1.1 案例七：某省电科院新能源工控网络安全实验室建设方案——新能源网络安全多功能演兵场

1.1.1 方案概述

通过建设电力行业新能源工控网络安全实验室，构建调光伏组件系统、综合自动化系统、光伏发电功率管控系统、箱变和逆变器系统、升压站系统、天气预报系统、办公网络等，为新能源场站网络安全防护技术研究、攻防实战演练提供必要的仿真环境。针对电力行业关键信息基础设施网络安全保护与测试验证，开展新能源场站工业控制系统信息安全评估、测试、攻防竞赛、应急演练、技术培训等工作，将有力提升地区电力行业整体工控安全研究水平。

1. 方案背景

电力是国家的支柱能源和经济命脉，其安全稳定运行不仅关系到国家的经济发展，而且维系国家安全。随着电网规模的逐渐扩大，安全事故的影响范围越来越大，安全问题越来越突出，电力网络安全运行已经成为全球的研究热点。

当前，世界各国在网络空间的投入不断加大，网络军备竞赛愈演愈烈。国家行为体参与的网络犯罪活动日益猖獗，所使用的工具和手法越来越先进，利用网络攻击破坏电力等国家关键基础设施已成为现实，自网络空间向物理电网发起攻击成为当前大国博弈、大规模战争的重要手段。

电力行业的工业信息系统作为国家关键基础设施的重要组成部分，很容易成为国家之间网络对抗和有组织黑客的攻击目标，电力行业信息安全面临着严峻的形势。

2. 方案简介

新能源工控网络安全实验室是一个仿真的网络安全、产品测试、教育培训、漏洞挖掘和风险评估的虚拟训练场。新能源工控网络安全实验室的第一目标是提供关键信息基础设施和工业控制系统训练环境，训练网络安全人员如何防御关键网络设施受到攻击，以及如果针对假定目标实施网络攻击。此外还可以针对仿真网络场景进行风险评估、记录攻防行为、提供大型关键信息基础设施和工业控制网络仿真复现、支持攻防演练、教育培训等事件复盘、为安全产品提供测试展示平台等功能。

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。

3. 方案目标

（1）现有安全问题

当前 IT 和 OT 融合发展趋势加速，新能源行业智慧转型离不开新兴的云计算、大数据、物联网、人工智能等技术的支撑，传统的安全威胁和新技术带来的新型安全风险将交织扩散，给风力发电、光伏发电造成巨大安全威胁。除了环境条件恶劣、运维成本极高、远程通信困难、风场可利用效率不高的挑战外，新能源场站并网后也同样面临 APT 组织的网络战级别的各种攻击，如勒索攻击、蠕虫病毒、远程操纵等定向攻击。在基础结构安全方面则表现为典型的物理安全、设备运行数据安全、远程运维网络安全等突出问题。

- **物理安全风险**

现场设备防护措施不到位，面临暴力入侵。设备分布区域广，普遍人烟稀少，预防预控成本高；对风机及光伏阵列运行状态的自动化

监视程度和巡检人员网络安全技术水平低。

- **设备运行数据安全风险**

新能源场站生产运行数据主要存储于风机控制器、光伏矩阵监控系统、风机监控系统服务器、升压站综自系统服务器、风功率预测系统服务器、光功率预测系统服务器、在线振动监测系统服务器以及中控室内的各操作员站主机内。面临系统弱口令、服务器加固不及时、调试端口、空闲端口未关闭、冗余配置不到位、移动存储介质乱用等等问题。

远程运维网络安全风险；

安全防护对厂家或设备供应商依赖度高；

边界防护设备缺失；

风场与调度数据网边界未配置纵向加密装置；

边界防护装置安全策略配置不规范。

同时，与常规能源不同的是，新能源场站的发电终端数量较多且户外分散分布，恶意攻击很容易通过发电终端渗透到站控层及各类业务应用中。因此部署新能源并网发电环境，开展新能源场站并网发电工控安全研究、隐患发现、漏洞验证、攻防演练和人才培养等工作对公司电网安全意义重大。

2.安全目标

（1）打造完善工控安全课程体系

工控网络安全是一个综合、交叉的学科领域，涉及数学、物理、通信、计算机、自动化、管理等诸多学科领域的知识和最新发展成果，同时该专业也是一个实践性很强的专业。因此，应以电力行业需求为导向建立科学的课程体系，课程体系中应理论基础与工程实践并重，注重参训学员的综合素质和自学能力的培养，加强自动化、计算机网

络和实践课程的训练；确立核心课程，并在保证工控安全专业教育的基础性、全面性的同时，并按照其内容联系、应用需求、岗位需求、竞赛需求等划分成若干个课程模块，建立“理论教学+安全实操”的多模式相结合的创新的教学模式，促进学员安全能力的全面掌握。

（2）加强红蓝方实战对抗水平

“红队攻点、蓝队防面、以攻促防、全面消缺”，全面提升电力行业新能源场站网络安全人才梯队的工控网络安全“战时”水平，培养复合型人才，提升专业技能，并可有效提高该地区新能源场站网络安全“战时”应急响应能力。

（3）构建工控安全实训基地

建成的新能源工控网络安全实验室既可以为某电科院相关研究人员提供实战对抗的环境，也有能力为行业内相关从业人员提供培训环境。通过这种理论与实践结合的特色教学模式，以及工控网络安全实验室涵盖的工控网络安全各领域的丰富实验内容，实现参训学院安全意识和实操能力的快速提升，最终实现培养新能源领域工控网络安全专业人才的目标，并成为地区特色电力工控网络安全实训基地。

1.1.2 方案实施概况

电力行业新能源工控网络安全实验室依托于工业网络靶场平台和电力行业仿真装置，构建电力行业典型业务虚实结合仿真场景，提供现场工艺设备、工业控制设备、工业系统软件等资源，能够针对现场数据进行深入分析、展示，其中包含攻防演练过程数据、攻防研究测试数据、网络运行实时数据、工业安全监管数据。电力行业新能源工控网络安全实验室建成后可开展工业控制系统信息安全评估、测试、攻防竞赛、应急演练、技术培训等工作，能够帮助电业行业搭建高效快速的安全团队，构建安全便利的工控系统准入机制，实现某电科院

工业互联网安全防护能力的整体提升。

1. 方案总体架构和主要内容

（1） 总体架构

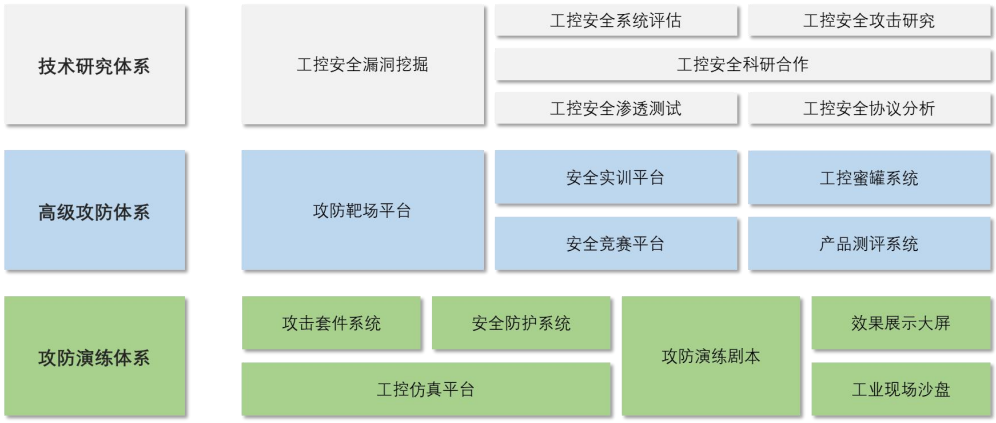

图 7-1 新能源工控网络安全实验室总体架构图

平台采用分层递阶的设计思路进行设计，整个平台具备稳定性好、可信度高、扩展性强、维护便利的特性。

攻防演练系统：是整个平台的基座，通过工控仿真平台 100%还原新能源场站生产场景，并部署攻击系统、安全设备系统、工业现场沙盘和效果展示系统，为安全应用系统和技术研究系统提供基础支撑。

安全应用系统：通过工控靶场系统配置网络资源，利用攻击套件系统和安全设备系统实现攻防对抗，同时可开展攻防比赛和安全实训。现场沙盘和效果展示系统与生产场景联动，可对攻防比赛和安全实训结果进行可视化展示，有效提升培训效果。系统内置流量分析系统对全场景、全周期的数据进行收集，实现攻防分析和复盘推演。

技术研究系统：在攻防对抗过程中，对现有安全系统、攻击技术进行深入研究。同时也可在仿真平台的基础上，模拟或接入专有工控系统，完成渗透测试、协议分析和漏洞挖掘等工作。

（2）总体流程

- 根据剧情所设定的工控系统典型场景进行仿真部署，对工控系统设备、网络、安全产品进行布置并完成相应参数配置；
- 模拟网络攻击、用户异常操作、非法入侵以及蠕虫、病毒等各类攻击源对工控系统的多个层面进行渗透攻击，对攻防数据进行采集并记录；
- 综合分析攻防演练态势，对目标工控系统进行多维度综合分析评估，精准评测评估目标工控系统的安全性、可恢复性和灵活性；
- 以可视化方式实时呈现工控系统网络拓扑情况、安全产品部署情况、攻防演练态势、测试评估统计分析及结果等内容。

2. 网络、平台或安全互联架构

（1）演练场景规划与编辑

通过搭建新能源场站生产现场的仿真平台，实现对于真实设备、系统的还原。

由于工控安全攻击事件多是针对上位机、下位机、上位机和下位机之间的网络进行攻击，而攻击的结果多是影响到执行器这一层面，因此最基础的工控仿真平台应当具备如下几个特点：

- 具有电力行业工控系统代表性
- 完整的“上位机-下位机-执行器-传感器”架构
- 具备丰富鲜明的展示效果
- 能够实现对于著名工控事件的还原和深度解读，从而起到教育意义
- 能与工控安全实验室中的其他系统进行联动

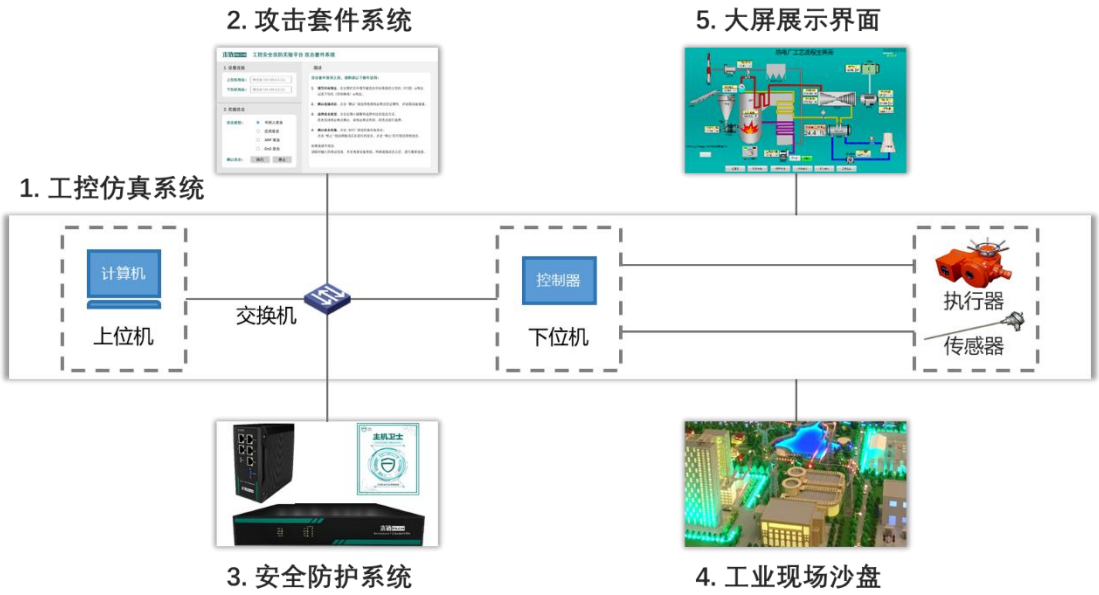

图 7-2　电力行业工控安全实验室演练场景规划示意图

（2）安全攻防演练与监测

要实现完整的安全攻防演练，在工控仿真平台的基础上，还需要各类攻击手段以安全防护系统进行对抗演练。安全攻防演练与监测系统主要包括两部分，即安全防护系统，以及攻击套件系统。

攻击套件系统提供一些工控环境中常见的攻击手段，包括嗅探、IO 点篡改、中间人攻击、U 盘攻击、泛洪攻击、DoS 攻击等等。

安全防护系统提供业界常用的主流安全防御体系，如工业防火墙、工控审计平台、主机卫士等等。

（3）安全防护效能评估

依靠安全防护系统能够实现针对病毒、攻击的防御，但并不能做到提前发现系统薄弱环节，预知安全事件的发生，安全防护效能评估系统提供对于系统内资产、安全设备的有效管控，同时能够进行针对漏洞、流量的分析管理，增强系统安全防护能力。

（4）安全效果综合呈现

考虑到工控网络安全实验室不仅承担着辅助技术人才进行演练提升的作用，还承担着人才安全意识培养、安全事件分析、安全制度

优化、应急响应培训等各类职责，需要面向组织中各个级别、每一位学员，因此如何呈现攻防演练的过程及结果，这也是工业控制系统安全攻防演练平台建设的一项重点。

安全效果综合呈现系统主要包括两部分，电力行业工业沙盘，以及大屏展示界面。

通过直观、形象演练功能的工控沙盘，有效还原新能源场站发电业务的现场情况，方便参观者了解电力系统业务流程、现场情况，以及安全事件发生前、中、后阶段，会造成的各类实际影响。

通过定制化的展示界面，可以通过大屏幕展示，直观了解攻击事件的发生流程，从哪些设备侵入、干扰哪些系统，从而能够深入理解工业控制系统安全的严重性，增进对攻击事件的理解，吸取未来应该如何做安全防范、应急响应的经验。

3. 具体应用场景和安全应用模式

新能源工控网络安全实验室的建设以培养能够适应现阶段电力行业工控网络安全需求的综合性人才和开展实战化攻防演练来提升新能源场站工控网络安全防护与应急响应能力为目标，通过新能源工控网络安全实验室的建设，可以有效的提高电网的工控安全人才的综合能力，改善现阶段专业人才缺乏的现状，通过强化理论知识学习，培养实践操作能力，实现理论与实践的有机结合，并周期性开展“战时”攻防演练，在促进新能源工控网络安全人才素质能力全面提升的同时，也为某电科院工控安全科研支撑提供有力环境。

（1）新能源光伏场站仿真平台建设

新能源光伏场站仿真平台通过控制系统和新能源光伏场站生产仿真场景物理沙盘组合而成，按照新能源光伏场站典型模块化柔性生产线工艺场景定制，仿真模型台大小为 2m * 2m，接入控制系统由控

制设备进行控制，仿真模型台为新能源光伏场站典型微缩示意模型，是以新能源光伏场站为原型，开发的机电一体化教学、实验、实训综合应用平台，使研究和参训人员对光伏发电的实际过程有大体的了解，掌握光伏发电过程一些实际应用技术。并较好地解决了自动控制系统只能看不能操作，达不到理想的攻防演练和教学效果的问题。此外，新能源光伏场站仿真平台还可向参展人员展示新能源光伏场站正常生产控制流程及攻击、防护效果。

新能源光伏场站仿真平台沙盘通过高度还原新能源光伏场站生产设备和关键工艺流程实现真实场景模拟，包括光伏组件阵列、逆变器、箱变、交流柜、升压站等工艺，考虑到风光互补场景，还应包括风机，以还原整个生产场景。该系统是将机械传动技术、声光控制技术、姿态跟随系统、PLC 控制技术和系统工程有机的融于一体，是现新能源光伏场站生产全过程的缩影。整个软件系统，整合了控制软件，组态软件，数字工厂仿真软件等。软件功能充分体现工业 4.0 的应用功能。它既符合工业自动化生产实际又能满足自动化控制、虚拟融合等专业创新、实验、实训教学需要。

控制系统采用市面主流的系列 PLC。每个工作站的控制单元由 PLC、传感器、执行机构、光伏组件整列转动机构组成。PLC 根据输入信号和用户程序，执行相应的计算和控制过程，并输出各种控制信号，实现对各单元的自动控制。每个工作单元 PLC 都装有组态监控软件，监控本模块的运行。

SCADA 系统集成了数据采集模块，品质模块，定单模块，设备维护模块，报表模块，看板模块。SCADA 系统通过以太网，连接每站的 PLC。通过 Modbus 实现对个工艺流程的工作过程数据管理，SCADA 实时采集 PLC 工作过程数据。把生产的进展数据，通过看板显示在大屏

幕上。并可通过 HMI 实时查看生产数据。

- **新能源光伏场站总控制台**

新能源光伏场站仿真平台总控台 PLC 系统使用市面上主流的系列 PLC 设备，集成的 通讯接口用于 HMI 通信和 PLC 之间通信。此外还通过开放的以太网协议支持与第三方设备的通信。

整个控制系统利用工业级交换机，建立设备之间的通讯网络。

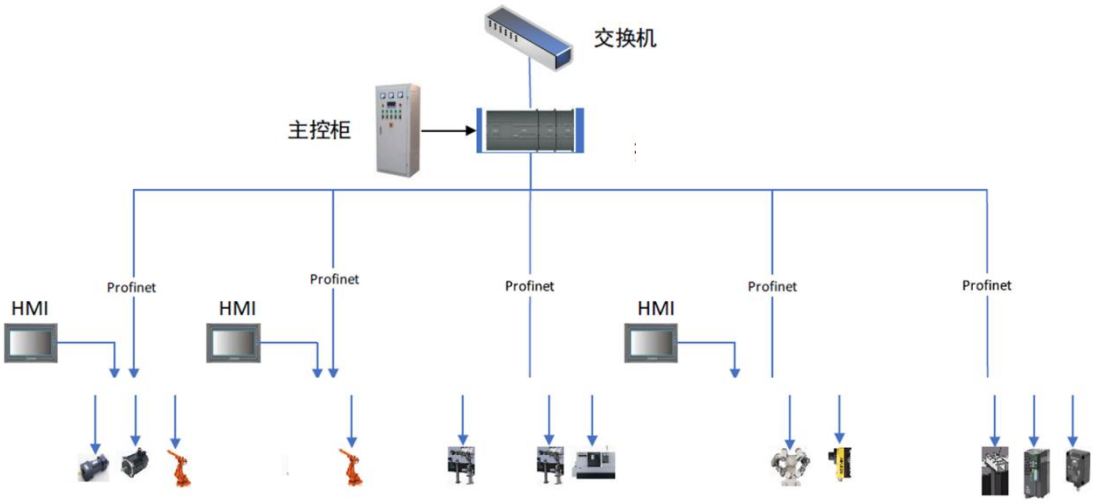

图 7-3　新能源光伏场站总控制台

主控柜（主控板）安装有光伏发电场站专用控制器，用于光伏发电流程的统一调度与各子系统之间协调控制。

例如可实现以下功能：

光伏组件的工作控制：从上位机软件系统接受信息，控制光伏组件的方向转动和工作状态。

实现箱变、逆变器运行模式控制：运行/停机/故障报警。

实现升压站运行模式控制：运行/停机/故障报警。

实现各子系统工作协同控制：对各系统的状态进行统一调度管理。

各子系统分别安装 PLC 控制器，用于子系统的运动执行机构、传感器等设备的控制与数据采集。各子系统 PLC 相互独立，单系统故障不会影响其它系统的设备状态。各子系统 PLC 均受专用光伏发

电场站控制器统一调度控制。

- **功能结构及任务流转**

新能源光伏场站仿真平台还原光伏发电流程，模拟仿真的生产流程如下图所示：

图 7-4　新能源光伏发电工艺流程

- **新能源光伏场站控制系统**

新能源光伏场站仿真平台的控制系统采用真实控制设备，模拟光伏发电过程。本实验室新能源光伏场站仿真平台采用各厂商主流型号 PLC 设备。包含控制器、工业交换机、操作员站、工程师站几类自控组件。自动控制系统挂置于工控安全实验室中心挂板上。

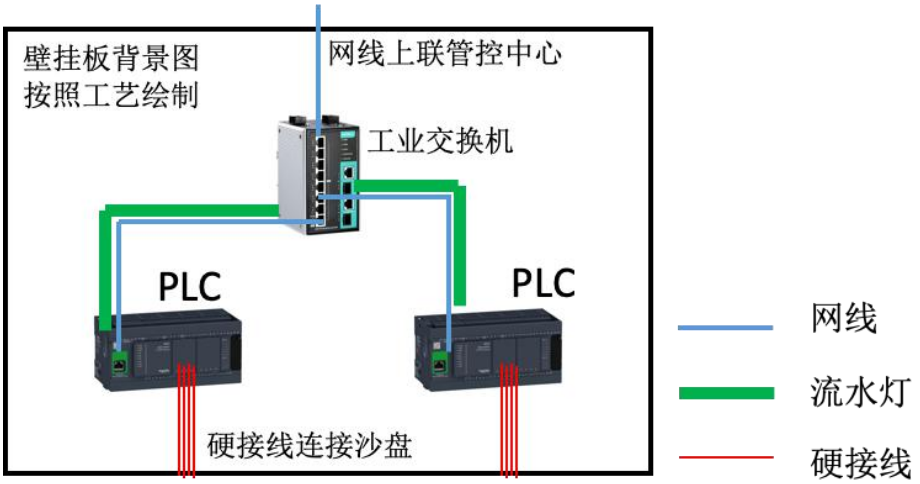

图 7-5　自动控制系统挂置于工控安全实验室挂板的示意图

图 7-6　壁挂板效果图参考图

控制设备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；

新能源光伏场站仿真平台建设所选择现场控制设备为新能源场站主流控制设备品牌型号，共包含 4 套 PLC 设备，控制设备均配置以太网模块，用于同操作员站、工程师站实现网络连接；控制设备配置

DI/DO，同现场沙盘连接，实现沙盘内机械转动装置、声音报警器、灯带、开关和计数器等的控制以及数据采集。

新能源光伏场站仿真平台组态软件安装于操作站上，可通过组态软件控制现场设备停车、运行过程中操作、监控，并对外开放 OPC Server 服务。

新能源光伏场站仿真平台建设所选择的组态软件为三维力控公司的组态软件 ForceControl7.0（也可采用其他），具有良好的兼容性、稳定性，与西门子、ABB、施耐德、罗克韦尔的 PLC 互联，按照新能源光伏场站工艺特点实现组态界面，实时监视、控制现场设备运行。

新能源光伏场站仿真沙盘

新能源光伏场站仿真场景沙盘按照光伏发电场站真实环境定制，仿真模型台大小为 2m*2m，接入控制系统由控制设备进行控制，仿真模型台为光伏发电场站发电生产模型，向参展人员展示光伏发电生产控制流程及攻击、防护效果。

场景模拟：场景根据实际光伏发电场景定制，等比例缩小仿真。沙盘示意图及展示效果如下：

图 7-7　新能源光伏场站仿真场景沙盘效果图

图 7-8　新能源光伏场站仿真场景沙盘示意参考图

沙盘通过微缩物体实现真实场景模拟，根据光伏发电工艺流程、

业务特点形成沙盘场景，包括光伏组件阵列、箱变、逆变器、升压站等不同工艺流程，多个工艺流程组合形成整个光伏发电场景。

新能源光伏场站仿真平台沙盘场景内各工艺段有可操作控制点，可操作控制点通过接线与 PLC 相连，由 PLC 控制进行相应动作，通过不同的动作内容对比模拟仿真系统正常工作与遭受攻击情况所造成的现场影响，包括影响位置、影响路径及影响结果。

场景内可操作控制点包括：

等比例缩小光伏组件：按照实际光伏组件等比例进行缩小，简化机械转动等细节工作内容，能够通过 PLC 控制机械转动装置，带动光伏组件以不同速度、不同方向的做启停和旋转动作。

计数器：按照实际工艺在沙盘内放置计数器，对于通过计数器探测范围零件进行计数，计数结果反馈给组态软件，组态软件进行相应显示，数量达到设定值后，停止机械转动、逆变器工作等动作。

流水灯：流水灯铺设于沙盘内主要业务流程中，由流水灯引导参观人员了解正常发电流程。流水灯分为绿色、红色两种灯光颜色和高、中、低流水速度以及正向、反向流水方向。用于展示当前模拟场景设备运行状况、发电负荷等。

背景灯光：背景灯光采用微型 LED 矩阵式铺列于沙盘各工艺流程内，通过不同矩阵呈现不同工艺区域。通过灯光开、关及闪烁状态展示灯光所处区域内安全状态，正常情况为灯光开启，遭受攻击后对应区域灯光闪烁，攻击导致生产中断后对应区域灯光关闭，代表区域生产停止。

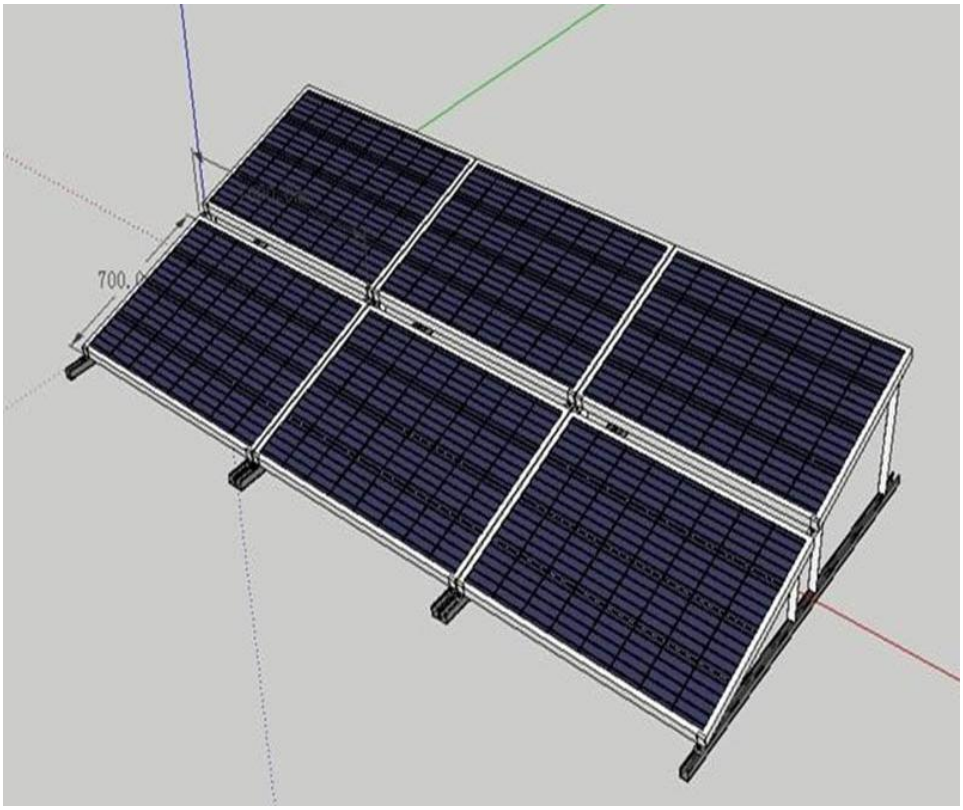

图 7-9 光伏组件参考图

图 7-10　光伏箱变示意图（参考）

图 7-11 光伏逆变示意图（参考）

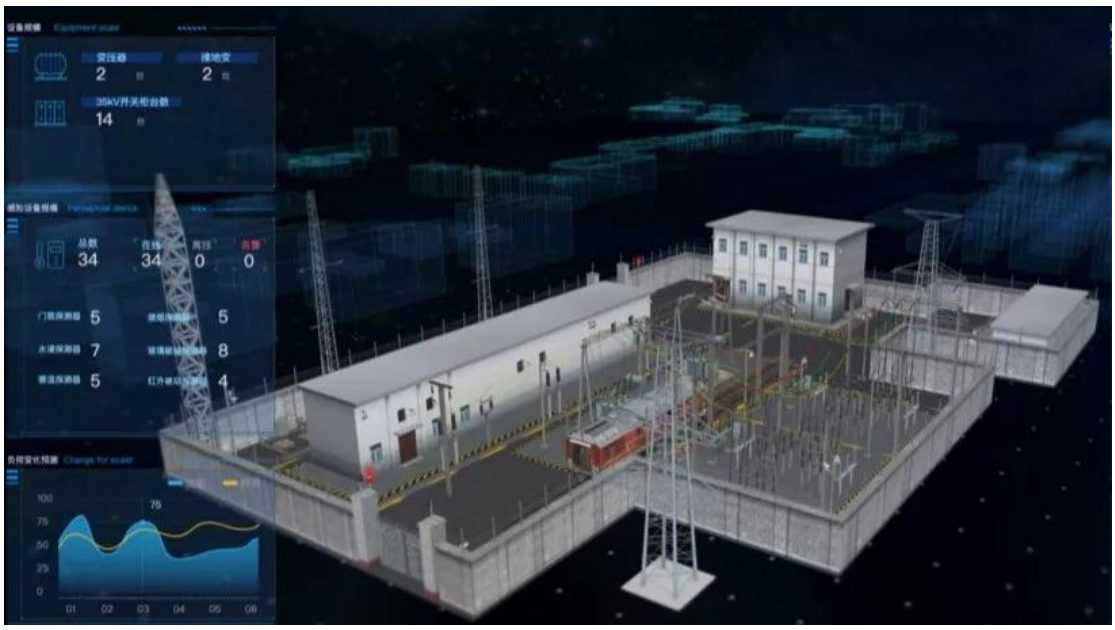

图 7-12 升压站结构图（参考）

新能源光伏场站虚拟沙盘：新能源光伏场站仿真场景沙盘采用数字孪生技术，对新能源光伏场站进行数字孪生，通过和控制系统以及物理沙盘的联动，更加直观、量化的展现新能源光伏场站的工作状况。

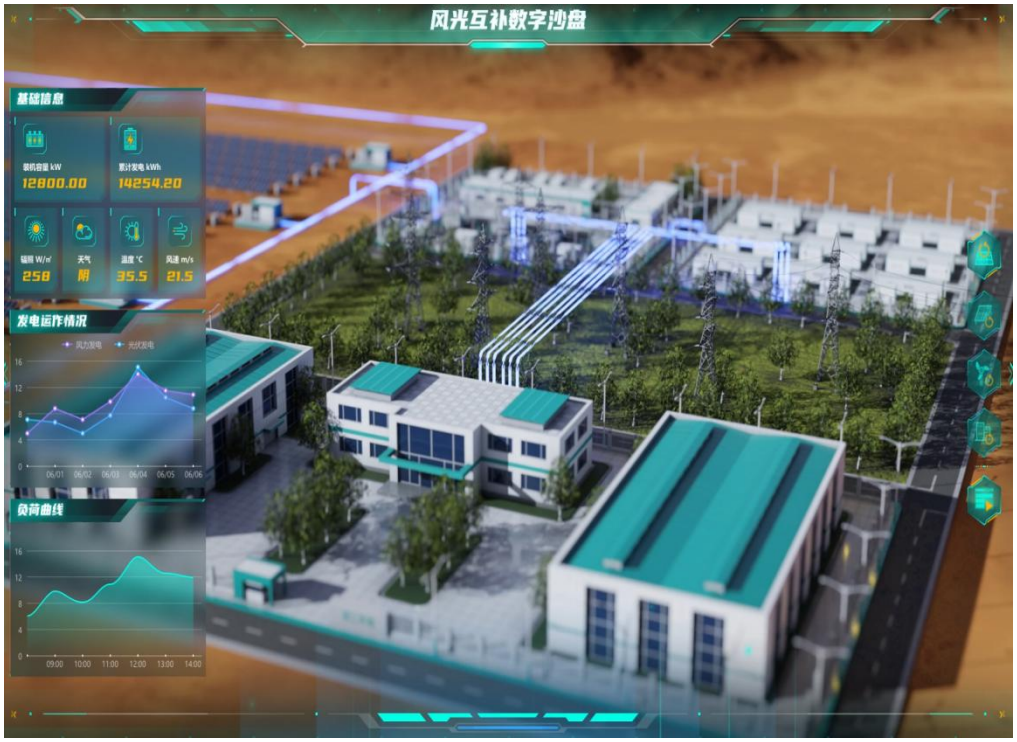

图 7-13　新能源光伏场站虚拟沙盘效果图

（2）新能源光伏场站攻防设计

➢　攻防演练流程

新能源光伏场站仿真平台将作为标靶，工业网络靶场负责提供实验网络环境组网和安全设备灵活集成接入和网络隔离的资源管控，并提供虚拟机服务器，在受防火墙保护的服务器组里配置了实验实训的攻防靶标服务器，并通过靶场安全竞赛系统配置攻防演练任务和攻防演练可视化大屏展示和安全监测分析功能，结合每次攻防演练和实验科研内容，设置具有一定脆弱性的网络服务，提供了攻击演示和验证性实验的环境。实验 PC 组的网络设置方式有效支持了对抗性攻击演练。

具体的攻防演练流程设计如下：

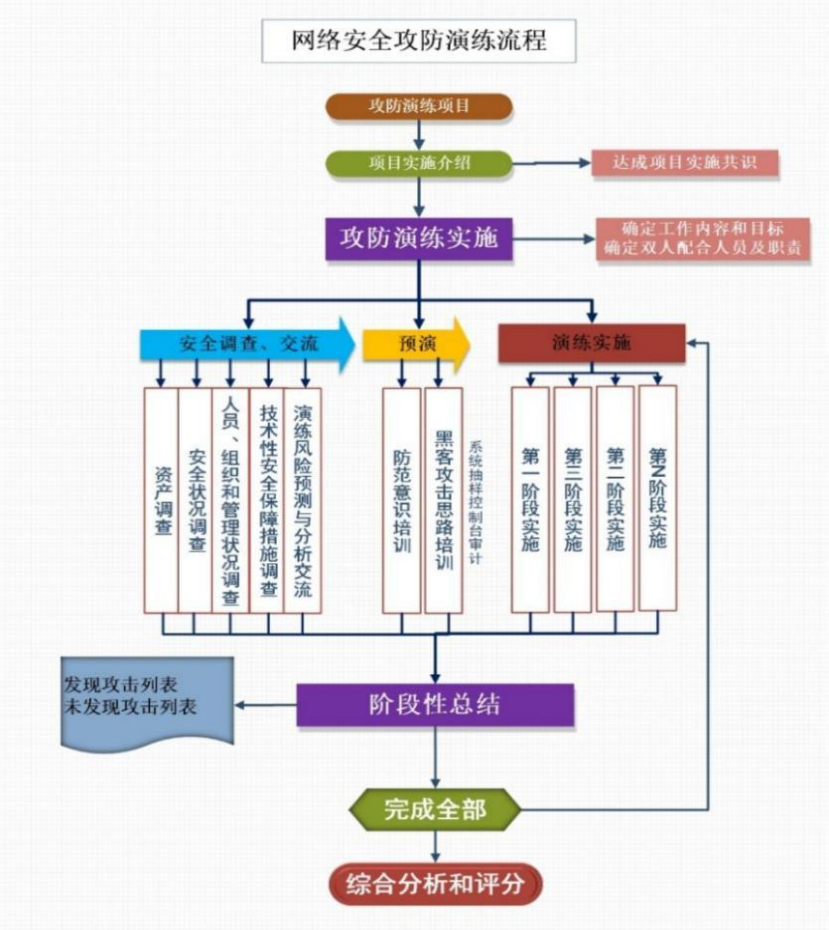

图 7-14　攻防演练流程概览（参考）

- **攻击套件设计**

针对新能源光伏场站仿真平台，设计的攻击套件如下：

序号	攻击套件名称	描述	效果
1	新能源光伏场站仿真平台DoS攻击脚本	模拟黑客伪装成运维人员进行PLC拒绝服务攻击	通过DoS攻击套件无限次给控制器发送合法指令,导致其崩溃
2	新能源光伏场站仿真平台病毒攻击脚本	模拟PLC 病毒在控制器间传播导致控制网络瘫痪	PLC设备感染病毒后设备宕机
3	新能源光伏场站仿真平台控制器数据篡改脚本	模拟黑客网络嗅探篡改操作指令造成PLC错误动作	篡改后控制指令导致PLC出现误动作
4	新能源光伏场站仿真平台指示灯任意控制脚本	对PLC中的寄存器进行数据篡改造成对指示灯任意控制。	可根据脚本提示输入对指示灯任意控制,如指示灯亮或灭
5	新能源光伏场站仿真平台arp欺骗攻击	模拟黑客网络嗅探对网络发起ARP攻击	成功使用arp欺骗攻击获取PLC和SCADA的通讯数据，造成信息泄露
6	新能源光伏场站仿真平台arp欺骗数据篡改	模拟黑客网络嗅探对网络发起ARP攻击,实施工控协议数据篡改	使用arp欺骗进行数据篡改,导致scada上显示的数据非真实数据
7	新能源光伏场站仿真平台恶意流量攻击脚本	使用peach工具构造非法流量对PLC进行攻击	服务软件崩溃，拒绝服务
8	新能源光伏场站仿真平台工业主机web拒绝服务攻击脚本	模拟黑客进行工业主机的Web发起攻击	利用攻击脚本发送超长get请求造成组态软件的web服务软件崩溃，拒绝服务
9	新能源光伏场站仿真平台工业主机暴力破解攻击脚本	模拟黑客进行工业主机的发起暴力破解攻击	使用工具暴力破解工业主机telnet服务并且连接telnet获取系统控制权限
10	新能源光伏场站仿真平台控制系统任意文件上传getshell	模拟黑客进行对SCADA进行任意文件上传getshell攻击	使用SCADA文件上传漏洞获取工业主机控制权限
11	新能源光伏场站仿真平台HMI未授权访问调用系统程序	模拟黑客进行对HMI进行未经授权的访问攻击	使用HMI TELNET服务进行未授权访问控制HMI
12	新能源光伏场站仿真平台HMI SNMP默认口令获取信息	模拟黑客进行对HMI进行SNMP的口令攻击	利用HMI 默认口令获取HMI系统信息

- **攻防演练效果设计示例**

根据具体的攻防演练流程及攻击套件设计，结合新能源场站仿真平台的工艺和控制系统，我们设计的攻防效果展示参考如下：

正常工作场景下，光伏组件机械转动按照设定旋转速度、旋转方向动作；箱变和逆变器按照设定正常工作，状态指示灯和网络状态之时等待为正常运行；计数器正常显示累计发电量，并上报数据在组态界面显示，计数达到特定值后，重新开始动作。各区域背景灯光正常开启，持续保持正常亮度，代表各区域安全状况良好，生产正常运行。

拟设计攻击场景包括病毒传播、黑客入侵等多种攻击类型：

第一种是模拟黑客伪装成运维人员进行 PLC 拒绝服务攻击：

新能源光伏场站仿真平台中所选择 PLC 存在拒绝服务类安全漏洞，入侵者能够通过构造特定结构的数据包发送给 PLC 导致 PLC 设备拒绝服务。

模拟场景中，黑客伪装成运维人员接入现场控制网络针对控制传送带的 PLC 进行运维。但黑客通过运维电脑连接其他未经授权的 PLC 设备，打开事先准备好的攻击包，针对控制光伏组件矩阵机械转动装置的 PLC 发起攻击，发送数据包。

首先光伏组件矩阵区域背景灯光闪烁，代表此区域受到网络攻击。PLC 设备收到数据包后设备指示灯闪烁，故障灯亮起，设备宕机。机械转动装置原有动作停止，光伏组件矩阵区域生产工艺段流水灯颜色由绿变红代表此工艺段故障。此区域背景灯光由闪烁转为关闭，代表此区域生产中断。

第二种是模拟 PLC 病毒在控制器间传播导致控制网络瘫痪：

模拟场景中，将感染病毒的 U 盘插入工程师站，病毒自动扫描探测控制系统内可被感染 PLC 设备，传播至第 1 台 PLC 设备后，继续探

测其他 PLC 设备并依次感染。PLC 设备感染病毒后设备依次宕机。

首先光伏组件矩阵机械转动装置区域背景灯光闪烁，代表此区域受到网络攻击。PLC 设备感染病毒后，设备宕机。机械臂原有动作停止，光伏组件矩阵机械转动装置工艺段流水灯颜色由绿变红代表此工艺段故障，此区域背景灯光由闪烁转为关闭，代表此区域生产中断；然后箱变和逆变器区域背景灯光闪烁，代表此区域受到网络攻击，紧接着宕机，箱变和逆变器停止原有动作，箱变和逆变器工艺段流水灯颜色由绿变红代表此工艺段故障，此区域背景灯光由闪烁转为关闭，代表此区域生产中断；最终所有限位开关失效、计数器停止。各区域背景灯光依次闪烁后关闭，全工艺段流水灯变成红色。全网设备宕机。

第三种是模拟黑客网络嗅探篡改操作指令造成 PLC 错误动作：

新能源光伏场站仿真平台中所选择 PLC 设备与上位机通讯协议存在安全漏洞，入侵者能够通过网络嗅探分析上位机下发指令内容，并进行篡改，篡改后控制指令导致 PLC 出现误动作。

模拟场景中，黑客接入现场控制网络嗅探 PLC 设备与上位机通讯。上位机通过组态界面内参数调节，调整光伏组件矩阵机械转动装置、箱变和逆变器、流水灯运行动作。黑客通过对通讯协议内指令内容篡改，发送至 PLC 后，改变光伏组件矩阵机械转动装置、箱变和逆变器、流水灯运行状态。

整个沙盘各区域背景灯闪烁，表示各区域遭受入侵。光伏组件矩阵机械转动装置旋转紊乱，箱变和逆变器改变正常运行状态，升压站宕机，整个发电工艺逻辑混乱，现场设备运行状态错误。

（2）工控安全攻防及监测系统建设

● 系统定位

工控安全攻防及监测系统是工控安全实验室的必要组成部分，也

是其核心系统。基于工控安全攻防及监测系统，能够实现完整的攻击、防御、监测演练活动。

● **技术架构**

工控安全攻防及监测系统的核心内容包括攻击系统和防御系统、监测系统，其中攻击系统包括各类攻击组件，防御系统包括软件、硬件结合的安全防护体系，监测系统以工控审计平台、流式处理平台等设备系统组成，用于监测当前工控仿真系统的安全情况。

● **组成结构**

此系统主要分为三个模块：攻击套件系统、安全防护系统、安全监测系统。

其中攻击套件系统采用硬件形式，通过以太网接入工控仿真系统上下位机之间的交换机，通过计算机进行访问操作，实现各类针对工控仿真系统的攻击行为。

其中安全防护系统、安全监测系统均是由各类工控系统常用安全设备及系统组成。

● **功能性能**

1) **攻击套件系统：**提供各类针对工控仿真平台的攻击行为，包括中间人攻击、泛洪攻击、DoS 攻击、ARP 攻击等等，同时支持根据客户诉求进行攻击方式的定制化，支持在各类攻击方式基础上进行攻击参数自定义的定制工作。

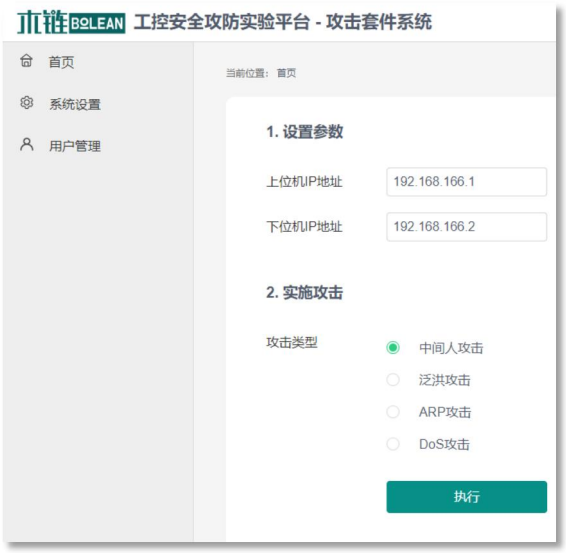

图 7-15　新能源工控安全实验室攻击套件示意图（参考）

基于对各类控制器的漏洞挖掘和长久的工控安全技术累积，此方案可以提供一些常见的攻击手段，这里列举部分攻击方式：

攻击方式一：通过攻击将控制器（PLC）宕机

攻击者非法接入监控层网络，通过内网嗅探，分析了 PLC 的 IP 地址以及传输数据信息后利用 PLC 通讯认证缺陷成功与 PLC 建立了连接。

攻击者向 PLC 发送非法控制指令进，从而远程控制 PLC 的 IO 模块。

攻击者远程控制 IO 模块，可将 PLC 复位，使 PLC 处于瘫痪状态。

攻击方式二：对 PLC 的 IO 点直接篡改

攻击者非法接入信息层网络，通过信息网进一步入侵监控层网络。

分析了 PLC 的 IP 地址以及传输数据信息后利用 PLC 通讯认证缺陷成功与 PLC 建立连接。

攻击者向 PLC 发送非法的控制指令，从而远程控制中控的 IO 模块。

攻击者远程控制 IO 模块，进而恶意改变 PLC 的参数，如使机械转动装置一场，升压站无法正常进行工作，导致全面停产。

攻击方式三：中间人攻击：篡改 WINCC 参数值，PLC 及现场无变化；

正常控制网络中操作员站的控制软件时刻检测 PLC 各信号状态，并将数据反馈显示。

攻击者可通过一定手段成为控制软件与 PLC 设备通信的中间人，两者的通信数据将完全流过中间人设备。中间人设备可以通过监视、转发等手段获取网络通信中的敏感数据，修改部分敏感数据以达到攻击目的。

如中间人设备截获 PLC 回报的温度传感器报文，并修改为自定义数值，欺骗操作员站控制软件，但 PLC 和现场没有任何变化。

攻击方式四：U 盘攻击——通过 U 盘作为载体，对 PLC 进行攻击

攻击者将U盘插入上位机的USB接口，自动传播病毒感染上位机。

攻击者侵入控制网络，更改 PLC 中的程序和数据

攻击者通过专用后门程序，可成功的窃取或篡改系统应用站中的数据，从而影响工控系统。

2) **安全防护系统：**包含工业防火墙、主机卫士等各类常见工控安全设备，提供针对攻击行为的防御功能，发现并阻拦攻击行为。

3) **安全监测系统：**包含工控审计平台、威胁感知平台、流式大数据分析组件等，对工控仿真平台的安全性进行实时监测与告警。

安全设备，包括主流的工控系统安全防护设备，此处仅列出四款主流产品。一是工控防火墙，工控系统因其设计的私有性，一直以来被认为是相对安全的，但 2014 年以来针对工控系统网络的 APT 攻击增加，工控系统内部网络安全问题的严重性也逐渐增加。工控防火墙

是专门针对工控环境的专用防火墙设备。通过多种安全策略，结合安全漏洞库，对 APT 攻击、异常控制行为和非法数据包进行告警和阻断，并对各类安全威胁实施监控，快速直观地了解工业控制网络安全状况，实现全网安全防护。

二是主机卫士，主机卫士是针对工控上位机和各类服务器在工控环境中的安全难题，并结合我国工业控制系统现状，自主研发的主机防护产品。主机卫士建立在白名单机制、环境固化机制之上。针对工控环境杀毒软件无法实时更新，工控软件易被误杀的难题，以全新思路来解决问题。将多个主机卫士分布部署到工控上位机与服务器中，通过综合管理平台统一管理主机卫士，有效提高管理效率、节约管理成本。

三是工控安全监测系统（工控审计），工业控制系统的生命周期通常都很长。目前国内大量运行中的工控设备在当初设计时没有充分考虑到网络安全问题，或者拥有的安全机制无法应对现在不断涌现的各类安全威胁挑战。监控审计终端通过对控制网数据的采集、解析、鉴别，实时动态监测通信内容，发现并捕获异常指令和数据，实时告警响应，全面记录控制网中各种会话和事件，实现对控制网信息的风险审计和对安全事件的准确回溯定位，为工控网络安全策略的制定提供可靠的支撑，同时保障生产安全、系统可靠性和可扩展性。

四是工业网闸，工业网闸可以部署在安全 II 区与安全 III 区之间，作为电力监控系统网络边界的第一道防线，用来阻止来自管理信息大区的病毒、木马、网络入侵等安全威胁。保证生产数据安全交换，通过对工业数据的访问进行控制，有效防范恶意攻击和敏感信息泄漏，保障生产网与办公网隔离的同时，实现安全、高速、可靠的数据交换。

运行流程即攻防及监测系统的核心运行流程为攻击、防御、监测

之间的对抗流程。其中：

攻击准备阶段：攻击者准备好攻击套件设备，或其他自主攻击内容，准备攻击；

攻击实施阶段：针对工控仿真平台实施攻击；

攻击防御及告警阶段：各类工控安全防御产品进行对攻击的防御阻断，安全监测产品进行告警；

回顾提升阶段：经历一轮完整的攻防演练流程，发现安全系统建设、安全管理机制、应急处理制度中的不足，进行改进，加强安全防范。或者寻找更加隐秘的攻击手段，从而对下一轮攻防演练中的安全防御体系提出更高的要求。

内外接口：工控安全攻防及监测系统的内外接口较为简单，其硬件设备（包括攻击套件、安全防御及监测设备）均可通过网线/光纤接入工控仿真平台上位机和下位机之间的交换机上，接口通常为千兆/万兆的以太网光口/电口。其软件系统则通常装在主机（上位机）上，也有的安装在服务器上，对主流操作系统均有兼容性。

（3）工业网络靶场平台建设

工业网络靶场平台侧重于攻防实战学习环境的演练，类似兵棋推演，提供一个类似新能源场站面临各种网络威胁的真实环境，让研究人员和参训人员学习和观摩攻防演练过程，学习到正确的应对经验，在演练过程中，会有专家或系统指导说明从旁协助，于攻防演练完成后会深入检讨过程之应对技巧，讨论有哪些可以改善或做得更好的地方。譬如在面对勒索软件、高级持续性渗透威胁(APT)攻击或拒绝服务式(DDOS)攻击，都需要透过实际情境训练来提升相关人员之攻防能力，并研拟与实施不同情境下的防御措施，目标是培育相关安全人员具备充裕的防御作战能力。

工控网络攻防靶场提供真实的工控网络攻防靶场，基于工控仿真系统，可仿真工控安全问题，包括工控设备通信数据截获及防御、通信协议劫持及动态加密、GPS、GIS 欺骗及安全验证防御技术、工控设备弱账号密码入侵、工控设备仪器参数设置误修改，工控传感器数据劫持，及与之对应的防御技术等。

工控网络攻防靶场还可以仿真通讯网络病毒感染、嗅探器扫描入侵、通讯网络 ARP、IP 欺骗入侵、DDOS 攻击、SCADA、EMS 等数据库非法注入、通讯无线信号干扰、通讯网络路由器入侵、通讯节点破坏等，及与之对应的安全防御技术。

工控网络攻防靶场基于工控仿真系统，在此基础上搭建以下系统构成完整的靶场。

通讯仿真系统：由专业并行实时通讯仿真平台组成，与仿真系统并行实时交互；

工控网络攻防靶场演示系统：直观的展示整个仿真平台的运行情况；

控制仿真系统：可以进行数据采集和监控，以及指令下达等功能，包括 SCADA 和调度等功能；

工控网络攻防靶场监控系统：实时监控工控网络攻防靶场。

- **拓扑组网**

工控安全靶场的目标是提供训练环境，训练网络安全人员如何防御关键网络设施受到攻击，以及针对假定目标实施网络攻击。这个训练环境包含了网络空间关键信息基础设施和工业控制系统组件、网络环境、软硬件资源、网络安全攻防资源及协作训练流程。组件包括了网络设备、主机设备、操作系统、应用程序、安全设备、嵌入式处理器和控制系统等内容；网络环境包含基础架构、互联网、无线网、各

种计算机网络、电信网等内容，组件与网络环境结合仿真关键信息基础设施和工业控制系统的虚拟环境。

可视化拓扑组网技术实现采用木链科技科技研发的网络仿真器实现，为了最大限度的设计和优化用户交互体验，采用可视化组网拓扑引擎的 Web 交互方式实现组件、场景的拖拽组网及实验访问交互操作。为了更进一步的仿真真实网络环境，达到网络及网络安全教学研究测试的目的，靶场网络仿真器集成路由器交换机模拟器实现真实路由器和交换机 OS 仿真模拟运行的效果，达到路由器和交换机真实可配置，可编辑和可管理。即可满足学员学习路由交换及网络安全需求，也可满足关键信息基础设施和工业控制系统可快速复现网络环境专注安全学习、研究的目的，达到灵活多变的网络环境支持，是工控安全靶场的特色功能。

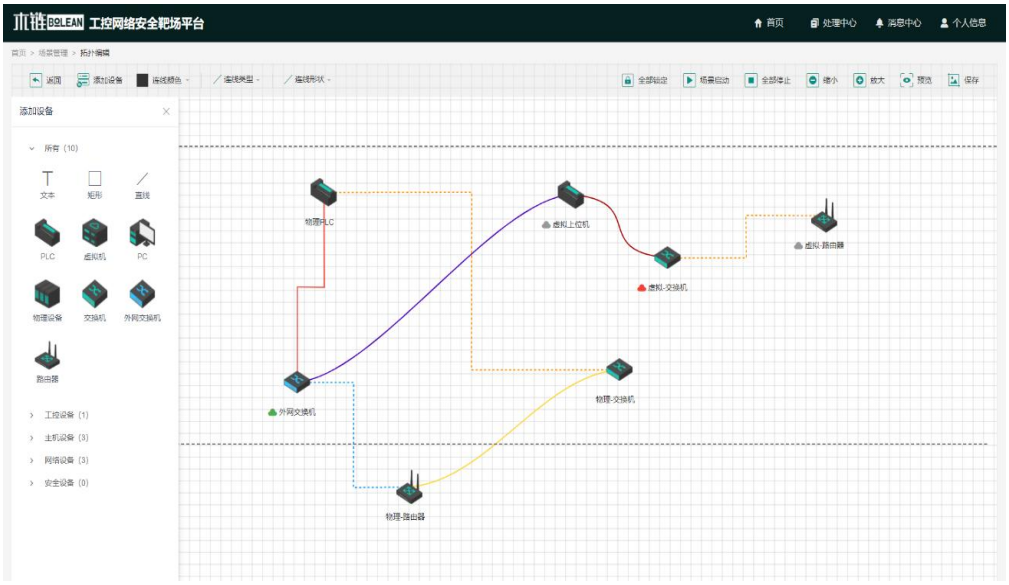

图 7-16　新能源工控安全实验室网络拓扑编辑图（参考）

➢　场景管理

在场景管理中，场景管理模块通过拓扑模板管理、模板配置管控实现对资源的场景拓扑及模板的版本控制、场景列表、场景信息、场景复制等功能的进行操。基于光伏电站发电的工艺流程和网络架构，

可定制场景从多个点发起网络攻击，并开展相关攻防演练。

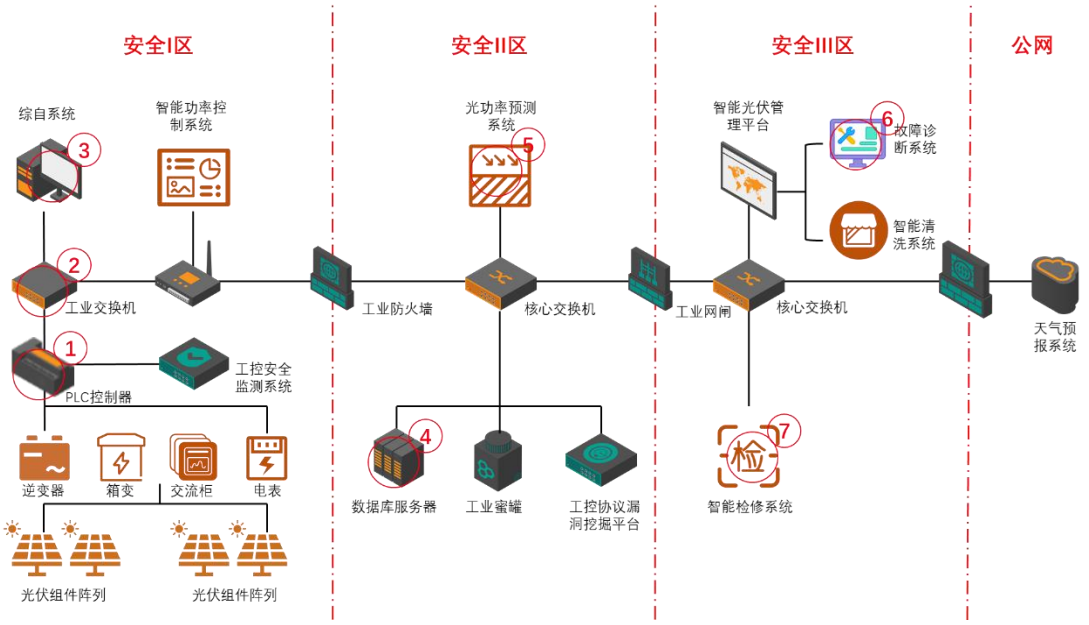

图 7-17　新能源工控安全实验室场景编辑图（参考）

攻防演练剧本的设计围绕工控安全事件中易受攻击的对象，如综自系统、工业交换机、控制器、数据库服务器、光功率预测系统等。

（3）安全实训系统建设

➢　系统概述

安全实训系统是用户直观获取安全知识的功能模块，系统内置理论资料、教学视频、操作文档、实验环境丰富的培训资源，借助这些资源，企业可以开展多样化的实操培训，实现通过实践来验证理论的教育效果。同时还可以通过靶标管理+网络拓扑绘制构建多种多样的实训场景，利用自动化裁决系统来记录和判断学员每一步实操的一个正确性。

系统包括基础培训模块、实验操作模块、技能考核模块、测评练习模块、拓扑编辑模块及课程编排模块 6 部分。

基础培训模块：提供了多方向多类型的海量安全理论知识课程、从入门到高级安全知识，一站式学习。

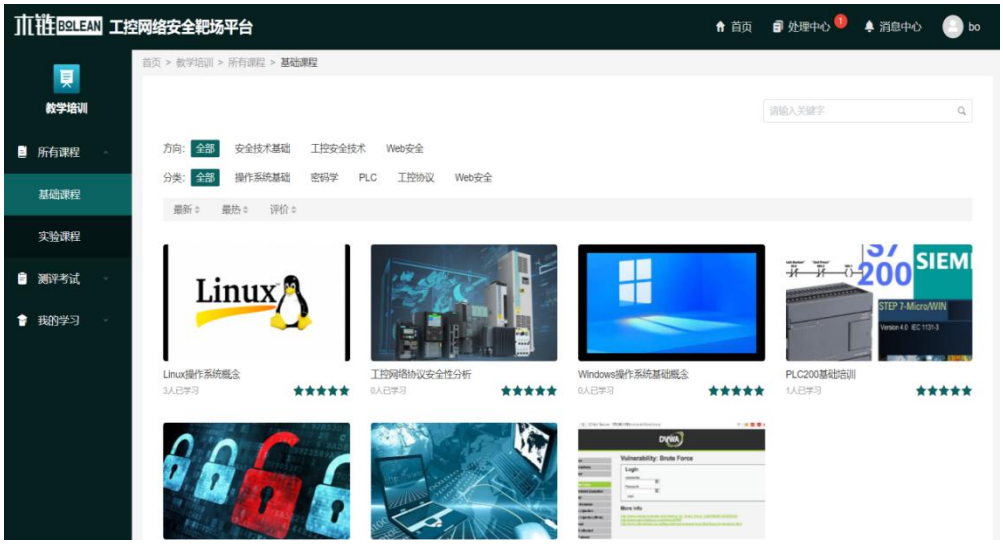

图 7-18　新能源工控安全实验室实训系统示意图 1（参考）

系统内置了超过 500 课时的理论课程和实验课程，包含了像操作系统基础、工控安全技术、工控协议、密码学、web 渗透等主流基础知识及攻防技术的课程。

实验操作模块：通过构建虚拟、虚实结合网络环境，集成操作文档、视频、附件等多样化培训资源，开展形态多样的实操培训；

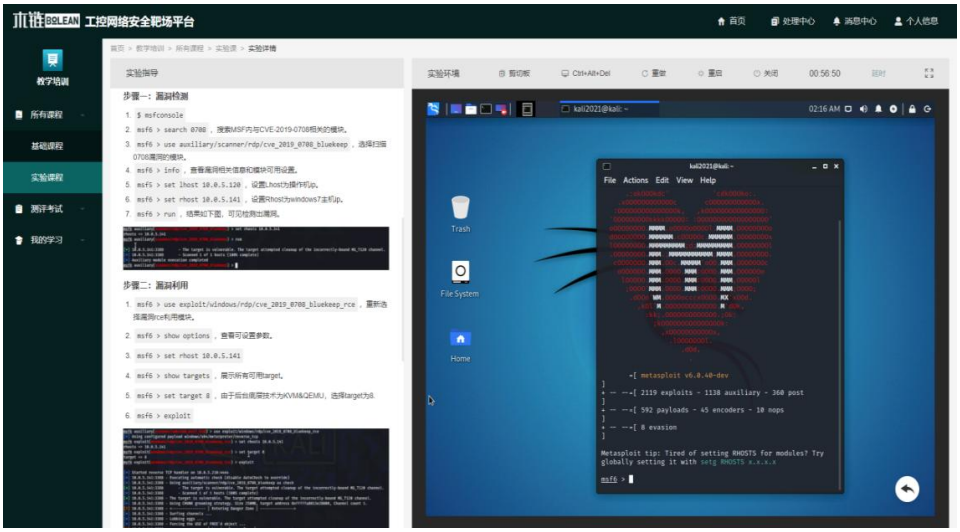

图 7-19　新能源工控安全实验室实训系统示意图 2（参考）

技能考核模块：提供考核评估的功能，允许用户在考试试卷中添加各类实操题目，全面考核人员的理论与实战能力。

测评练习模块：提供已学知识的练习环境，巩固知识点，随学随练。

拓扑编辑模块：提供全可视化的拓扑编辑器，方便课程开发人员快速构建实操环境。

课程编排模块：靶场提供开放的环境，可以针对性的设计自定义课程；客户可以将企业内部的工艺、安全等知识形成教学课件应用于靶场。

- **配套的工控安全课程**

工控安全理论课程：学习工业控制系统安全基础概念并理解其安全态势。该项建设所支持的工控安全理论课程内容：

理论课程	**第一部分工控安全基本原理**	**第 01 课时-工业控制系统简介**
		第 02 课时-工业控制系统架构和网络
		第 03 课时-可编程逻辑控制器（PLC）
		第 04 课时-数据采集与监控系统（SCADA）
		第 05 课时-工控其他软硬件介绍
		第 06 课时-历史/实时数据库
		第 07 课时-集成软件（ERP/MES）
		第 08 课时-工业控制系统发展历史及现状
		第 09 课时-工业控制系统应用领域
		第 10 课时-常见工业控制系统的对比
		第 11 课时-工业控制系统现场设备 IED、HMI 介绍
		第 12 课时-PLC 的产生与特点、组成与工作原理
		第 13 课时-电力监控系统网络介绍
		第 14 课时-工控行业应用及业务介绍
		第 15 课时-工控安全隔离类产品（工业防火墙、网闸）
	第二部分工控安全态势	第 16 课时-工业控制系统安全概述
		第 17 课时-传统信息安全与工控安全比较分析
		第 18 课时-工业控制系统网络安全事件
		第 19 课时-国外工控安全保障体系建设
		第 20 课时-中国工控安全态势
		第 21 课时-互联网工控安全态势
	第三部分工控隐患知识	第 22 课时-工控网络资产识别
		第 23 课时-工控安全隐患来源
		第 24 课时-工控安全隐患分析
		第 25 课时-工业控制系统威胁监测
		第 26 课时-工业控制系统现场检查安全分析
		第 27 课时-工控安全风险评估
		第 28 课时-工控安全等级保护
	第四部分工业	第 29 课时-工业控制网络常用通信协议概述

	协议基础	第 30 课时-S7 协议介绍及机制
		第 31 课时-Modbus 总线协议概述及协议安全缺陷
		第 32 课时-DNP3 协议安全缺陷
		第 33 课时-IEC60870-5-104 协议安全缺陷
		第 34 课时-OPC 协议安全缺陷
	第五部分工控安全政策和标准	第 35 课时-网络安全法
		第 36 课时-国内外工控安全政策与标准简介
		第 37 课时-工控安全防护指南
		第 38 课时-常见工控安全标准
		第 39 课时-常见工控安全架构
		第 40 课时-国内常见的工控安全解决方案

4. 安全及可靠性

木链科技创建初期既得浙大 AAA 战队主力成员加盟，尔后迅速聚集安全领域行业专家，国内外高等院校自动化、软件工程学术菁英等优质安全研究员，组建起星期五安全研究实验室。实验室团队多次承担国家级科研课题任务并将其研究成果梳理成能力模块，为驱动产品演进和技术更迭注入创新因子。实验室团队凭借业内领先的漏洞挖掘能力，对公司产品进行了大量的检测工作以确保产品的安全可靠。此次方案全套产品均采用全自主研发系统与配套软硬件，确保符合国家要求与企业安全发展的需要。并经过长达 3 年以上的实际方案运行考验，产品可靠性与稳定性已非常成熟。

为响应国家号召，积极支持国产化进程推进，确保工控安全防护相关产品都是完全国产化产品，拥有完整的自主研发支持产权。通过长期快色的版本更新迭代，保护用户的工控数据核心资产安全与完整、私密等特性。

5. 其他亮点

（1）打造完善工控安全课程体系

工控网络安全是一个综合、交叉的学科领域，涉及数学、物理、通信、计算机、自动化、管理等诸多学科领域的知识和最新发展成果，

同时该专业也是一个实践性很强的专业。因此，应以电力行业需求为导向建立科学的课程体系，课程体系中应理论基础与工程实践并重，注重参训学员的综合素质和自学能力的培养，加强自动化、计算机网络和实践课程的训练；确立核心课程，并在保证工控安全专业教育的基础性、全面性的同时，并按照其内容联系、应用需求、岗位需求、竞赛需求等划分成若干个课程模块，建立“理论教学+安全实操”的多模式相结合的创新的教学模式，促进学员安全能力的全面掌握。

（2）加强红蓝方实战对抗水平

“红队攻点、蓝队防面、以攻促防、全面消缺”，全面提升新能源场站网络安全人才梯队的工控网络安全“战时”水平，培养复合型人才，提升专业技能，并可有效提高该地区新能源场站网络安全“战时”应急响应能力。

（3）构建工控安全实训基地

建成的新能源工控网络安全实验室既可以为某电科院相关研究人员提供实战对抗的环境，也有能力为行业内相关从业人员提供培训环境。通过这种理论与实践结合的特色教学模式，以及工控网络安全实验室涵盖的工控网络安全各领域的丰富实验内容，实现参训学院安全意识和实操能力的快速提升，最终实现培养新能源领域工控网络安全专业人才的目标，并成为具有地区特色的电力工控网络安全实训基地。

1.1.3 下一步实施计划

1. 计划 1

系统名称	方案工期	设备型号规格/环改费支出用途
新能源光伏场站仿真平台	一期方案本期建设	新能源场站电力监控系统：使用 PLC 和必要网络设备进行控制系统进行组网，并采购相关的组态软件，进行控制逻辑的搭建和控制画面的开发。 选择现场控制设备为新能源场站主流控制设备品牌型号，共包含 PLC 设备，控制设备均配置以太网模块，用于同操作员站、工程师站实现网络连接；控制设备配置 DI/DO，同现场沙盘连接，实现沙盘内机械转动装置、声音报警器、灯带、开关和计数器等的控制以及数据采集。
	一期方案本期建设	复现光伏发电典型工控场景，采用工控安全沙盘的方式进行工控环境搭建，含光伏组件、综合自动化系统、操作员站、工程师站、智能功率控制系统、箱变、逆变器、升压模块等关键组件来还原新能源光伏电厂生产流程。沙盘采用物理仿真沙盘+数字虚拟沙盘的“孪生双胞胎”模式进行生产运行状态的展示。
	一期方案本期建设	
	一期方案本期建设	用于驱动整套仿真装置运行，并实现仿真装置数据的传输与收集。
工控安全防护及监测系统	一期方案本期建设	提供各类针对新能源场站仿真平台的攻击行为，包括中间人攻击、泛洪攻击、DoS 攻击、ARP 攻击等等，支持攻击方式的定制化，支持在各类攻击方式基础上进行攻击参数自定义。
	一期方案本期建设	安全防护系统是攻防演练过程的必要组成部分，也是工控安全实验室建设中的核心系统。安全防护系统包括工控网络中必需的各类软硬件工控安全设备，依据设备防护类型，又可以划分为安全防御系统和安全监测系统，其中安全防御系统是指能够主动防御攻击行为、异常行为的设备集合，如工控安全防火墙、主机卫士、网闸设备等，安全监测系统以安全审计、监测、管理为主，如工控审计平台、综合管理平台，用于监测当前工控仿真系统的安全情况。 安全防护系统包括了业界常见的工控安全设备，如工控安全防火墙、工控审计平台、主机卫士、综合管理平台、单向隔离网闸设备等，也可融合传统的信息安全设备如防火墙、入侵防御/检测系统、防毒墙、WAF、身份认证设备等。

系统名称	方案工期	设备型号规格/环改费支出用途
工业网络靶场平台	一期方案本期建设	靶场知识图谱主要由多个资源管理模块组成，这些资源主要以数据库和主机服务资源形式存在，用户可以在靶场平台的环境内进行调用。其中场景资源为用户提供包含虚拟主机设备、虚拟网络设备、虚拟工控设备和虚拟安全设备等资源，可实现虚实结合的网络仿真场景。攻防资源管理系统为用户在现有的基础测试环境上提供了攻击、防御、测试等多种资源，用户可以根据需求进行整合和利用。
	一期方案本期建设	靶场平台提供核心的网络拓扑搭建功能，提供全可视化的拓扑编辑工具，可以在同一网络中添加虚拟、物理靶标组成混合网络，并直接在编辑器为其设置 IP、DNS、网关等各种参数。提供攻防演练活动管理功能，快速将网络拓扑、安全事件、以及攻防任务进行组合，构建应用场景，组织演练任务，靶场内置了多种安全事件剧本，能够为用户提供学习和演练安全技能必要的环境和工具资源。 高级演练系统中包含对靶场内业务数据的监控，可对演练活动的全过程进行过程安全监控，并能实时捕获安全事件动态，管理员可以根据需要实时的调整演练任务，使整个演练活动更接近实战。
	一期方案本期建设	靶场提供可视化系统，可以将靶场各项运行指标，以及网络攻防演练活动中的数据实时监控和采集，并能够通过数字化看板的形式进行展示，可用于宏观地把控靶场运行及活动进展情况等。
安全实训系统	一期方案本期建设	支持在线和线下实训，支持随堂考试，在线实操等功能，学情管理等功能。 课程资源包：包含理论课程、实验课程，体系化课程、电力安全课程。
操作台、装修及其他费用	一期方案本期建设	满足用户装修风格的操作台 1 套，并完成计实验室装修设计和实施。 其他费用包括材料费用、运费等。

2. 计划 2

系统名称	方案工期	设备型号规格/环改费支出用途

安全竞赛系统	二期方案 高级应用	安全竞赛模块支持知识赛、解题赛、攻防赛等多种形态竞赛模式，内置大量工控安全挑战库，可以向客户定制有针对性的工控主题类型的竞赛，系统提供赛前配置、赛中监控、赛后复盘等管理功能。 标准模块：答题系统、竞赛监控系统、竞赛管理系统、裁判系统。 赛题资源包：包括传统 CTF 赛题和工控安全赛题资源包
测试验证系统	二期方案 高级应用	产品测评系统主要为用户提供针对不同工控产品及工控安全产品的测试环境以及测试工具，以及为用户提供常见的产品测试流程方法支撑资源环境。 结合木链科技的漏洞挖掘系统，针对工控网络自身脆弱性和通信协议的安全性，主要围绕工控网络中可能存在的各类工控系统、设备、协议等方面的已知和未知安全漏洞，开展有效的分析和研究，对如何防御这些安全威胁提供指导作用。

1.1.4 方案创新点和实施效果

1. 方案先进性及创新点

（1）建设能源工控网络安全人才孵化基地，探索产学合作模式

通过网络安全实验室的搭建，推行产学融合的人才培养模式，推动专业设置、课程内容、教学方式与生产实践对接，建设具有特色的优质能源行业工控安全人才培养孵化基地，在区域内树立标杆形象。

（2）打造完善工控安全课程体系，实践“理论+实践”的教学理念

工控网络安全是一个综合、交叉的学科领域，涉及数学、物理、通信、计算机、自动化、管理等诸多学科领域的知识和最新发展成果，同时该专业也是一个实践性很强的专业。因此，应以电力行业需求为导向建立科学的课程体系，课程体系中应理论基础与工程实践并重，注重参训学员的综合素质和自学能力的培养，加强自动化、计算机网络和实践课程的训练；确立核心课程，并在保证工控安全专业教育的基础性、全面性的同时，并按照其内容联系、应用需求、岗位需求、竞赛需求等划分成若干个课程模块，建立“理论教学+安全实操”的

多模式相结合的创新的教学模式，促进学员安全能力的全面掌握。

（3）加强关基安全应急响应能力，提升红蓝方实战对抗水平

“红队攻点、蓝队防面、以攻促防、全面消缺”，全面提升地区新能源场站网络安全人才梯队的工控网络安全“战时”水平，培养复合型人才，提升专业技能，并可有效提高该地区关基设施安全“战时”应急响应能力。

2. 实施效果

（1）方案效果

- 已经完成面向核电、火电、新能源和钢铁等多个行业的实验室建设项

目和交付，系统运行平稳，各项参数良好，获得用户的好评和欢迎。

- 已经积累了数字孪生技术和虚拟融合仿真技术，实现电力行业生产业务仿真（包括生产工艺仿真、控制系统仿真和通讯协议仿真），帮助用户 1：1 还原了生产环境，并实现了生产数据的流动，为安全分析和攻防对抗提供了高可用性的研究载体。

- 完成多个行业数十种生产场景的还原，为用户定制了自动化攻击流量和安全防护系统，并集成了“震网”等 50 余中典型攻防剧本，聚焦战时关基设施安全防护和应急响应，通过基于“挂图作战”理念的攻防对抗，有效提升能源行业安全从业者的实战水平。

- 搭载了漏洞挖掘和设备固件测试高级研究工具，为客户提供最优的工控安全设备检测及安全分析工具，助力用户形成契合企业实际需求的安全标准及规范。

（2）行业效益

- 提高行业内单位全员安全意识

通过建设电力行业工控信息安全仿真系统，能够向组织内部全员普及工控安全防范概念，通过参观讲解、基于工控安全仿真系统做一些知名工控安全事件的还原分析，以及进行工控安全基础概念、政策法规、攻防演示培训，增强单位各部门、各级别人员的安全意识。

- 规划行业内单位生产安全发展趋势

通过紧跟国内网工控安全防护理念的最新发展趋势，结合工控安全仿真系统内部攻防研究和行业内生产现场调研，做出对于行业内工控安全发展趋势的预测，从而提出具备可行性、先进性、可靠性的研究方向，支撑行业内工控安全研究团队的科研方案，提升行业内工控安全研发技术实力。

- 加强行业内单位生产安全管理能力

通过模拟工控安全事件发生全流程，让电力关基运营管理人员对安全事件的准备阶段、发生阶段、处置阶段有直观的认识，从而能够梳理当前组织内部在安全管理方面的不足，提升组织在安全事件防范、治理等方面的管理能力。

- 提升行业内单位应急响应能力

安全事件的发生往往无法预知，因此除了安全防御体系的建设，安全事件应急响应处理也是整个安全防范工作的重中之重。通过工控攻防实验室能够模拟各类主流安全事件，结合真实直观的“实战演练”场景，提升组织对于安全事件的应急响应能力。

- 降低行业内单位工控安全风险

通过建设工控安全仿真系统，能够做到：增强全员安全意识、增强安全管理水平、培养工控安全人才、提升安全事件的应急响应能力，

同时能够结合蜜罐系统、靶场系统等系统，在通用安全设备+安全软件的基础上，有效降低工控系统的安全风险，提升安全防范实力。

（3）经济效益

- 面向行业的工控安全人才培养

鉴于当电力行业对工控系统信息安全人才的需求，利用攻防实验室能将理论与实践结合，在实现工控安全概念、政策法规培训的基础上，通过攻防演示、协议解析等偏技术类课程，培养工控安全相关的攻防人才，从而提升组织内部的工控安全防范技术实力。

- 面向行业的工控安全标准体系研究

基于对电力能源等相关在工控安全领域已经建立较为完善标准体系的行业的标准调研，结合工控安全实验室内攻防经验、行业内单位工业现场现状和工控安全防护体系部署现状，研究面向煤化工行业的工控安全标准体系，在理论与实践结合的过程中将标准体系逐步推广至实验室仿真环境、试点环境、工业现场非核心区域、工业现场，在不断论证中打磨电力行业工控安全标准体系。

- 推广行业内先进安全防护解决方案

从安全部署、安全测评、安全服务等多个角度评估行业内工控安全解决方案和产品向行业进行集成推广的可行性与应用价值，为行业典型系统和装备的集成推广奠定坚实基础，并进一步将先进工控安全解决方案、技术和产品推广向行业内有需求的典型单位，提升行业内单位的工控安全综合建设水平。

- 面向行业的工控安全测评体系

随着终端用户对工控网络安全的逐渐重视，工控网络的安全防护产品和各种安全解决方案在市场端逐渐增多，众多的工控安全产品和解决方案对工控网络防护的效果良莠不齐，产品测试系统可以帮助用

户和解决方案应用单位了解产品的具体功能性和详细指标，也可以通过使用测试与验证工具对安全设备和工控设备的功能与性能进行完整性和达标性测试。

目前电力行业工控系统中所采用的核心设备，国产设备有一定占比，在“数字换转型”和“双碳”背景下，新型电力系统及海量终端广泛并网，未来电力监控系统将迎来更多新型智能终端、5G 设备、工控设备和工控安全设备接入，会带来各类安全风险。通过建立完善的安全测评与准入制度体系，加强工控安全测试、评估、验证，让新技术、新产品、新系统能够在完善的监管测评之下进入现有工控系统当中来，将极大地增强行业发展安全稳定性，同时有利于逐步提高单位在工控安全测评方面的技术实力，推进工控系统、工控安全系统自主化的进程。

1.1.5 单位基本信息

浙江木链物联网科技有限公司是专注于工业互联网安全技术研究、安全产品开发的国家高新技术企业，为客户提供产品定制、安全咨询、威胁评估、等保建设、人员培训、系统运维等全流程服务，已打造军工、烟草、电力能源、轨道交通、智能制造等多个行业整体解决方案。

木链科技依托国内领先的大数据处理引擎和协议解析能力，形成了自主可控的技术体系。通过覆盖工业企业全产业链、全生命周期、全业务流程的产品和服务，以工控安全为切入点，实现了从工业生产网络到工业互联网的全方位防护，并已承担多个国家关键信息基础设施安全方案。

木链科技坚持技术驱动，与国家工业信息安全发展研究中心、中国信息安全测评中心、中国工程物理研究院、工业控制系统信息安全

技术国家工程实验室、浙江大学、上海交通大学等众多高校科研院所达成合作。

在国家大力发展“新基建”、“工业互联网”的背景下，木链科技以推进工业领域信息化建设与应用为根本导向，致力于构建安全的工业互联网，打造安全价值生态，赋能我国工业信息化建设。