长春工程学院吉林省水利电力工程安全仿真验证靶场平台建设内容、功能与需求

一、项目建设内容

吉林省水利电力工程安全仿真验证靶场平台建设立足国家关键信息基础设施在水力电力方面的教学和科研实践需求，主要涵盖工业控制系统安全和计算机系统安全建设方向，在专业课程、新型软硬件实验设施等方面进行重点建设，支持安全仿真验证靶场平台同时进行实验授课，定制一套水力发电厂水力发电物理仿真装置、一套水力发电厂升压站物理仿真装置和一套水力发电厂水工构筑物物理仿真装置，并建设一套驱动水力发电厂仿真装置的PLC控制系统和保护装置、工业环网交换机，以及工业安全网关、工业安全监测、工业主机安全防护、工业协议漏洞挖掘装备为主体的安全产品体系。结合仿真装置实施水力发电厂组网和攻防流程演示，全面兼顾实验教学、科研创新、攻防演练等多样化需求，力争建成水利电力工控安全领域软硬件资源齐全、功能完善、课程体系完备、技术拔尖的安全仿真验证靶场平台，助力安全研究模式发展，培养出多学科知识交叉融合、攻防实践能力突出、具备持续竞争力的知识技能复合型专业人才。

二、项目功能及需求

（一）水力发电厂水力发电物理仿真装置：

1.水力发电厂水力发电物理仿真装置主要模拟仿真水力发电厂的水轮机和发电机，仿真水力发电厂水轮机将水的势能转换为机械旋转的机械能，并将机械旋转的机械能转换为电能。

2.水力发电厂水力发电物理仿真装置按照水力发电厂水力发电典型工艺场景定制，水力发电物理仿真装置为水力发电厂水力发电典型微缩示意模型，向参展人员展示水力发电厂水力发电正常生产控制流程及攻击、防护效果。

3.水轮机含4个叶片，含润滑组件；

4.发电机发电能力不小于100瓦，三相三线制，电压不高于36VAC；

5.水力发电物理仿真装置进行水力发电厂水力发电的业务流程进行实验教学、科研创新、攻防演练等工作；

6.水力发电厂水力发电物理仿真装置将结合升压站物理仿真装置、水工构筑物物理仿真装置及工业网络组网设备能力组建水力发电厂工控网络仿真环境，接入安全防护设备并对该控制系统进行安全能力保护，通过攻防能力验证和演示，测试安全防护能力和效果，并验证安全防护解决方案的可行性和必要性。

（二）水力发电厂升压站物理仿真装置：

1.水力发电厂升压站用于仿真水力发电厂发电机产生的三相低压交流电转换为同频三相高交流电，并实现多发电机所发电能并联实现长距离跨区域传输微缩示意模型，向参展人员展示水力发电厂升压站正常生产控制流程及攻击、防护效果。

2.升压站物理仿真装置按照典型水力发电厂升压站工艺场景定制，规格不小于2\*3米，可仿真220kV升压站，可动作开关不小于3个，具备电量计量功能。

3.系统采用工业级流水线设计，符合实际工业生产的节拍与精度要求；

4.升压站物理仿真装置基于水力发电厂升压站进行仿真水力发电厂升压站的业务流程进行实验教学、科研创新、攻防演练等工作；

5.水力发电厂升压站物理仿真装置将结合水力发电物理仿真装置、水工构筑物物理仿真装置及工业网络组网设备能力组建水力发电厂工控网络仿真环境，接入安全防护设备并对该控制系统进行安全能力保护，通过攻防能力验证和演示，测试安全防护能力和效果，并验证安全防护解决方案的可行性和必要性。

（三）水力发电厂水工构筑物物理仿真装置：

1.水力发电厂水工构筑物物理仿真装置用于仿真水力发电厂除水轮机、发电机及升压站以外的水力发电厂建筑物、构筑物，比如水力发电厂的挡水建筑物(坝)、泄洪建筑物(溢洪道或闸)、引水建筑物(引水渠或隧洞，包括调压井)等设施；

2.水工构筑物物理仿真装置按照典型水力发电厂水工构筑物工艺场景定制，规格不小于3\*4米，闸门不小于9个，可控制闸门2个；

3.装置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；

4.整个水工构筑物物理仿真装置建设动态，直观，它能反映水工建筑物的一些细部结构特点，对一些结构复杂，层次较高的结构用不同的颜色的建筑材料表示；

5.水工构筑物物理仿真装置基于水力发电厂挡水、泄洪、引水等的业务流程进行实验教学、科研创新、攻防演练等工作；

6.结合水力发电物理仿真装置、升压站物理仿真装置及工业网络组网设备能力组建水力发电厂工控网络仿真环境，接入安全防护设备并对该控制系统进行安全能力保护，通过攻防能力验证和演示，测试安全防护能力和效果，并验证安全防护解决方案的可行性和必要性。

（四）驱动水力发电厂仿真装置的PLC控制系统：

1.PLC设备主要用于水力发电厂闸门LCU工业控制，实现输入与输出之间的控制逻辑；实现远程通讯功能；

2.PLC设备规格采用：控制器、电源模块、数字量输入、输出模块，模拟量输入、输出模块；PLC控制至少具有48个点I/O；支持基于TCP/IP的工控协议；PLC标准配置编程软件；与所选型号PLC对应；能够进行PLC硬件组态：含PLC控制逻辑编程软件，能够进行PLC逻辑编程：能够进行PLC网络组态；能够进行PLC在线诊断；能够更新PLC固件版；

3.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，实现対各单元的自动控制；

4.闸门控制单元LCU，轮机控制发点单元LCU，以及电力输送等部分有动态效果，动态部件通过PLC控制。

（五）驱动水力发电厂仿真装置的保护装置：

1.保护装置用于水力发电厂1#LCU发电控制和开关站LCU控制，实现水力发电厂1#LCU发电机和水电厂开关站继电保护,用于对水轮机和发电机实现温度保护；

2.测控保护一体化继电保护装置；支持串行和TCP/IP的工控协议；温度保护水轮机和发电机，测温点不少于32个，含32个RTD传感器；支持串行和网络通讯；

3.高标准电磁兼容性，密闭机箱设计，满足装置下放安装的苛刻要求，也可集中组屏；

4.提供中文界面，操作简便，可提供六个快捷功能键，实现打印及定值区切换的快速操作，十一个指示灯实时指明装置运行状态；

5.具备完善的软硬件自检功能和免调节电路设计，安装调试简单。

（六）工业环网交换机：

1.工业环网交换机用于工控网络的接入及组网，为仿真装置组成工业环网，搭建水力发电厂级生产监控网络；

2.业务端口：固定端口，24个以上10/100/1000Base-TX以太网端口；4个千兆SFP光口，含4个千兆单模SFP模块；交换模式端口；

3.存储转发模式，支持IEEE802.3X流控，支持端口镜像；支持基于端口速率百分比的广播风暴抑制；支持基于pps的广播风暴抑制；

4.端口汇聚：支持LACP，支持手工聚合，支持128个聚合组，每组支持8个端口；

5.VLAN：支持基于端口的VLAN，支持基于协议的VLAN，支持基于MAC的VLAN；支持静态路由、RIPng；支持策略路由，ECMP。

（七）水力发电厂工业安全产品体系：

1.建立以工业安全网关、工业安全监测、工业主机安全防护、工业协议漏洞挖掘装备等为主体的工业安全产品体系，并结合集成到水力发电厂物理仿真装置中，通过接入水力发电厂物理仿真装置的水力发电、升压站和水工构筑物进行工业控制系统、网络安全、系统安全等的科学研究和攻防培训/竞赛/演练活动。

2.工业安全网关：用于水利水电控制工控网络访问控制，防护工控网络安全，实现工控网络边界安全防护。导轨式工业防火墙，4电口（2对Bypass），1管理口。产品3年维保服务。产品定制开发；

3.工业安全监测：用于水利水电控制工控网络及主机审计，审计工控网络及主机日志及威胁。技术规格：接口6\*电口（支持10/100/1000Mbps自适应）、2\*扩展槽（4电/4光/8电/8光/2万/4万）、MGT接口、带内管理、Console接口、RJ45串口、USB接口、2个CPU，Intel E3-1225 3.3GHZ 4核心，内存，16GB，存储，1T 企业级硬盘，4G CF，机箱尺寸（深\*宽\*高）2U(560mm\*440mm\*88mm)，电源规格，100V AC～240V AC，50Hz/60Hz，冗电，反应实效（告警延迟）10ms、最大并发连接数-200万、最大每秒新建连接数-10万/秒、3层吞吐量3Gbps。

4.工业主机安全防护：用于水利水电控制主机安全防护，防止针对工控主机的预埋程序和USB设备攻击。工业主机软件白名单防护、日志记录审计，支持微软32位/64位 Windows XP SP2及以上等，含50个安装授权，产品3年维保服务包（软件维护，硬件维保，远程支持，电话咨询）

5.工业协议漏洞挖掘装备：用于对水力发电相关设备、主机进行基于工业协议的漏洞挖掘，基于工业通讯协议实现漏洞挖掘。便携式，外置电源适配器,6×千兆电口+4\*RS-232/422/485,6×USB口。