激增，IT 技术、自动化技术、网络安全技术融合的跨学科人才教育培训可通过工业网络靶场有效开展。

（二）我国网络靶场仍处于发展与跟进阶段

国际上，网络空间靶场（Cyber Range）起步至今，基本已经走过了三个阶段：第一阶段是以 21 世纪初期针对单独的木马类攻击武器而建立的实物高逼真型靶标时期。第二阶段是以 2005 年开始的小型虚拟化互联网靶场时期。第三阶段是 2014 年开始的支撑泛在网的大型虚实结合网络空间靶场时期。



我国网络靶场研究及建设相较于国外仍处于跟进及发

展阶段，当前我国大力推动数字化转型、新型基础设施建设、工业化和信息化高质量发展等重要工作，对网络空间技术研究、人才培养、应用创新等方面提出更高得要求。网络靶场作为网络空间安全研究、学习演练的新型重要基础设施，各地各部门纷纷加紧布局网络靶场相关的研究，建设规模与应用范围还有很大的拓展空间。

（三）工业网络靶场平台应用面临的挑战及问题

一是缺乏具备最佳示范及共识性解决方案，工业网络靶场建设需要明确的定位，我国未形成政府及权威机构主导推动，由技术供应商、科研单位、行业用户全面参与的发展模式，在主要概念、关键技术、建设实践、应用目标等方面未形成共识性解决方案。体系化、集成化、协同化发展尚未实现，行业产品技术能力及运营服务水平参差不齐。

二是工业网络靶场具有工业领域特殊性，工业网络靶场重点是 IT 与 OT 融合能力，在工业领域存在以下挑战：（1）工业控制系统关键软硬件设备核心技术由国外主导，闭源软件、私有通信协议、专用硬件等导致工业靶场虚拟仿真能力存在瓶颈。（2）工业网络安全研究必须结合实际工艺流程与业务场景，但工业领域工艺仿真难度较大；我国拥有 41 个工业大类、207 个工业中类、666 个工业小类，生产制造工艺较为复杂专业，且部分关键工艺数据具有保密性，导致工业靶

场仿真存在场景构建及业务复现真实性及逼真度存在瓶颈。（3）工业网络流量及用户行为采集量不足，由于以往工业系统多为信息孤岛，网络流量、数据、行为不对外开放，技术及产品供应商在工业网络靶场流量仿真及用户行为模拟开发上缺乏大量真实数据支撑，流量仿真及行为模拟在复杂度上与真实工业环境存在差距。

三是市场认知度较低、运营模式不清晰，当前工业网络靶场在网络安全技术攻防比赛、高校实训课程、集团公司技术研究等场景应用较多，这些工作大部分由政府、事业单位、国企等大机构主导，市场认知度和应用程度仍较低；并且由于工业网络靶场运营模式和相应需求不匹配，使用频率较低，导致建设方投资回报率不高，未能体现工业网络靶场价值。

二、工业网络靶场平台测试测评工作

（一）国外网络靶场测评工作现状

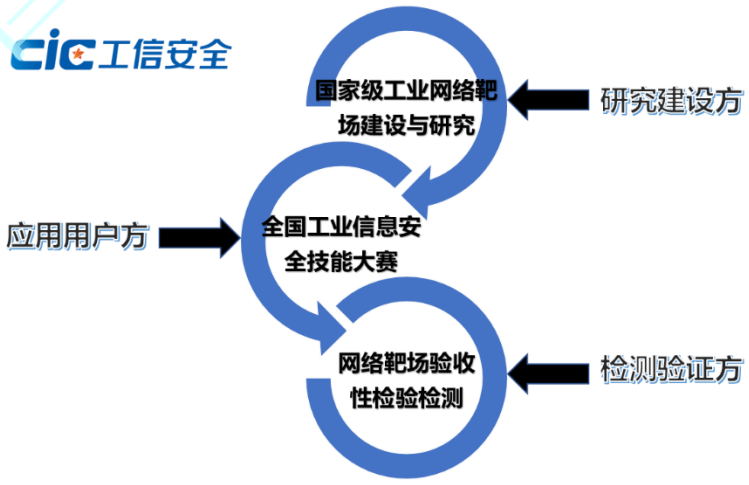
欧洲网络安全组织（ECSO）在欧洲已发起呼吁，希望联合网络靶场产品供应商、服务提供商、行业用户、科研机构等多方单位开展靶场资源整合等一系列行动。通过识别、收集多方单位网络靶场信息、整合欧洲网络靶场主要概念及服务实践方法，促进和定义“欧洲网络靶场”最佳实践和指南。并在此基础上，支持建立“欧洲网靶场联盟（ECRA）”，联盟

作为第三方开展网络靶场方法论、概念、最佳实践参考标准制定，网络靶场测试评价等工作，建立欧洲网络靶场市场地图，编制网络靶场供应商目录，建立匹配供需对接的第三方运营平台。

国际知名咨询公司埃森哲、德勤、安永、普华永道等公司在世界范围内均推出了网络安全靶场项目，尤其是在石油天然气、电力输配送、化工制造等工业领域，通过“咨询+靶场测试”模式，使客户更加直观体验新技术、新场景在靶场的应用，并选择最佳方案。

（二）中心工业网络靶场评价标准编制及测试评价工作

国家工业信息安全发展研究中心（以下称“中心”），在工业网络靶场领域，作为建设方参与多个国家级工业网络靶场建设与研究工作，作为用户方连续多年主办中国工业信息安全技能大赛、作为第三方权威机构参与各类网络靶场项目测评与验收工作。



中心综合利用工业网络靶场领域多维度技术积累与工作经验，推动研制工业网络靶场相关标准，旨在引导市场用户积极合理应用工业网络靶场、为研究建设机构提供技术能力参考基准、为第三方检验检测机构提供测评依据。

中心检查评估所本次发布 NQST-ICS/T C001-2021《工业网络靶场平台技术能力评价标准》（以下简称“标准”）作为中心建立工业网络靶场工作体系的起步推动标志。

2021 年，中心检查评估所开展了多轮“工业网络靶场平台测试征集活动”，对产品供应商、工业企业用户的多款工业网络靶场平台依据 NQST-ICS/T C001-2021《工业网络靶场平台技术能力评价标准》进行了综合技术能力评价测试（征集活动送测工业网络靶场平台简介见附录二）。

2021 年由中心主办的全国工业信息安全技能大赛决赛采用靶场互联方式开展，中心征集到包括哈尔滨工业大学（威海）、航天三院、大庆石油技术公司等全国 20 余家机构的 35 款工业网络靶场平台及场景作为决赛分布式场景（各征集工业靶场平台场景目录见附录三），进行资产识别、工艺触发、运行恢复、场景插旗等攻防竞赛，并在比赛使用过程中对各工业靶场场景进行深度测试。

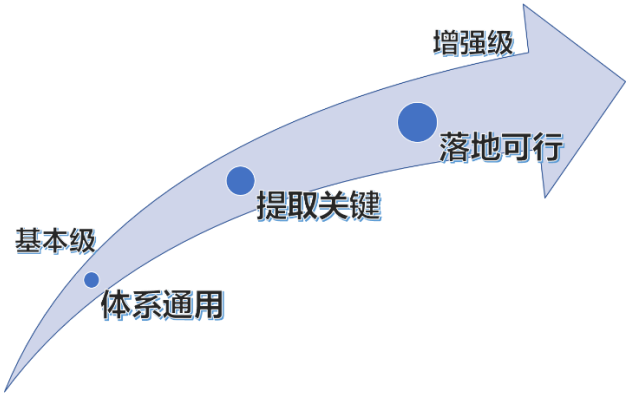
（三）标准体系架构及内容概述

1、标准测试评价对象：

NQST-ICS/T C001-2021《工业网络靶场平台技术能力评价标准》(标准全文见附录一)测试评价对象为面向用户交付或提供服务的工业网络靶场平台。当前，面向用户交付及提供服务的工业网络靶场产品主流为集成化、体系化、可定制的平台模式，用户通过客户端或 WEB 浏览器直接访问、使用相关平台服务。因此，标准通过测评面向用户的工业网络靶场平台功能、性能、兼容性等方面综合评价产品技术能力。

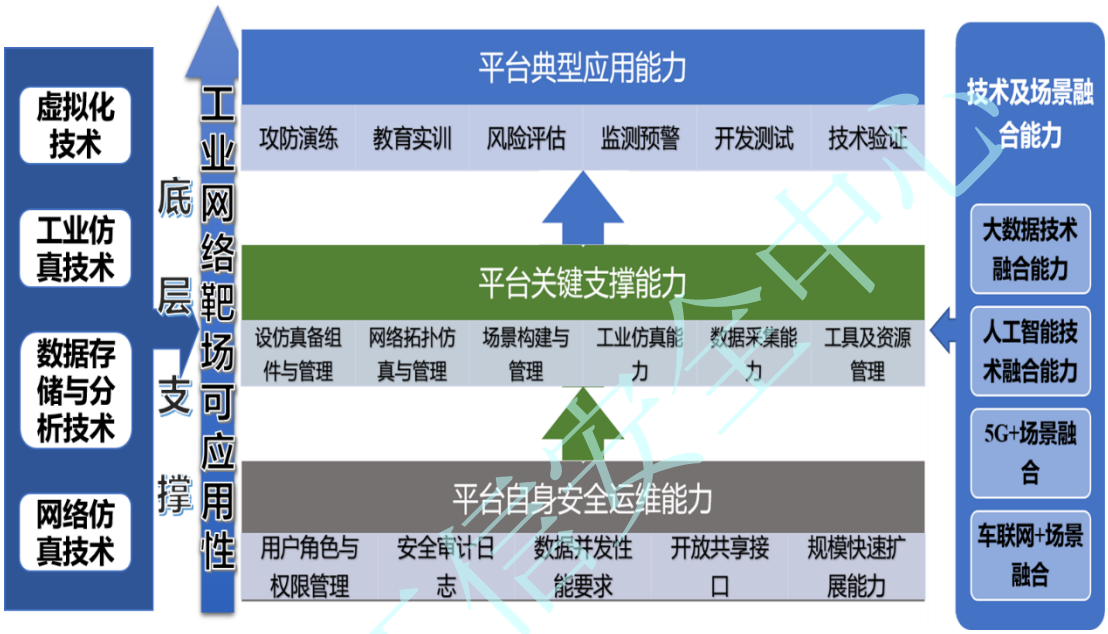
2、标准测试评价指标选取原则：

当前，市场上工业网络靶场产品在建设规模、技术架构、服务对象、目标需求、应用行业等方面存在着一定的差异性，并且未建立统一认可的体系架构。因此，标准测试评价指标选取原则为**“体系通用、提取关键、落地可行”**，并通过设置**“可选项”**指标以及“基本级”与“增强级”的分级体系，保障标准的科学性、合理性、可行性。



3、标准内容体系架构：

标准内容从平台自身安全运维能力、平台关键支撑能力、平台典型应用能力、平台新技术融合能力等层次对工业网络靶场平台进行技术能力评价，评价目标是工业网络靶场平台对于用户的**可应用性程度**。



（1）平台自身安全运维能力是产品运行及维护的基本保障，要求包括：用户角色与权限管理、安全审计日志、数据并发性能要求、开放共享接口、规模快速扩展能力等项目。

（2）平台关键支撑能力是工业网络靶场中支撑各类典型应用的基本功能，要求包括：设备组件仿真与管理、网络拓扑仿真与管理、场景构建与管理、工业仿真能力、数据采集能力、工具及素材管理等项目。

（3）平台典型应用能力是工业网络靶场用户核心应用需求，在面向不同用户需求时包含以下可选项：攻防演练、

教育实训、风险评估、开发测试、技术验证等项目。

（4）平台技术及场景融合能力是产品面向新技术、新应用的兼容与适配能力，可以展示平台在新需求下的快速响应能力，例如大数据技术、人工智能技术、车联网场景、5G 通信、车联网场景等项目。

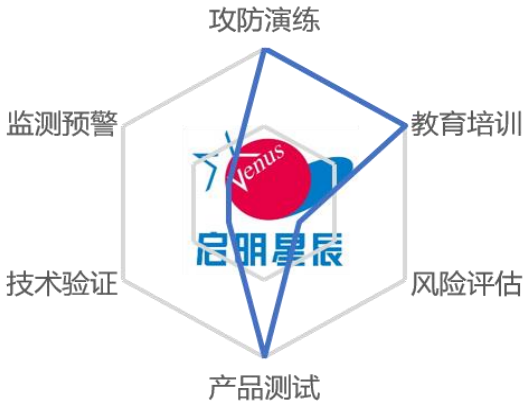
三、工业网络靶场平台综合测试评价

（一）工业网络靶场平台能力象限综合评价

工业网络靶场平台随着市场需求及技术创新，其用途也随之丰富，当前工业网络靶平台典型应用主要为：攻防演练、教育培训、风险评估、技术验证、产品测试、监测预警几大类。平台在满足客户最终应用需求的前提下，并需在投资成本与设备及组件丰富程度、靶场仿真能力、场景工艺仿真能力等要素之间进行平衡。

通过征集测试测评，各被测靶场平台基于目标客户的需求，对相应的典型应用能力进行了覆盖，截止本报告发布之日，当前各平台应用能力象限图表如下：

启明星辰-知白网络安全演练系统

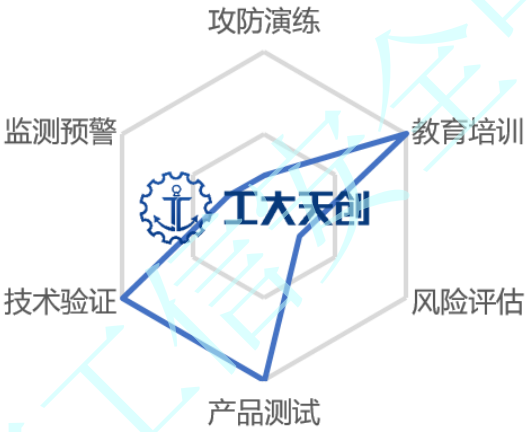


烽台科技-工控网络靶场平台

金川集团-工控安全仿真演练系统

博智安全-工业网络靶场平台

哈工大天创-工业网络靶场平台



木链科技-工控网络安全靶场平台

（二）平台自身安全运维能力综合测试评价

工业网络靶场平台作为交付用户的集成化平台产品，在平台计算及存储资源管理、用户权限与角色管理、自身安全审计、接口管理等功能应基本完备，才能保证产品交付用户后的稳定运行。

1、平台数据并发能力测试评价

工业网络靶场平台在攻防、培训、比赛、研究等各场景应用下，均具备大量用户同时在线并进行交互操作的需求，因此平台数据并发能力是关键指标之一。

以标准数据并发性能增强项要求为例，要求及测试评价数据如下:

3.1.3 数据并发性能要求:

（1）平台用户访问并发

支持用户平台访问并发（登录/退出）性能要求，根据靶场平台规模，[赋值]个用户访问请求并发情况下，事务成功率不低于 99%，平均响应时间不高于 0.5S。

（例：小型规模工业网络靶场平台，在 100 个用户访问请求并发情况下，事务成功率不低于 99%，平均响应时间不大于 0.5s。）

（2）资源数据请求并发

支持资源数据请求并发性能要求，根据靶场平台规模，[赋值]个用户同时请求关键资源接口情况下，事务成功率不低于 99%，平均响应时间不大于 1s。

（例：小型规模工业网络靶场平台，在 50 个用户同时请求关键资源接口情况下，事务成功率不低于 99%，平均响应时间不大于 1s。）

标准解读: 靶场平台规模、[赋值]用户并发、事务成功率、平均响应时间。

测试验证示范数据如下:

（1）平台用户访问并发测试验证数据: 以四款被测小型规模工业网络靶场平台测试数据为例，在 100 个用户访问请

求并发情况下，访问并发性能数据如下表。

表 1 平台用户访问并发性能

序号	平台名称	事务成功率	平均响应时间
1	启明星辰-知白网络安全演练系统	100%	0.396s
2	金川集团网络安全防护平台-工控安全仿真演练系统	100%	0.438s
3	烽台科技-工控网络靶场平台	100%	0.383s
4	木链科技-工控网络安全靶场平台	100%	0.424s
5	哈工大天创-工业教学实训靶场平台	100%	0.398s

（2）资源数据请求并发测试验证数据：以烽台科技-工控网络靶场平台为例，用户对某场景资源请求接口并发测试，在 50 个用户同时请求场景资源接口情况下，请求并发性能数据如下表。

表 2 资源数据请求并发性能

平台名称	事务成功率	平均响应时间
烽台科技-工控网络靶场平台	99.5%	0.891s

总结评价：在使用小型实验室规模物理资源进行建设的情况下，各被测靶场平台在并发性能测试中基本满足了标准要求的事务成功率及平均响应时间的要求；以并发性能测试估算算法，各平台基本满足 500 在线用户规模量的使用场景。

2、平台开放共享能力测试评价

工业网络靶场建设将从逐渐从独立封闭到资源共享是业内达成的共识，靶场场景、组件、平台等资源的开放共享能力将是靶场利用价值的衡量维度之一。

以标准增强项要求为例：

3.1.4　开放共享能力（增强项）

（1）标准化开放接口：平台应用支持对外标准化接口，用户可通过接口进行远程控制功能应用。

（2）共享互联：支持同构或异构靶场的资源共享互联解决方案。（可选项）

标准解读：

（1）平台自身具备对外开放能力；（2）平台作为中心节点具备共享互联解决方案能力。

验证示范：

2021 年工业信息安全技能大赛决赛采用远程互联靶场模式，互联全国 13 省及直辖市各分靶场节点，以决赛现场中心平台为核心节点，现场参赛选手访问各靶场进行比赛。

地点	黑龙江：哈尔滨，大庆；山东：威海；甘肃：金昌；江苏：南京、无锡；浙江：杭州；湖北：武汉；四川：成都；江西：南昌；贵州：贵阳；云南：昆明；北京；上海；重庆；

各地分靶场通过标准接口开放资源，决赛核心平台作为互联共享解决方案中心节点，完成了工业靶场互联共享示范。并根据比赛应用场景需求，进行下列方案设计：

（1）安全性：由中心节点控制的 VPN 网络，分节点 IPSEC VPN 方式远程接入；

（2）可靠性：网络链路冗余及链路优化，通过 5G 及有

线多种链路方式，保障通信持续可靠；

（3）性能（带宽）：中心节点支持最多 30 个分靶场节点接入；支持最多 300 人接入网络；中心节点带宽 2G 以上，单个节点带宽 200M 以上。

（4）网络隔离：接入点仅可访问某特定的分靶场节点，接入点之间无法相互访问，分靶场节点之间无法相互访问，隔离规则由中心控制节点下发。

（5）网络审计：部署网络流量监控采集分析，抗 DDoS 等安全防护措施。

总结评价：工业靶场互联共享当前仍处于探索发展阶段，未建设在各应用场景下的最佳示范，互联共享方式、性能效率、安全性、可靠性、适配性方案需要根据特定应用场景进行设计，在标准、协议、解决方案方面需进一步研究。

（三）平台关键支撑能力综合测试评价

1、设备组件仿真与管理测试评价

工业网络靶场支撑应用基础即为工业控制系统中网络设备、工业软件、系统软件、工业设备、数据库、应用服务等等设备组件的构建、仿真、接入及管理能力。

作为面向用户交付的平台产品，工业网络靶场平台内设备组件作为应用对象的封装性、作为环境构建基本单元的仿真可用性、以及可统一管理配置的易用性几个方面是重要的

测试评价指标。

以标准增强项要求为例，要求及测试评价数据如下:

3.2.1　设备组件仿真与管理

3.2.1.1　设备组件虚拟化仿真

支持网络设备、系统软件、安全设备、应用服务、工业设备等设备及组件的仿真能力，并支持各类设备组件封装为平台应用服务对象。

3.2.1.2　统一管理

支持对平台内设备组件及应用服务对象的统一管理，包括运行状态、资源占用、映射注册等方面。

标准解读:

1、封装性: 用户仅需通过平台应用服务对象（网络设备组件、安全设备组件、工业设备组件等）的暴露接口、服务等方式完成配置操作及交互。

2、仿真可用性: 用户对平台应用服务对象的配置操作得到正确的交互结果、反馈数据。

测试验证示范如下:

基于封装性、仿真可用性、统一管理等方面的判定，通过测评征集活动及工业技能大赛征集场景统计，整理出工业网络靶场平台设备及组件仿真接入管理能力图谱如下:

总结评价：工业网络靶场平台经过多年发展，在工业系统组件接入及仿真的品牌型号的覆盖范围上，已将工业控制系统各类主流软硬件设备及组件纳入应用服务对象范围，可根据用户需求进行相应的组件接入及封装。

在可用性及功能完备性方面，安全设备、网络设备、工业控制器等硬件的仿真及接入能力，与对应型号的真实设备相比仍有不足，并且需要一定的技术开发能力，无法根据需求快速拓展；在构建复杂网络、试验新型号硬件设备、验证配置合规性应用等场景，无法完全满足应用需求。

2、工业仿真能力测试评价

工业控制系统软硬件设备的技术开放性较低，使工业网络靶场仿真能力受限，并且根据应用目标，在平衡建设开发成本与收益的情况下，平台产品在工业仿真能力方面存在较大差异。

当前，工业仿真能力基本分为工业网络流量级仿真、设备级仿真、交互级仿真以及虚实结合构建等层次，在技术能力要求上逐步提高。大规模流量及行为仿真、数字孪生等概念在工业仿真领域逐步应用，但大多根据相应工业场景特定建设，标准未纳入到评价产品化平台的范围内。

以标准增强项要求为例，要求及测试评价数据如下:

3.2.4　工业仿真能力

3.2.4.1　工业协议仿真

支持主流工业协议流量仿真，如 Modbus、OPC、IEC104、S7comm、DNP3 等。

3.2.4.2　工控设备仿真

支持工业控制系统主流品牌各类软硬件设备仿真能力，如：PLC、RTU、DCS、SCADA 等，支持仿真设备连接测试、启停、位读写等基本操作。

3.2.4.3　工控设备交互仿真能力（增强项）

支持上位机软件与平台仿真设备的程序文件编写、工程文件的下发与上载等。

3.2.4.4　虚实结合能力（增强项）

支持真实工控设备与仿真组件共同搭建仿真场景的能力，并可采集真实设备数据并控制真实设备。

测试验证示范:

在通过流量分析工具、工业协议通信软件、上位机软件、场景业务验证等方式对测评征集活动及工业技能大赛征集场景的工业网络靶场平台的工业仿真设备进行仿真能力测试，测试验证统计如下。

参考基准	仿真能力	仿真要求	覆盖率
以工业控制系统西门子、罗克韦尔、三菱、欧	流量级	主要以流量回放的方式，达到反馈固定信息流的工业设备及组件仿真能力。	90%+
	设备级	以仿真软件集成的方式，达到可进行设备连接、启停、位读写等固定操作的仿真能力。	40%+

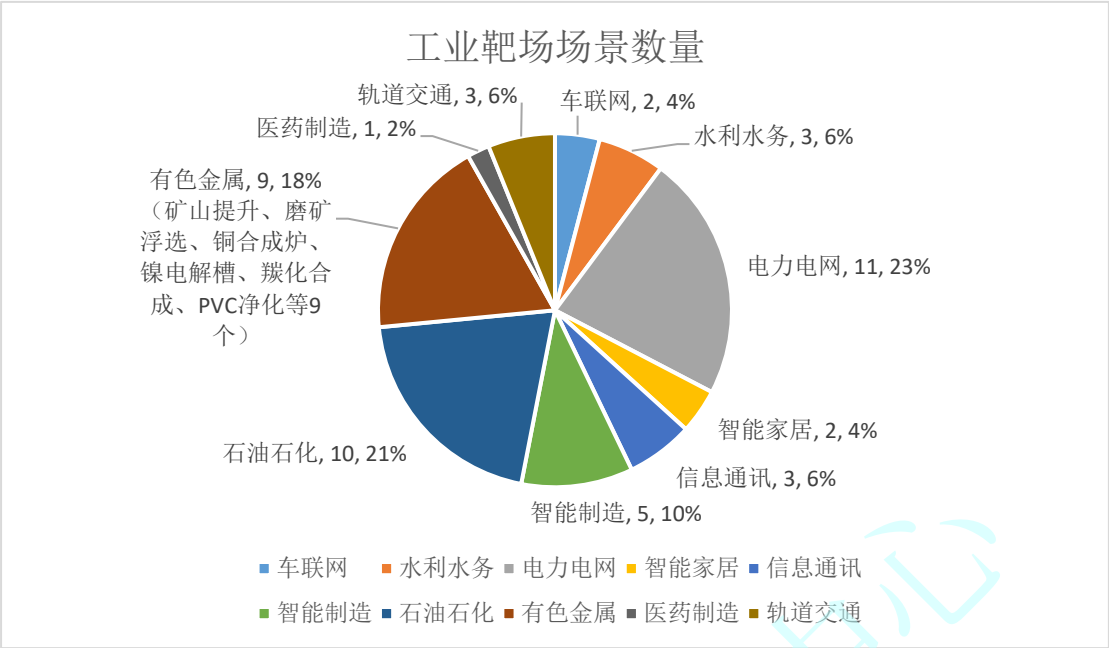
姆龙、施耐德、ABB 等主流品牌及型号共 40 种工业设备为参考基准	交互级	以软件集成或自主开发的方式，达到可进行设备组件基线配置、逻辑编程、文件下发等操作的仿真能力。	30%+
	虚实结合	真实工控设备与仿真组件共同搭建仿真场景的能力，达到真实设备数据采集及控制反馈的构建能力。	个别定制

总结评价：工业网络靶场平台工业仿真能力随着仿真要求的增加，仿真覆盖范围及深度体现出明显的不足，这是工业网络靶场向深层次应用的主要瓶颈。（实物部署与协议是强关联的）

工业靶场虚实结合构建过程中提高实物占比是快速提升仿真能力的方法，但其作为网络靶场的快速构建能力、低成本复用能力也随之下降；因此提高工业控制系统虚拟化仿真能力是推进工业网络靶场应用的关键。

3、工业场景能力测试评价

构建或复现用户的目标工业场景及业务流程是工业网络靶场支撑应用需求的核心，作为平台化产品，能够构建的工业场景数量以及涉及的行业、业务体现其平台适用范围。测评征集活动及工业技能大赛征集场景的工业网络靶场平台工业场景涉及行业统计图如下：



总结评价：样本包含了科研院所、工业生产企业、网络安全公司提供的 40 余款工业网络靶场及场景，可以看出在石油石化、有色金属、电力电网这样急需数字化转型的传统工业行业，工业靶场场景建设及研究已有较多应用；并且大部分工业生产企业采用了虚实结合的高成本建设方式，为提供目标工业场景、业务流程、生产工艺高仿真能力，为新技术研究、员工技能培训提供良好支撑环境。

以有色金属行业为例，工业场景内（矿山提升、磨矿浮选、铜合成炉、镍电解槽、羰化合成、PVC 净化等 9 个）仿真生产流程数量与实际生产工艺流程数量存在着数量级的差距，行业内工业网络靶场应用广度和深度还有巨大的发展空间。

四、工业网络靶场发展趋势及工作展望

工业网络靶场在未来的发展趋势中，**一是形成行业性工业网络靶场联合运营平台**由于建设成本及运营需求，将会逐渐形成靶场互联互通，分散“小靶场”通过联合运营的方式，形成具有行业共同性、应用共同性的分布式互联平台，有效提高工业网络靶场组件设备丰富度及仿真能力的覆盖率，并可开展协同演练、技术交流等更有价值靶场应用活动。

二是关键能力的模块化与专业化，当前大规模网络仿真、网络流量与用户行为模拟、数据采集与分析、高逼真度工业设备仿真、工业场景工艺复现等当前仍存在较大短板的工业靶场关键能力需要依靠科研院所、工业企业、安全厂商发挥自身优势形成通过标准接口、模型库等方式的对外服务能力，共同提高工业靶场技术能力。例如工业企业利用自身工业数据、工艺参数等优势资源构建关键工艺场景，在工业数据保密的情况下，提供靶场场景服务。

三是工业领域的信创应用，传统信息系统国产化替代工作已全面开展，但工业控制系统软硬件系统国产化工作还处于起步阶段，工业网络靶场可充分发挥其场景快速构建、资源低成本复用的特点，在工业控制系统国产化工作推进过程中发挥重要作用。

在我国各行业数字化大背景下，网络空间新技术、新场

景、新应用效能验证都对靶场能力及技术提出了更高的要求，中心将定位于“安全技术咨询+靶场测试验证”模式的权威机构，有效支撑两个强国、新基建等重要战略工作，并加速推进以下方面工作。

一是加快工业网络靶场关键技术、关键应用等标准及规范研制工作，发挥标准指导作用，联合科研机构、工业行业典型用户单位、产品及技术开发商，推动解决工业典型行业在工业网络靶场建设、应用、测评过程中亟待规范化、标准化、体系化的问题。

二是长期开展工业网络靶场专业化测试测评工作，中心下设国家工控安全检测中心通过实验室专业人员、标准设备对工业网络靶场产品或服务进行测试测评，出具第三方检测报告；同时完成调研行业技术能力，验证标准可行性，核心技术研究等工作目的。

三是深入研究工业网络靶场典型场景建设及运营模式创新，开展优秀产品或服务案例征集等活动，积极探索创新模式，联动各类资源、降低建设成本、提升服务能力、拓展应用范围，使工业网络靶场充分发挥持续运营和服务能力。

附录一 标准全文

NQST-ICS/T C001-2021 工业网络靶场平台技术能力评价标准

1. 概念和定义

工业网络靶场：主要基于虚拟化技术、大规模网络仿真技术、网络流量与用户行为模拟技术、数据采集与分析技术、工业仿真技术等进行开发，对工业网络、工业控制系统中的网络架构、系统设备、业务流程、工艺状态、运行环境和用户行为进行模拟仿真和复现，形成主要包含弹性云资源分配、可视化组网、工业软硬件仿真、数据存储与分析、应用服务及运行等核心功能的产品或系统。

工业网络靶场平台：面向用户交付或提供服务的集成化、体系化、可定制化工业网络靶场产品，用户可通过客户端或 WEB 浏览器直接访问、使用、配置平台相关资源、功能及服务。

2. 基本级要求

2.1 平台自身安全运维能力

2.1.1 用户角色与权限管理

2.1.1.1 唯一性标识

应保证任何用户都具有全局唯一的标识。

2.1.1.2 属性定义

应为每个用户规定与之相关的安全属性,包括用户标识、鉴别信息、权限等。

2.1.1.3 用户角色

（1）应设置多个用户角色并规定与之相关的权限,同时保证任何角色都具有全局唯一的标识。

（2）应可支持权限管理，可针对系统的所有资源进行权限的设计和编辑。

2.1.2 安全审计日志

2.1.2.1 审计数据生成

（1）对于所有成功和失败的访问事件,都应生成审计记录。审计日志中应包括:每个事件发生的日期、时间、IP 地址、所请求的 URL、成功或失败标识、匹配规则。

（2）管理员成功和失败鉴别日志,审计日志中应包括:每个事件发生的日期、时间、IP 地址、用户名、成功或失败标识。

（3）管理员操作日志,包括:过滤规则和防护策略的增加、删除和修改;管理员的增加、删除和修改。

2.1.3 数据并发性能要求

2.1.3.1 平台用户访问并发

支持用户平台访问并发（登录/退出）性能要求，根据靶场平台规模，[赋值]个用户访问请求并发情况下,事务成功率不低于 99%,平均响应时间不高于 0.5S。

（例：小型规模工业网络靶场平台，在 100 个用户访问请求并发情况下，事务成功率不低于 99%，平均响应时间不大于 0.5s。）

2.1.3.2 资源数据请求并发

支持资源数据请求并发性能要求，根据靶场平台规模，[赋值]个用户同时请求关键资源接口情况下，事务成功率不低于 99%，平均响应时间不大于 1s。

（例：小型规模工业网络靶场平台，在 50 个用户同时请求关键资源接口情况下，事务成功率不低于 99%，平均响应时间不大于 1s。）

2.2 平台关键支撑能力

2.2.1 设备组件仿真与管理

2.2.1.1 设备组件仿真与接入

支持网络设备、系统软件、安全设备、应用服务、工业设备等设备及组件的

仿真与接入能力，并支持各类设备及组件封装为平台应用服务对象，提供设备及组件相应的功能及服务。

2.2.1.2 统一管理

支持对平台内设备组件及应用服务对象的统一管理，并支持映射注册、配置管理、状态资源监视等能力。

2.2.2 网络拓扑仿真与管理

2.2.2.1 拓扑可视化组网

（1）应支持可视化拓扑组网，可进行组件可视化拖拽、连线等操作完成网络拓扑绘制。

（2）可通过平台统一对拓扑内网络进行组网、隔离、路由等设置。

2.2.3 应用场景仿真构建与管理

2.2.3.1 组件管理

支持统一组件资源库，对各类资源组件应用服务对象进行统一管理，供应用场景构建或复现进行调用。

2.2.3.2 工业场景仿真构建

支持通过设备组件调用及配置、网络构建及配置、系统配置、业务配置及工艺配置等能力，构建或复现目标工业场景业务及应用。

2.2.3.3 场景管理

支持场景基本管理能力，支持场景列表、场景基本信息展示，场景状态展示、搜索场景等功能。

2.2.3.4 工业场景模板

支持工业典型行业中重要业务的仿真场景复现与构建模板，具备关键控制操作、主要业务流程、典型工艺等仿真要素。

2.2.4 工业仿真能力

2.2.4.1 工业协议仿真

支持主流工业协议流量仿真，如 Modbus、OPC、IEC104、S7comm、DNP3 等。

2.2.4.2 工控设备仿真

支持工业控制系统主流品牌各类软硬件设备仿真能力，如: PLC、RTU、DCS、SCADA 等，支持仿真设备连接测试、启停、位读写等基本操作。

2.2.5 工具及知识库管理

（1）支持各类素材库集成、接入及管理，例如漏洞库、补丁库、脚本库、流量库、策略库等。

（2）支持各类工具集成、接入及管理，例如攻防工具、测试验证工具、数据测量工具等。

2.3 平台典型应用能力

2.3.1 攻防对抗演练（可选项）

2.3.1.1 攻防应用

支持利用平台内工业场景、设备及组件、工具及知识库进行攻防比赛、应急演练、红蓝对抗等应用能力。

2.3.1.2 任务管理

支持任务管理、流程管理能力，如任务控制、任务检索、任务汇报等能力。

2.3.1.3 过程监控

支持攻防演练过程、状态、结果过程监控可视化能力。

2.3.1.4 复盘分析

支持攻防演练复盘总结、分析汇报、报告输出等能力。

2.3.2 教学实训（可选项）

2.3.2.1 教学编排能力

支持教学素材库及工具库，支持对教学素材、教师及学员、实训场景、课程体系及流程的整体编排及管理能力。

2.3.2.2 实训实验能力

支持利用平台内相关仿真组件、实验场景及工具知识库进行实训实验性课程。

2.3.2.3 管理统计能力

支持课程、任务、结果、评价等教学过程数据的统计、汇总、查询及分析等能力。

2.3.3 风险评估（可选项）

2.3.3.1 合规知识库

支持风险评估工具及合规知识库资源，例如国家/行业标准库、渗透测试工具库、评估脚本库等。

2.3.3.2 风险评估应用

支持对平台内目标工业场景级系统开展国家相关标准符合性或定制化要求的网络安全风险评估工作，利用标准、工具、脚本评估目标工业场景及系统是否满足网络安全标准或体系要求、是否存在网络安全脆弱风险等。

2.3.4 产品测试（可选项）

2.3.4.1 产品接入

支持各类工业设备、工业网络安全产品、工业组态软件与平台内目标场景及系统的集成与接入能力。

2.3.4.2 产品测试评估

支持在目标场景及系统中，进行被测产品功能、脆弱性、安全性等方面进行测试，并评估产品在目标场景中可能引入的安全威胁。

2.3.5 技术验证（可选项）

支持利用目标工业场景开展安全技术研究能力，验证相关技术在目标工业行业及场景应用的有效性，例如私有协议开发、系统或固件升级、工具效能验证等。

2.3.6 监测预警（可选项）

2.3.6.1 仿真伪装能力

支持在目标网络或系统中发布或部署仿真工业场景、系统及设备组件，对网络攻击者进行欺骗伪装。

2.3.6.2 监控检测能力

支持网络扫描、资产探测、网络攻击等行为捕获及分析能力，支持蠕虫病毒、植入木马等威胁检测及清除能力，支持网络流量、网络行为审计与分析能力，具备监测预警综合功能。

3. 增强级要求

3.1 平台自身安全运维能力

3.1.1 用户角色与权限管理

3.1.1.1 唯一性标识

应保证任何用户都具有全局唯一的标识。

3.1.1.2 属性定义

应为每个用户规定与之相关的安全属性,包括用户标识、鉴别信息、权限等。

3.1.1.3 用户角色

（1）应设置多个用户角色并规定与之相关的权限,同时保证任何角色都具有全局唯一的标识。

（2）应可支持权限管理，可针对系统的所有资源进行权限的设计和编辑。

3.1.2 安全审计日志

3.1.2.1 审计数据生成

（1）对于所有成功和失败的访问事件,都应生成审计记录。审计日志中应包括:每个事件发生的日期、时间、IP 地址、所请求的 URL、成功或失败标识、匹配规则。

（2）管理员成功和失败鉴别日志,审计日志中应包括:每个事件发生的日期、时间、IP 地址、用户名、成功或失败标识。

（3）管理员操作日志,包括:过滤规则和防护策略的增加、删除和修改;管理员的增加、删除和修改。

3.1.2.2 统计功能（增强项）

（1）对资源的访问总次数以及单个 IP 访问的总次数按照不同的时间段(如:天、小时等)进行统计。

（2）能生成统计分析报表,并以图形化方式展现，能以常见格式导出。

3.1.3 数据并发性能要求

3.1.3.1 平台用户访问并发

支持用户平台访问并发（登录/退出）性能要求，根据靶场平台规模，[赋值]个用户访问请求并发情况下，事务成功率不低于 99%，平均响应时间不高于

0.5S。

（例：小型规模工业网络靶场平台，在 100 个用户访问请求并发情况下，事务成功率不低于 99%，平均响应时间不大于 0.5s。）

3.1.3.2 资源数据请求并发

支持资源数据请求并发性能要求，根据靶场平台规模，[赋值]个用户同时请求关键资源接口情况下，事务成功率不低于 99%，平均响应时间不大于 1s。

（例：小型规模工业网络靶场平台，在 50 个用户同时请求关键资源接口情况下，事务成功率不低于 99%，平均响应时间不大于 1s。）

3.1.4 开放共享能力（增强项）

（1）标准化开放接口：平台支持对外标准化接口，可通过标准化接口对平台应用服务或资源进行调用。

（2）共享互联：作为中心节点支持同构或异构靶场的资源共享互联接入。（可选项）

3.1.5 规模可扩展能力（增强项）

支持通过弹性部署模式、虚拟化本地化扩展或互联接入扩展等方式进行平台资源规模快速扩展能力。

3.2 平台关键支撑能力

3.2.1 设备组件仿真与管理

3.2.1.1 设备组件仿真与接入

支持网络设备、系统软件、安全设备、应用服务、工业设备等设备及组件的仿真与接入能力，并支持各类设备及组件封装为平台应用服务对象，提供设备及组件相应的功能及服务。

3.2.1.2 统一管理

支持对平台内设备组件及应用服务对象的统一管理，并支持映射注册、配置管理、状态资源监视等能力。

3.2.2 网络拓扑仿真与管理

3.2.2.1 拓扑可视化组网

（1）应支持可视化拓扑组网，可进行组件可视化拖拽、连线等操作完成网

络拓扑绘制。

（2）可通过平台统一对拓扑内网络进行组网、隔离、路由等设置。

3.2.2.2 统一组网控制（增强项）

支持利用 SDN 技术等进行组网编排，实现组网、隔离、路由、网络复现及网络安全策略统一控制及管理能力。

3.2.3 场景构建与管理

3.2.3.1 组件管理

支持统一组件资源库，对各类资源组件应用服务对象进行统一管理，供应用场景构建或复现进行调用。

3.2.3.2 工业场景仿真构建

支持通过设备组件调用及配置、网络构建及配置、系统配置、业务配置及工艺配置等能力，构建或复现目标工业场景业务及应用。

3.2.3.3 场景管理

支持场景基本管理能力，支持场景列表、场景基本信息展示，场景状态展示、搜索场景等功能。

3.2.3.4 工业场景模板

支持工业典型行业中重要业务的仿真场景复现与构建模板，具备关键控制操作、主要业务流程、典型工艺等仿真要素。

3.2.4 工业仿真能力

3.2.4.1 工业协议仿真

支持主流工业协议流量仿真，如 Modbus、OPC、IEC104、S7comm、DNP3 等。

3.2.4.2 工控设备仿真

支持工业控制系统主流品牌各类软硬件设备仿真能力，如: PLC、RTU、DCS、SCADA 等，支持仿真设备连接测试、启停、位读写等基本操作。

3.2.4.3 工控设备交互仿真能力（增强项）

支持上位机软件与平台仿真设备的程序文件编写、工程文件的下发与上载等。

3.2.4.4 虚实结合能力（增强项）

支持真实工控设备与仿真组件共同搭建仿真场景的能力，并可采集真实设备数据并控制真实设备。

3.2.5 工具及知识库管理

（1）支持各类素材库集成、接入及管理，例如漏洞库、补丁库、脚本库、流量库、策略库等。

（2）支持各类工具集成、接入及管理，例如攻防工具、测试验证工具、数据测量工具等。

3.2.6 数据采集能力（增强项）

支持平台内底层资源、仿真组件、工业场景、用户行为、网络流量等数据采集能力。

3.3 平台典型应用能力

3.3.1 攻防对抗演练（可选项）

3.3.1.1 攻防应用

支持利用平台内工业场景、设备及组件、工具及知识库进行攻防比赛、应急演练、红蓝对抗等应用能力。

3.3.1.2 任务管理

支持任务管理、流程管理能力，如任务控制、任务检索、任务汇报等能力。

3.3.1.3 过程监控

支持攻防演练过程中，设备及组件状态监控、工业场景及系统态势感知、攻防效果及路径可视化等能力。

3.3.1.4 复盘分析

支持攻防演练复盘总结、分析汇报、报告输出等能力。

3.3.2 教学实训（可选项）

3.3.2.1 教学编排能力

支持教学素材库及工具库，支持对教学素材、教师及学员、实训场景、课程体系及流程的整体编排及管理能力。

3.3.2.2 实训实验能力

支持利用平台内相关仿真组件、实验场景及工具知识库进行实训实验性课程。

3.3.2.3 管理统计能力

支持课程、任务、结果、评价等教学过程数据的统计、汇总、查询及分析等能力。

3.3.3 风险评估（可选项）

3.3.3.1 评估知识库

支持风险评估工具、标准合规知识库、主流风险评估模型库等资源库，例如国家/行业标准库、渗透测试工具库、评估脚本库、定性及定量评估模型等。

3.3.3.2 风险评估应用

支持对平台内目标工业场景及系统开展国家相关标准符合性或定制化要求的网络安全风险评估工作，利用标准比对、工具渗透、脚本攻击等方式，在一定的风险评估模型中评估分析目标工业场景及系统是否满足网络安全标准或体系要求、是否存在网络安全脆弱风险。

3.3.3.3 自动化评估（增强项）

支持根据一定的评估标准和模型，编排自动化风险评估流程及操作，在平台内目标工业场景及系统开展自动化网络安全风险评估，并支持自动化生成定性或定量的评估结果及评估报告，例如等级保护评估、工业控制系统信息安全防护能力评估等主流评估模型。

3.3.4 产品测试（可选项）

3.3.4.1 产品接入

支持各类工业设备、工业网络安全产品、工业组态软件与平台内目标场景及系统的集成与接入能力。

3.3.4.2 产品测试评估

支持在目标场景及系统中，进行被测产品功能、脆弱性、安全性等方面进行测试，并评估产品在目标场景中可能引入的安全威胁。

3.3.4.3 自动化评估（增强项）

支持设备及组件自动化检测及渗透测试能力，实现批量化产品信息安全测试，并生成检测结果及报告。

3.3.5 技术验证（可选项）

支持利用目标工业场景开展安全技术研究能力，验证相关技术在目标工业行业及场景应用的有效性，例如私有协议开发、系统或固件升级、工具效能验证等。

3.3.6 监测预警（可选项）

3.3.6.1 仿真伪装能力

支持在目标网络或系统中发布或部署仿真工业场景、系统及设备组件，对网络攻击者进行欺骗伪装。

3.3.6.2 监控检测能力

支持网络扫描、资产探测、网络攻击等行为捕获及分析能力，支持蠕虫病毒、植入木马等威胁检测及清除能力，支持网络流量、网络行为审计与分析能力，具备监测预警综合功能。

3.4 平台技术及场景融合能力（增强项）

3.4.1 大数据技术融合能力（可选项）

支持融合大数据技术，通过对平台内多源异构数据的采集、存储、分析，支撑例如效能评估、攻防推演、威胁溯源等应用能力。

3.4.2 人工智能技术融合能力（可选项）

支持融合人工智能技术，通过深度学习算法等支撑例如自动化渗透测试、自动化风险评估、自动化攻防对抗等应用能力。

3.4.3 5G 通信场景（可选项）

支持 5G+工业互联网 垂直行业应用能力测试验证，支持 5G 通信安全性进行测试验证。

3.4.4 车联网场景（可选项）

支持智能车联网场景融合能力，通过平台场景集成，实现例如车辆 CAN 总线攻防检测、关键 ECU 部件渗透、协议逆向分析等仿真场景构建。

附录二 “工业网络靶场平台测试征集活动”案例简介

一、烽台科技-工控网络靶场平台

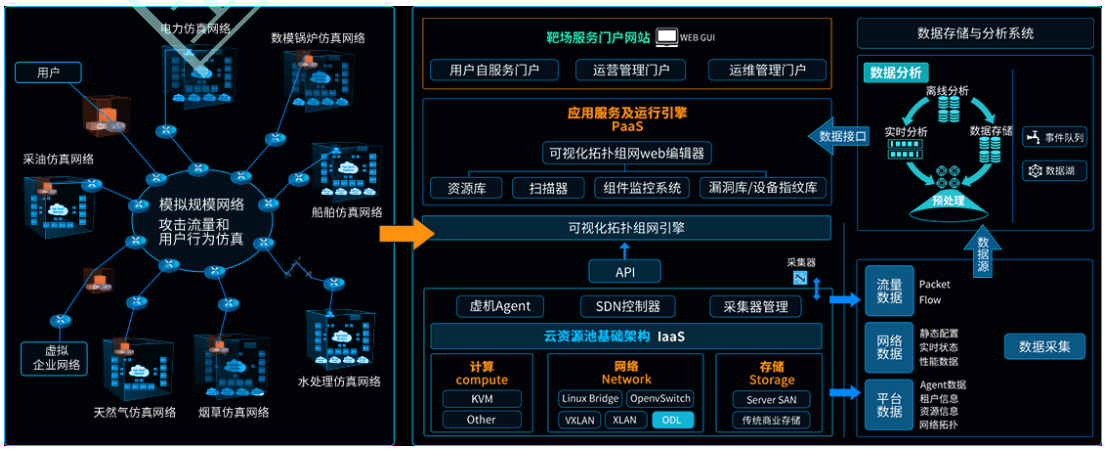
（一）平台及场景简介

烽台科技工业基础靶场平台，是自主研发的面向工控网络仿真环境建设的基础网络设施。旨在通过工业网络靶场建设，为能源、电力、通信、交通、国防等关系到国计民生、经济社会运转、国家安全等核心重点行业和领域提供分析、设计、研发、集成、测试、评估、运维等全生命周期保障服务，解决无法在真实环境中对复杂大规模异构网络和用户进行逼真的模拟和测试，以及风险评估等问题，实现工业信息安全能力的整体提升。烽台科技靶场能够全面模拟仿真工业控制设备、工业控制系统、网络设备、安全设备、工业应用、工业协议、传统流量、攻击流量等，能够对多个行业及场景的工控信息网络进行 全面仿真。

在行业方向上，能够仿真电力行业、石油行业、钢铁行业、市政燃气 行业、智能制造行业等十余种工业行业场景。包括电力行业的火电发电、新能源发电、配电、 变电、用电等场景，石油行业的石油开采、油气炼化、石油输送、石油储运等场景，钢铁行业的烧结工艺、炼钢工艺、炼铁工艺、轧钢工艺、能源工艺、采矿工艺等场景，市政燃气行 业的燃气门站、燃气调压站、燃气管线控制等场景以及智能制造行业的轮胎装备制造、船舶 生产制造、电子器件制造、军工生产制造等场景。

（二）平台技术解决方案

产品借助虚拟化技术、软件定义网络、虚实互联、网络安全检测与分析等技术研发，具备便捷的网络拓扑构建细粒度的用户行为监控、全方位攻防数据采集、宏观微观兼具的态势展示、开放的第三方接入支撑、逼真的场景仿真复现、丰富强大的靶标资源、灵活快捷的虚拟机与靶场数据交互、多维度可量化的能力评估等功能。满足科研院所、大型企业、政府以及军队增强自身网络安全能力等业务需求。



（三）平台应用示范项目

昆钢集团工业信息安全仿真演练实验室工业靶场建设:

用户需求: 昆钢集团作为工业和信息化部重点实验室钢铁行业分中心，基于昆钢集团自身工业信息安全建设工作，建设包含重点行业工业信息安全测试床和工业互联网企业级集中化安全监测平台及防护方案的选型测试环境功能的仿真演练实验室，能够实现业务仿真、应急演练、检测验证、教育培训及成果展示等功能。对部署在昆钢集团的集团级集中化监测平台、钢铁行业安全通报与共享平台提供集团展示中心。对昆钢集团及下属各分公司的工业信息安全建设提供全面的安全态势监控、安全巡检、防护加固、应急演练、安全教育等能力。

交付成果: 烽台科技为昆钢集团工业信息安全仿真演练实验室规划了业务仿真区、应急演练区、检测验证区、安全教育区四个主要区域，并建设工业网络靶场:

（1）业务仿真区按照前期调研钢铁生产主要生产工艺，采用虚实结合的方式搭建模拟仿真环境，仿真钢铁生产全业务流程控制系统。自动控制系统采用真实控制设备，模拟钢铁生产制造控制过程。

（2）应急演练区为昆钢建立线上实操演练环境，结合具体的规范化流程进行实际操作，提升演练人员针对信息安全的认知和技能水平，达到理论实践结合一体化的目的，提高昆钢应急响应人员应急响应能力。

（3）检测验证区将提供产品测试能力，靶场具备真实环境复现能力，因此针对产品的测试将具备在真实环境下的功能及性能表现属性。

（4）安全教育区主要面向安全研究人员安全实践需求，工业靶场实训管控中心以理论与实践相融合的方式提升工控安全技术人员基础安全理论知识、攻防实战能力以及场景化安全研究能力，使之能对各种主流安全实践具有独立分析、应对处理能力。

项目价值: 昆钢集团以工业信息安全仿真演练实验室为基地，组织钢铁行业的工业信息安全研讨会，向同行业企业推广建设经验，扩大了昆钢集团在钢铁行业影响力。借助安全通报与共享平台面向钢铁行业提供工业信息安全能力建设经验、风险处置案例等多方面情报共享。为集团管理者提供全集团工业信息安全态势的呈现；为安全巡检提供多类信息化工具，提高人员巡检效率；对于后续在各分公司部署的工业信息安全产品、方案，提供安全检测、验证环境，确保各类工业信息安全产品对真实业务的无影响并验证其真实安全防护效果；为集团工业信息安全集中应急演练提供场所；为集团内工业信息安全管理、运维等人员提供安全理论、安全实操的环境及场地，提升各类人员安全能力。

二、博智安全-工业网络靶场平台

（一）平台及场景简介

博智工业网络靶场平台是以孪生仿真技术为基础、威胁模拟生成为手段、攻防推演验证为目标的一体化综合演训平台，能够仿真电信、变电、核电、卫星、轨交、水处理、火力发电、化工制造等多种关基重保行业场景，并提供配套的教学课件、靶标镜像、试题赛题、训练场景、训练科目、攻防工具、漏洞验证等内容，支撑教学培训、比武竞赛、安全评估、渗透测试、技术验证等活动的开展。

博智靶场产品在高校、职院、企业已有许多应用案例，支撑了多场全国和省级的工控安全大赛，并已在多个军工项目中交付使用。

（二）平台技术解决方案

博智工业网络靶场基于 OpenStack 虚拟化平台进行了二次开发，对虚拟计算资源、存储资源和网络资源进行统一的管理和调度，通过软件定义网络（SDN）技术实现仿真场景的按需构建。能够通过虚实结合的方式构建目标仿真场景，实现虚拟设备和真实设备的互联互通。

博智孪生仿真靶场分为资源支撑层、数据支撑层、功能支撑层和应用服务层。资源支撑层提供了靶场用到的各种物理资产和虚拟资产的管理能力，并提供了统一的资源编排调度接口；数据支撑层使用分布式文件系统提供了数据的存储和管理服务，为靶场平台数据的可靠性提供了保障；功能支撑层实现了数据采集、流量模拟、场景编排、攻击溯源、效果评估等靶场平台的关键能力；应用服务层通过对功能支撑层功能的编排和调度，对外提供教学培训、比武竞赛、攻防演练、安全评估、渗透测试等典型应用服务。

（三）平台应用示范项目

浙江大学变电站监控系统靶场项目

建设一套遵循国家电力行业标准的纯虚拟化变电站监控系统靶场，用于验证各种攻击手段对变电站运行产生的影响，对变电站防护体系进行研究。

变电站监控系统是典型且复杂的工业控制系统，涉及电力系统、计算机、通信、网络安全等多个技术领域。系统逻辑上分为三层，包括站控层、间隔层以及过程层。站控层主要由监控计算机、通信网关机以及其他附属设备构成；间隔层主要由测控设备、保护设备或保护测控一体化设备、安全自动装置以及其他自动化设备构成；过程层主要由智能终端以及合并单元构成；各层之间通过光纤网络进行通信。

博智安全交付的变电站监控系统靶场是通过纯虚拟化方式端到端构建了变

电站的监控场景。纯虚拟化的方式使得用户可以根据国家标准的规定，灵活地构建组成 500kV、220kV、110kV、35kV 等各电压等级变电站自动化监控系统。改变电站监控系统靶场主要具备 5 个主要功能：

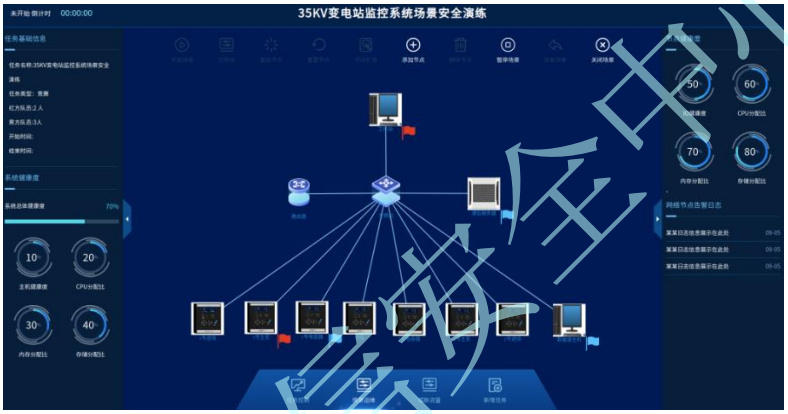
1）具备变电站监控系统一次过程的仿真功能，包括站控层软硬件、间隔层软硬件以及变电站运行仿真功能；

2）具备变电站监控系统环境管理功能，可实现仿真环境的备份和恢复等工作，为用户提供了系统异常情况下，快速恢复自动化仿真系统的能力；

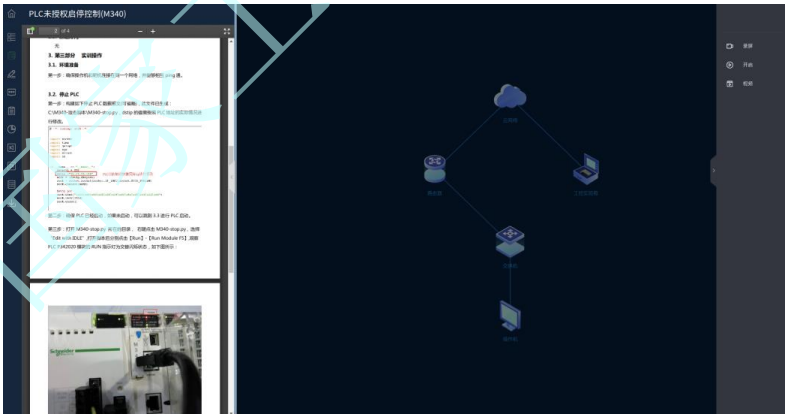
3）具备仿真真实通信设备的各种能力，实现变电所常用的主站 Modbus TCP、主从 IEC104、主从 IEC61850 等网络协议以及主从 Modbus RTU、主从 IEC101、从 CDT、主从 IEC103 等串口协议规约，完成仿真系统的数据采集以及转发工作；

4）能够仿真再现各层软硬件存在的各种安全漏洞，并能够模拟漏洞被利用时遭受攻击情况下变电站运行所遭受的影响；

5）能够基于变电站监控系统提供网络攻防红蓝对抗。实现以攻促防的安全演练和安全研究。



该变电站监控系统靶场提供了针对该场景的攻防对抗演练。可以通过攻防实战进行安全应急演练，基于实战进行技能、功能和性能的验证。



人员的安全技能教育培训也是靶场一个重要功能，同样变电站监控系统靶场提供了各种关于工控网络安全相关的学习和训练工具，为变电站系统网络安全的研究工作提供了有力的支撑。

三、木链科技-工控网络靶场平台

（一）平台及场景简介

木链科技——工控网络安全靶场通过虚拟化及仿真技术重现真实工业网络

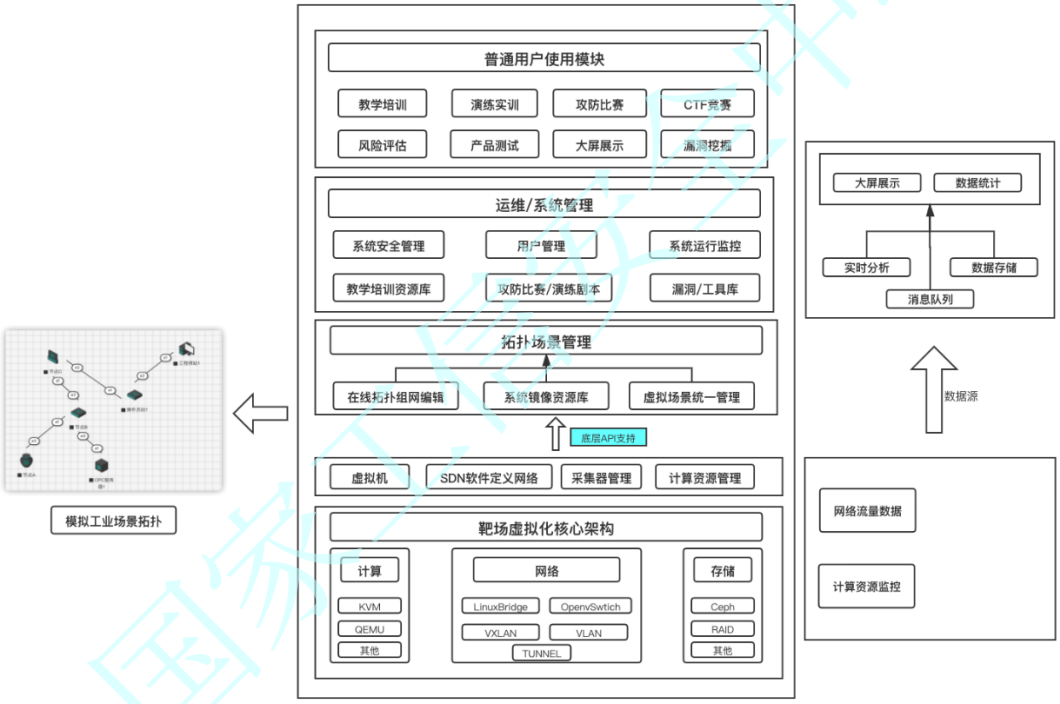
节点及链路，科学的架构设计，将工控系统与安全体系完整结合，利用可视化组网引擎为靶场实现多种工业领域的网络场景仿真编排，并向用户提供优质的教学培训、攻防演练、安全竞赛、产品测试等核心安全服务；靶场平台可支持火力发电、核能发电、新能源发电等电力场景，汽车、电子、军工制造等智能制造多种工业生产场景；

通过仿真跨区域工业以太网、大规模互联网、无线网络等，结合行业场景，提升工控安全人员的 ICS 网络杀伤链的理解，帮助工控安全人员可以学到更多的知识，更加有效地提高 ICS 的安全性。

（二）平台技术解决方案

工控网络安全靶场总体技术框架主要由虚拟化核心架构（工控设备、计算、网络、存储）、拓扑场景管理引擎、运维/系统管理及靶场应用等模块组成。

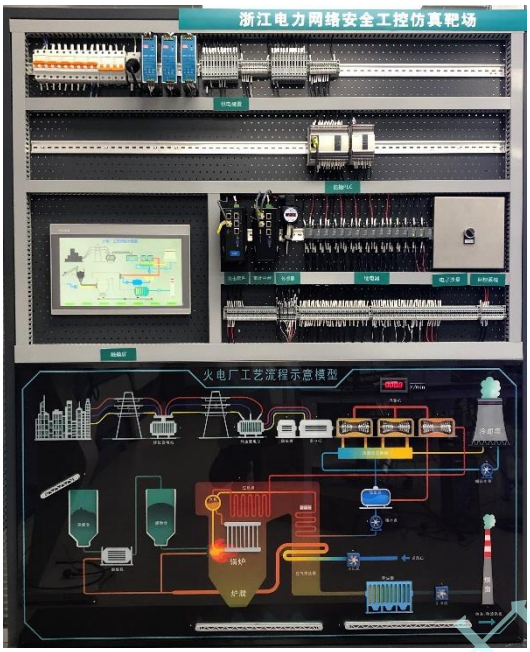
其中虚拟化核心架构，融合了云计算、软件定义网络、分布式存储等技术，将离散异构资源变为统一的资源池，集中管理软硬件资源，将基础架构与服务解耦，是靶场平台技术解决方案的关键。



（三）平台应用示范项目

浙江电力科学研究院靶场项目：

本项目部署了热电厂汽轮机控制系统和电厂涉网配电控制系统；靶场平台用于模拟电力行业的真实工业网络和环境，以进行复现和仿真，包括上位机、下位机、执行器、传感器等工控系统常见组件，以及必要的网络设备和环境部署。



解决需求：本项目利用靶场平台提供的场景构建、虚实结合模块，搭建起高仿真的靶场环境，解决了客户内部受训人员开展工控网络安全教育课程，组织客户内部大量安全技术人员的攻防技术演练需求，以实战演习追踪前沿网络安全技术，不断提升专业技能水平；

项目价值：并能形成以实验室技术研究为中核心，指导企业实践验证试验的工作模式，充分体现浙江电科院在集团中，研究核心共性问题，指导企业实践的职责职能。

附录三 “2021 年工业信息安全技能大赛决赛”征集工业靶场攻防场景

序号	公司名称	互联场景名称	介绍	工业场景概述
1.	哈尔滨工业大学（威海）	污水处理	哈尔滨工业大学威海校区建有面向城市燃气、轨道交通、污水处理等典型行业的工控安全靶场，涵盖施耐德、西门子、台达等主流厂商的工业设备，可支持 S7Comm、Modbus 等主流工业协议模拟，用于支撑校内工业信息安全实训竞赛。	本场景为水处理系统，场景模拟了污水处理过程，可实现污水过滤，水传输过程。
2.		城市燃气		本场景为燃气系统，场景模拟了燃气输送过程，可对燃气传输过程的压力、温度等数值进行监控及控制。
3.		轨道交通		本场景为轨道交通系统，场景模拟了红绿灯变轨过程，红绿灯可展示目前变轨状态，指导安全通行状态。
4.	大庆油田信息技术北京分公司	采油工艺联合处理站	大庆油田信息技术公司长期致力于工业控制系统相关安全研究，结合大庆油田业务特色，构建贴近油田生产工艺的工控安全仿真验证平台，结合组态软件、PLC 等工控软硬件模拟实现油气生产工艺流程、网络架构及安全防护环境。	本场景为采油工艺，场景模拟了油气生产环节中联合处理站工艺流程，通过各类 plc、电磁阀门、泵、仪表等设备实现工业现场的生产工艺和生产过程模拟。

5.	北京京航计算通讯研究所	综合场景（火箭发射场景、装备制造场景）	航盾工业信息安全仿真平台采用虚实结合的方式进行搭建思路，包含实验平台管控中心（提供虚拟资源）、自动控制系统（实物）、场景仿真沙盘（仿真沙盘）。主要通过攻防对抗、产品测试、应急演练和培训教育等，综合提升工控安全人员攻防实战能力，能对各种主流安全实践具有独立分析、应对处理能力。	模拟了某装备生产的工艺路线：零件配送、料盘进料、精密装配、检测入库等工艺；火箭发射场景模拟了火箭发射程序、发射架移动、点火、升空等主要流程；用作装备制造工艺及火箭发射的高度模拟仿真复刻，实现航空航天领域工控系统仿真测试、漏洞挖掘、安全技术研究、攻防演练等。
6.	云南昆钢电子信息科技有限公司	钢铁行业工业信息安全测试床	昆钢工业网络靶场与钢铁行业工业信息安全测试床进行多级联动，涵盖钢铁生产中动力能源、综合料场、烧结、炼铁、炼钢、轧钢、仓库管理、物流运输等场景，满足工业控制系统大规模网络安全仿真需求。	钢铁行业工业信息安全测试床，场景模拟了典型钢铁生产的全工艺流程，包括：动力能源、综合料场、烧结、炼铁、炼钢、轧钢、仓库管理、物流运输等，场景与昆钢工控安全靶场进行虚实互联，建立多套 1:1 还原的生产工艺软硬件仿真环境，以此为基础形成了昆钢特色的工控安全应急演练、质检、培训、竞赛、方案验证、技术研究中心。
7.	启明星辰信息技术集团股份有限公司	综合场景-水务系统仿真试验台、智能制造仿真试验台、输配电仿真试验台、火力发电仿真试验台、化工仿真试验台	启明星辰工控安全靶场包括水务系统、智能制造、输配电、火电发电、化工流程五大仿真场景，工控靶场通过对各业务场景的等比例仿真，还原各工艺场景的生产控制全流程，旨在为用户提供工业软件安全验证等实际用途，切实提高用户在工控系统安全评估、渗透测试领域的实战综合能力。	本场景主要描述真实火力发电中输煤，高炉，冷凝等流程、电网系统输配电流程与双侧变压流程、智能工厂中的二维平面自动加工台工作流程、原油蒸馏分层的过程、城市自来水公司送水入户的环境。帮助用户熟悉火电攻防、电网系统输配电、智能制造的自动化控制环境、化工系统场景

8.	北京安帝科技有限公司	水利发电场景	安帝科技工业互联网安全虚拟化平台是一款针对工控设备、控制、网络、业务数据、应用进行真实业务网络的虚拟仿真，并能进行攻防演练以避免对真实业务网络的破坏的平台，具有成本低、部署灵活、过程可重复，是工业互联网网络攻防演练、测试研究、虚实结合、场景高度模拟仿真的重要工具。	水利发电场景，场景模拟了水电厂 OT/IT 多层网络结构，作用：仿真真实水利发电场景。
9.	威海天之卫网络空间安全科技有限公司	楼宇电梯	威海天之卫网络空间安全科技有限公司建有面向远程配电、风力发电、智能楼宇等典型行业的工控安全靶场，涵盖西门子、罗克韦尔、和利时等厂商的工业设备，可支持 S7Comm、CIP、Modbus 等主流工业协议模拟，用于工业防火墙、安全审计的测试。	本靶场接入场景为智能楼宇系统，场景模拟了电梯运行过程，可实现电梯上下行及停止控制。
10.		远程输电		本靶场接入场景为输配电系统，场景模拟了电力分配传输过程，可进行多线路的定压电力传输。
11.		发电行业		本靶场接入场景为风力发电系统，场景模拟了风机工作发电、供电过程，可对发电过程进行监控及调节。

12.	博智安全科技股份有限公司	核发电场景	博智孪生仿真靶场平台是一个基于数字孪生技术，具备工业自动化网络、电信、电力、轨道交通、IOT、传统网络等多种行业场景仿真能力的应用服务平台，能高效地开展与工业网络安全相关的学习、研究、检验、竞赛、演习等活动。	本核电仿真靶场通过虚实结合技术模拟了核电企业网络场景结构及真实核发电工艺，网络划分三大区域，最外层是管理网区域存在官网及管理服务，主要提供管理的服务。第二层为办公网区域涵盖内网办公、运维管理等服务，提供对内办公的服务。第三层为生产区域，针对核电站反应堆、蒸汽-给水系统、反应堆辅助系统、安全应急系统进行较为真实还原，真实模拟核电生产区的管理和核发电能力。
13.	山东泽鹿安全技术有限公司	车机渗透场景	车联网综合测试靶场基于虚实结合技术，可实现对车联网核心组件的虚拟化，提供整车部件的车体组件资源库，包含多类仿真环境模板库，车载娱乐系统仿真、T-BOX 仿真、TSP 平台仿真、V2X 仿真、移动 APP 仿真、OTA 升级仿真，并且提供了的海量武器库、车联网安全典型场景库、漏洞库、全套课程资源、基于业务的资产分布视图，帮助安全人员对车联网设备快速开展漏洞研究、安全测试、风险预判、漏洞处置工作。	整车漏洞挖掘场景模拟了车载娱乐系统、车内总线等智能网联汽车相关组件，作用于车端整车的模拟仿真进行安全测试及研究。
14.		T-BOX 渗透		车联网漏洞挖掘场景模拟了 T-BOX、TSP 平台等智能网联汽车相关组件，作用于云、管、端车联网的模拟仿真进行安全测试及研究。
15.	北京顶象技术有限公司	水利水电水坝闸门控制系统	水坝控制场景最真实还原了水坝设施的工业控制系统，选手通过破解场最中的题目，实现对大坝闸门控制系统的攻击，能对现实场景	场景模拟了真实环境中水坝设施的工业控制系统使，选手对现实场景中黑客攻击水利水电系统有深刻理解。

16.		智能电网二次设备	中黑客攻击水电系统有深刻理解。电网二次设备场景是对智能电网中二次设备系统仿真，学员通过破解场景中的问题，使参赛选手深入了解目前电力系统中存在的网络安全风险。	场景模拟了真实环境中智能电网的二次设备，学员通过破解场景中的问题，使参赛选手深入了解目前电力系统中存在的网络安全风险。
17.	浙江木链物联网科技有限公司	电力仿真场景	网络靶场系列产品通过虚拟化、虚实结合组网等技术，能够低成本高效率的仿真出接近真实的网络环境。为网络攻防对抗训练、应急响应演练、攻防技术培训以及网络对抗工具评测研究等需求提供安全可靠的仿真试验场地。	场景模拟了火力发电厂在原料处理、炉膛燃烧、送风除尘、冷凝热交换、升压变电等一系列工艺流程，作用是通过该场景模型可看到受到攻击时的设施状态，攻防可视化平台会展示各类安全产品采集到的数据。
18.	上海云剑信息技术有限公司	用电场景	“电力工控数据安全靶场”系上海云剑信息技术有限公司研发的产品，该项目获得上海自然科学基金（面上项目）支持，应用在电力工控安全漏洞分析，电力系统未知病毒分析，公司系“国家工业信息安全漏洞库”的技术支撑单位。	场景模拟了智能电表数据采集，变频电机运行和家用灯泡照明，用于检验智能电表数据采集的安全性，变频电机运行的安全性，居民用电侧的安全性。
19.		FTU 通讯场景		场景模拟了 FTU 的数据传输，作用：用于检验 FTU 数据传输安全性
20.	国网浙江省电力有限公司电力科学研究院	火力发电场景	电力工控网络靶场是致力于发电、输电、变电、配电的工控系统仿真，电力信息系统安全监测、检测、攻防演练等研究的服务平台；是电力企业安全人才培养，电力工控网络安全技术研究的综合训练场。	场景模拟了热电厂与配电站的主要工艺流程，作用主要有：1.开展针对火力发电场景仿真环境的网络安全验证工作；2.针对验证得出的结果，开展网络安全技术研究，提高人员网络安全技能，提升全员安全意识，强化网络安全理念。

21.	国网湖北省电力有限公司电力科学研究院	综合场景-智能变电站、智能配电、岸电、综合能源采集	国网湖北省电力科学研究院以工业网络靶场为基础，建设覆盖变配用 3 大环节的仿真验证环境。支持继电保护，智能终端，合并单元，测控装置，FTU,TTU，智能电表，集中器等智能二次设备，可采集刀闸开关，变压器等一次设备参数，充分还原了现代智能电网的工艺流程，充分展现了一次设备智能化，二次设备网络化的特点。靶场内置 iec61580,iec104,mms,goose,sv 等电力专有协议 10 余种。	变电场景接入了继电保护，智能终端，合并单元，测控装置二次设备，可采集刀闸开关，变压器等一次设备参数；配电场景接入了 FTU,TTU 等设备，真实还原了智能配电场景。综合能源采集场景，配备了智能电表、集中器等主要设备，模拟用户用电采集环节。岸电场景包括：岸上的供电系统、电缆的连接设备、船舶的受电系统，模拟船舶船舶在靠港期间接入码头侧的电网，从岸上电源获得电力的工艺流程。充分还原了现代智能电网的工艺流程，充分展现了一次设备智能化，二次设备网络化的特点。
22.	重庆市工业高级技工学校	工控协议仿真场景	在国家关键信息基础设施、典型工业仿真基础设施重点策划下，依托工业平台，提供工业仿真环境，全面模拟能源、电力、交通等关键信息基础设施行业，展现各个不同行业的真实物理设备、网络组成以及工艺流程。	模拟了工业发电与制造监控，作用还原真实工业生产场景
23.	国核自仪系统工程有限公司	新能源发电场景	工控网络安全攻防靶场整体设计结合发电行业典型系统特征，搭建了火、风、光、水、核、储典型的不同发电类型电站的仿真系统场景，实现各类型电站电力监控系统的攻防实战演练环境，以研究电力监控系统网络安全	本环境包括火力发电仿真场景、风力发电仿真场景、光伏发电仿真场景、水力发电仿真场景，场景模拟了各类型电站电力监控系统典型运行模式及工艺流程，以研究电力监控系统网络安全攻防技术，挖掘系统漏洞。

24.		核能发电	攻防技术，挖掘系统漏洞。	本场景为核能发电仿真场景，通过生产控制层、数据分析层、数据存储层仿真典型核能发电仿真环境，通过渗透测试和漏洞挖掘的手段以研究在核能发电场景中的网络安全攻防技术。
25.	金川集团股份有限公司	综合场景-矿山提升、磨矿浮选、铜合成炉、镍电解槽、羰化合成、PVC 净化	工控安全仿真演练系统搭建了有色冶金行业典型的网络安全仿真环境，呈现了有色金属采、选、冶及化工新材料全产业链关键流程，承担金川集团工业网络安全综合监测系统的呈现。工控安全仿真靶场平台具备开展工控网络攻防演练、攻防实训、测试验证、应急演练和安全培训等功能。	本综合场景包括：矿山提升场景，展现的是网络对采矿过程中破碎和提升生产的控制系统的攻防模拟。磨矿浮选场景，展现的是网络对选矿过程中磨矿和浮选工序生产的控制系统的攻防模拟。铜合成炉场景，展现的是网络对有色金属火法冶炼过程关键炉窑的控制系统的攻防模拟。镍电解槽场景，展现的是网络对镍湿法冶炼中电解槽的控制系统的攻防模拟。羰化合成场景，展现的是金川公司特色的粉末冶金中羰基镍合成转动釜控制系统的攻防模拟。PVC 净化场景，展现的是化工新材料 PVC 生产过程中净化工序关键设备的控制系统的攻防模拟。

26.	江西省网络安全研究院	城市水务攻防演练沙盘	靶场模拟自来水厂的水处理净化过程，真实复制了自来水厂的原水池、调节池和消毒池的水处理过程，更接近真实自来水厂的工艺环节和控制系统。整体网络采用典型工控网络三层结构，包含门户网站、OA 办公系统、域控、办公终端、操作员站及工控设备等。	场景模拟了典型城市供水生产工业控制网络和管理办公网络，仿真了自来水处理净化过程各生产环节的工艺流程，设计了原水井、加氯间、消毒间、絮凝沉淀池、V 型滤池、送水泵房等。并结合工控系统常见威胁，在关键工艺环节预置了多种漏洞，在教育教学、工业培训、攻防演练等方面得到广泛应用。
27.	烽台科技（北京）有限公司	变电站场景-铁丝熔断	烽台科技（北京）有限公司（以下简称烽台科技）成立于 2015 年，是一家专业面向工控安全领域，提供专业化、标准化工控网络安全咨询与评估服务、工控网络安全产品研发与销售、综合一体化网络安全防护解决方案的高新技术企业。总部设于北京，在成都、贵州、哈尔滨、天津等地区设有分支机构。主要服务于政府、行业客户、设计院/所、科研院/所、	此场景高度还原了典型的继电器控制系统。继电器控制系统一般由主令电器、接触器、继电器和导线等部分组成,其逻辑功能由传统的继电器来完成的，控制方式包括了点动控制、自锁控制、互锁等控制方式。

28.		智能制造-焊接工业	集成商及软硬件厂商，通过可视化、专业化的产品和技术，协助用户进行有效的风险管理与可靠的运营支撑。	智能制造场景主要模拟汽车焊接工序，将采用两套工业级机器人模拟焊接工艺，系统部署探针、厂区 SEAM 集团级 SEAM，对场景中所有工控设备进行集中监测与管理，突出保障体系全生命周期管理与运维的特点。
29.		火力发电-汽水循环		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。
30.		石油开采-磕头机		此场景模拟采油工艺，系统由采油工程实物装置，仪表、手操阀、机泵，PLC 控制器及工作站组成。 实物装置设备的尺寸将真实采油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； PLC 控制器负责将现场设备及仪表信号收集、处理、运算实现装置自动控制，并将数据上传上位机工作站进行人机界面交互。

31.		化工炼化-蒸馏塔		此场景模拟化工常减压、催化列化工艺，系统由化工工程实物装置，仪表、手操阀、机泵，PLC 控制器及工作站组成。实物装置设备的尺寸将真实化工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; 此场景主要模拟某真实化工厂网络拓扑及防护方式。在系统中部署隔离网闸、防护墙等安全防护设备，主要起到边界隔离作用。通过此场景的模拟，突出边界隔离的特点。

32.	哈尔滨工大天创电子有限公司	综合场景（生物制药、炼化场景、石油储运、发电场景【发电输送】、采油场景【蒸馏工艺】、核电场景）	哈尔滨工大天创电子有限公司在网络安全防御技术方面以展开多项创新技术研究并形成了相关知识产权，已申请 10 余项蜜罐、安全监测等相关核心技术的国家发明专利。在网络安全防御相关产品的开发方面具有丰富与领先的技术经验，研发安全数据采集设备、蜜罐诱捕设备、工业安全监测平台、工业网络信息安全测试验证环境等产品，为安全厂商提供 OEM 等产品服务。公司产品已在石油、化工、钢铁、燃气、交通、政府等行业上百家以上大型企业或单位进行了应用，广受行业用户好评，具有良好的技术积累和产业应用基础。	本场景覆盖生物制药、石油炼化、石油储运、电力输送、采油蒸馏、核电等多行业工艺，复现复杂工业网络。
33.	成都烽创科技有限公司	综合场景-智能制造、风力发电、火力发电、智慧城市	成都烽创科技有限公司以运营工业互联网安全产品及服务为愿景与经营目标，专注于工业信息安全领域，致力于工业控制系统（ICS）、机器人、智能网联汽车、无人机、5G+工业互联网相关的安全研究与实践，主要提供专业化、标准化安全业务咨询、评估服务，为工业企业和行业用户开发和设计完整、有效、适合业务发展的管理方法，从而提升并强化用户在工业信息安全方面的防护能力。	本场景覆盖智能制造、风力发电，火力发电，智慧城市等多行业工艺，复现复杂工业网络。

34.	贵州烽创科技有限公司	综合场景-火力发电、采油联合站、石油化工	贵州烽创科技有限公司是一家专注于网络安全的技术企业，自成立以来，以技术体系和应用模式的不断创新为企业核心竞争力，凭借长期的技术积累、阶段性研发成果及多行业的项目实施经验，已经在 5G+工业互联网安全领域形成强有力的产品体系和技术框架，目前已研制多套工业网络靶场平台，覆盖汽车制造、电力、轨交等行业，并已在多个行业得到广泛应用。	本场景覆盖火力发电，采油站，石油化工等多行业工艺，复现复杂工业网络。
35.	江苏省电子信息产品质量监督检验研究院(江苏省信息安全测评中心）	综合场景（智能制造、智慧水务、城市燃气、轨道交通、火力发电、智能楼宇）	江苏省信息安全测评中心网络安全综合演练实验室建立工业网络靶场结合电力、智慧城市、物联网等行业实物仿真装置，构建重点行业工业互联网仿真环境，可开展攻防演练、教育培训以及测试验证等工作，并最终通过公共服务平台，形成资源共享能力。依托于网络安全综合演练实验室，江苏省信息安全测评中心已开展系统设备检测评估、地方工控竞赛支撑、地方工控企业人才培养等工作。	本场景包括燃气仿真场景仿真城市配气站，火力发电，轨道交通，智能楼宇和智慧水务。包括供气管路，电磁阀门，气泵，锅炉，汽轮机，发电机，交通灯、轨道交通控制系统，智能家居控制面板，窗帘电机，控制开关，智能网关，循环泵变频器等主要组件。