黎阳电厂电力监控系统安全防护评估、网络安全监测能力提升及缺陷整改项目
技术规范书

批准：

审核：

编写：

鹤壁鹤淇发电有限责任公司

2023 年 7 月

黎阳电厂电力监控系统安全防护评估、
网络安全监测能力提升及缺陷整改项目技术规范

一、工作目标

1、根据省调 2022 年下发的《河南电力调度控制中心关于下发 2022 年统调电厂调度自动化及网络安全重点工作的通知》、《河南电力调度控制中心关于开展统调电厂电力监控系统网络安全监测能力提升工作的通知》、《河南电力调度控制中心关于上半年统调电厂电力监控系统网络安全运行情况的通报》、《统调电厂网络安全监测能力验证评估实施指导手册》要求，以及 2022 年黎阳电厂网络安全评估报告未整改情况，2022 年 9 月 OMS 下发缺陷等问题，结合省调 2023 年下发的《河南电力调度控制中心关于下发 2023 年统调电厂调度自动化及网络安全重点工作的通知》，并按照国家相关政策要求，巩固提升电力监控系统网络安全监测能力，组织开展电力监控系统网络安全监测能力能力提升工作及 2023 年度电力监控网络安全风险评估工作。黎阳电厂根据工作计划安排，对我厂 2023 年电力监控系统安全防护评估、电力监控系统网络安全监测能力提升及缺陷整改项目进行专项技术服务，完成 2023 年电力监控系统安全防护评估、电力监控系统网络安全监测能力提升及缺陷整改项目并通过河南电力调度控制中心审核验收，缺陷消除。

二、标准、规范、要求

- 《电力监控系统安全防护规定》（发改委 14 号令）
- 《电力监控系统安全防护总体方案》（国能安全〔2015〕36 号）
- 《河南电力调度控制中心关于下发 2023 年统调电厂调度自动化及网络安全重点工作的通知》
- 《河南电力调度控制中心关于上半年统调电厂电力监控系统网络安全运行情况的通报》
- 国能发安全〔2018〕72 号-国家能源局《关于加强电力行业网络安全工作的指导意见》
- 《河南电力调度中心关于进一步加强违规外联风险防控的通知》
- 河南电力调度控制中心 2022 年下发的《关于开展统调电厂电力监控系

统网络安全监测能力提升工作的通知》和 OMS 下发缺陷。

- 《统调电厂网络安全监测能力验证评估实施指导手册》

三、项目内容

1、网络安全监测能力提升项目内容

1.1 梳理现场涉网设备，监测装置接入资产需满足"应接尽接要求，涉及新增设备需按评估要求进行告警测试

(1)对电力监控系统涉网部分资产接入情况进行排查，确保厂站侧资产按照“应接尽接”要求接入电力监控系统网络安全管理平台，针对未接入资产尽快开展接入工作，新接入设备按照要求进行告警验证测试。排查完成后将涉网部分全量资产信息填写至《黎阳电厂网络安全验证评估厂站自查清单》，并形成厂站拓扑图，涉网部分全量资产需与拓扑图中一一对应。

(2)完成资产接入监测装置，包含但不局限于以下资产：调度专网数据网交换机、NCS 系统 A 网交换机、NCS 系统 B 网交换机、保信交换机、录波交换机、#1 发变组故障录波、#2 发变组故障录波、#1 启备变故障录波、线路故障录波、电能计量终端、网安防火墙、网安工作站、RTU 系统 B 网交换机。

(3)对新接入设备按照要求进行告警验证测试，通过省调验收。

1.2 主机探针配置不合理，涉及整改设备需按评估要求进行告警测试

核查主机探针配置情况，对不合规部分进行修改，确保探针白名单、关键目录、危险命令进行精细化配置，修改完成后进行告警验证测试。对未过检探针进行升级，不可使用未通过检查的探针厂家的探针产品，所有主机探针必须是过检探针产品。

1.3 监测装置配备省调主备双通道

黎阳电厂电力监控系统增加调度主站管理地址配置，实现厂站 II 型网络安全监测装置双平面接入省调主站，形成主备双通道。

1.4 监测装置版本平台校验

黎阳电厂 II 型网络安全监测装置版本较低，导致无法通过省调网络安全管理平台版本校验，依照统调电厂网络安全监测能力验证评估实施指导手册装置进行软件版本升级，完成版本校验要求。

1.5 网络安全监测装置配置合规

确保黎阳电厂网络安全监测装置全部资产规范化配置，检查厂站的Ⅱ型网络安全监测装置是否进行可靠接地、是否采用双路独立电源供电。确保黎阳电厂网络安全监测装置接入的主机设备、网络设备、安防设备均在线。检查设备类型、所属安全区、设备名称、IP 地址等信息录入是否正确，对录入信息不明确的资产,进行修正,并将排查信息填写至《黎阳电厂网络安全验证评估厂站自查清单》。

1.6 纵向加密装置进行省调双管理中心配置

在黎阳电厂专网 1 平面、2 平面纵向加密装置中新增省调备用管理中心地址，实现省调接入网纵向加密装置双管理中心配置。

1.7 网安 I 区防火墙升级改造

完成网安 I 区防火墙升级改造，采购 1 台防火墙用于黎阳电厂继电保护室专网 1 平面网安 I 区，并负责设备供货、安装、电缆敷设、系统调试等工作。改造完成后，设备配置策略满足省调、地调对厂站网络安全防护的最新要求，满足河南省调对于关键基础设施网络安全风险评估的要求并提供符合省调要求的佐证材料。

2、2023 年网安风险评估服务

黎阳电厂根据《河南电力调度控制中心关于下发 2023 年统调电厂调度自动化及网络安全重点工作的通知》、《统调电厂网络安全监测能力验证评估实施指导手册》、《河南电力调度控制中心关于上半年统调电厂电力监控系统网络安全运行情况的通报》要求，开展 2023 年网络安全风险评估服务提交年度网络安全风险评估报告。

主要工作内容包括：A、完成 2023 年度电力监控系统网络安全风险评估工作，对空闲网络和 USB 端口加装物理锁,根据河南省调要求将网络安全整改报告上传 OMS 系统；B、完成黎阳电厂 2022 年安全风险评估问题整改工作；C、地调备调工作接入，根据地调相关要求，增加 RTU 系统至专网 2 平面地调备调通道开通工作，与地调相关部分完成调试工作。

2.1 要求和标准

本次风险评估工作依据《电力监控系统安全防护规定》(国家发展改革委 2014 年第 14 号令)、《电力监控系统安全防护评估规范》、《信息安全风险评估规范》、《电力监控系统安全防护总体方案》(国能安全【2015】36 号文)、

《发电厂监控系统安全防护方案》、《信息系统安全等级保护基本要求》、《信息安全等级保护管理办法》等国家标准从风险管理角度，运用科学的方法和手段，系统地分析网络与信息系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，提出有针对性的抵御威胁的防护对策和整改措施。并为防范和化解信息安全风险，或者将风险控制在可接受的水平，从而最大限度地为保障网络和信息安全。

2.2 评估服务原则

本次电力监控系统安全风险评估服务的实施应满足以下原则：

(1)保密原则：对评估的过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据进行任何侵害招标方网络的行为，否则招标方有权追究投标方的责任。

(2)标准性原则：评估方案的设计与实施应依据国家信息安全风险评估的标准进行。

(3)规范性原则：工作过程和相关文档应具有很好的规范性，可以便于项目的跟踪和控制。

(4)可控性原则：评估服务的进度要跟上进度表的安排，保证招标方对于评估工作的可控性。

(5)整体性原则：评估的范围和内容应当整体全面，包括国家信息安全风险评估相关要求涉及的各个层面。

(6)最小影响原则：评估工作应尽可能小的影响系统和网络的正常运行，不能对现有网络的运行和业务的正常产生显著影响。

2.3 项目范围

针对电厂电力监控系统及相关业务系统所涉及的所有软硬件资产及相关管理文档。包括但不限于以下，物理安全，网络安全，操作系统安全，数据库安全，通用服务安全，应用系统安全，安全措施，数据恢复及备份，信息安全评估管理，信息安全的宣传及监督等。

2.4 工作内容

提供从资产识别，资产赋值，威胁评估，脆弱性评估，漏洞扫描，风险计算和分析,安全风险整改建议，出具风险评估报告的完整风险评估实施流程。

资产赋值：对物理，网络，主机等资产进行识别，并根据机密性，完整性，可用性进行赋值。

威胁赋值：根据人为因素，环境因素，有意损害，无意损害等对资产进行威胁赋值。

漏洞扫描：对项目范围内所涉及资产进行漏洞扫描，发现其安全性弱点。

脆弱性赋值：对项目范围内所涉及的资产，确定其对应的安全措施，评估其脆弱性，并进行赋值。

风险计算和分析：对资产，脆弱性，威胁基本要素进行分析与计算，计算安全事件一旦发生所产生的影响，即风险值，并作出简述说明。

安全风险整改建议：对风险评估中分析出的风险情况出具专业的改正意见。并根据河南电力调度控制中心对电力系统网络安全的最新要求进行服务类整改。

2.5 工作质量要求

为保证本次项目的品质和质量，投标方要依据以下标准开展工作：

(1)根据标准性、规范性、可控性、整体性、最小影响性及保密性原则，做到守时保质；与招标方签署保密协议。

(2)指派工作经验丰富、技术实力雄厚的项目经理，结合技术领先、结论可靠的评估工具为招标方做全面的电力监控系统安全风险评估。承诺评估过程按照国家标准进行，并保证对客户的资料严格保密。

(3)在指定的地点进行评估工作，按照国家标准制定的报告模板规范进行电力监控系统安全风险评估报告的编写，在评估期间和评估结束后，对评估中的重要资料和结果做好严格保密。

(4)在关键评估内容实施前（如扫描或工具测试），和招标方充分沟通和协商，并制定详细的实施方案，确保在项目实施过程中不对招标方的监控系统造成影响。

四、交付成果

根据国家相关标准，电力监控系统安全防护方案及配置信息编制技术服务包括单不限于以下内容：

1、电力监控系统安全防护方案编制。

2、电力监控系统网络安全运行管理规定编制。

3、电力监控系统应急预案编制。

4、对各电力监控及网络安全设备配置信息截图，并导出相应配置文件。

5、电力监控系统网络拓扑图结构图。

6、电力监控系统设备清单编制。

7、安全加固报告及加固佐证材料。

8、2022 年黎阳电厂关键信息网络网络安全评估的问题整改。

提供电力监控系统风险评估报告、整改报告、网络安全防护方案及配置文件、加固报告、加固佐证材料一式叁份，并提供电子版本壹份，其中应包含拓扑图，安全风险整改建议，后续安全风险处置方式，扫描工作摘要等,并由具有风险评估资质的机构出具报告并通过河南省调的审核。

完成网络安全监测装置能力提升、2023 年风险评估及问题整改、OMS 缺陷整改工作，主要包括网安 I 区 1 台防火墙，保信子站及 NCS 系统共 4 台交换机更换（含冗余通道），并负责设备供货、安装、电缆敷设、系统调试等工作，改造完成后，设备配置策略满足省调、地调对厂站网络安全防护的最新要求，满足河南省调对于关键基础设施网络安全风险评估的要求并提供符合省调要求的佐证材料。符合国网公司、国家、行业相关标准和规范。

2023 年电力监控系统安全防护评估、电力监控系统网络安全监测能力提升及缺陷整改项目进行专项技术服务项目设备/服务清单

序号	设备、服务名称	规格、型号	备注	单位	数量
1	珠海鸿瑞 HR CRPM-3000 网监装置版本升级	技术服务，出具整改报告及佐证材料。	根据省调网络安全管理平台版本校验清单，完成 I 区、II 区网络安全监测装置版本升级。	项	1
2	PSTunnel-2000L 北京科东纵向加密双管理中心	技术服务，出具整改报告及佐证材料	按照河南省调最新要求完成纵向加密双管理中心配置服务。	项	1
3	HR CRPM-3000 珠海鸿瑞网监装置双管控中心及网监资产白名单	技术服务，出具整改报告及佐证材料。	满足省调要求。	项	1
4	兰吉尔 FFC3 电能量采集终端	技术服务，出具整改报告及佐证材料。	增加对应厂家的探针并接入 I 区网络安全监测装置	项	1
5	H3C S5130 调度专网 1、2 平面数据网交换机	技术服务，出具整改报告及佐证材料。	升级设备系统版本并接入网监装置接入网。	项	4

6	#1 机组、#2 机组、启备变、线路故障录波装置探针接入服务	技术服务，出具整改报告及佐证材料。	增加对应厂家的探针，并接入II区网安（故障录波装置为 3 台山东山大，1 台成都府河），按照河南省调要求接入网络安全监测装置，完成告警测试。	项	4
7	网安 I 区防火墙	博达F5100-22防火墙 电源规格内置双 AC 电源，需提供本次采购的防火墙原厂商（上海博达数据通信有限公司）出具的针对本项目的原厂授权支持函	更换网安 I 区防火墙，含安装、调试、告警测试及资产变更工作。改造完成后，设备配置策略满足省调、地调对厂站网络安全防护的最新要求，满足河南省调对于关键基础设施网络安全风险评估的要求并提供符合省调要求的佐证材料。	台	1
8	保信子站交换机	科玛瑞讯 KNS5000 双电源交换机，需提供本次采购的网络安全监测装置设备厂商出具的针对本项目的原厂授权支持函，确保提供的网监装置版本的合规性及稳定性	更换故障录波交换机、保信子站交换机，含安装、调试、告警测试及资产变更工作。改造完成后，设备配置策略满足省调、地调对厂站网络安全防护的最新要求，满足河南省调对于关键基础设施网络安全风险评估的要求并提供符合省调要求的佐证材料。	台	2
9	NCS 系统交换机	PSC-9882-Z-E24G4南瑞继保交换机，需提供本次采购的网络安全监测装置设备厂商出具的针对本项目的原厂授权支持函，确保提供的网监装置版本的合规性及稳定性。	更换 NCS 远动装置 A 网交换机、B 网交换机，含安装、调试、告警测试及资产变更工作。改造完成后，设备配置策略满足省调、地调对厂站网络安全防护的最新要求，满足河南省调对于关键基础设施网络安全风险评估的要求并提供符合省调要求的佐证材料。	台	2
10	2023 年电力监控系统网络安全风险评估	技术服务，主要内容包含：1、完成《2022 年黎阳电厂电力监	提供电力监控系统风险评估报告、整改报告、	项	1

	工作及完成 2022 年风评问题整改工作	控系统 安全防护评估报告》中问题整改工作。 2、根据《河南电力调度控制中心关于下发 2023 年统调电厂调度自动化及网络安全重点工作的通知》、《统调电厂网络安全监测能力验证评估实施指导手册》、《河南电力调度控制中心关于上半年统调电厂电力监控系统网络安全运行情况的通报》等要求开展 2023 年网络安全风险评估。	网络安全防护方案及配置文件、加固报告、加固佐证材料一式叁份，并提供电子版本壹份，其中应包含拓扑图，安全风险整改建议，后续安全风险处置方式，扫描工作摘要等,并由具有风险评估资质的机构出具报告并通过河南省调的审核。		
11	地调备调开通	技术服务，出具整改报告及佐证材料。地调备调开通满足地调自动化相关要求；解决 I 区网安端口少的问题，并将 RTU 系统B网交换机接入I区网安、调试。	地调备调开通后与地调自动化对调数据是否一致;按要求将 RTU 系统 B 网交换机接入 I 区网络安全监测装置、调试，满足调度要求。	项	1
12	RTU 系统 B 网交换机接入 I 区网安、调试	技术服务，解决 I 区网络安全监测装置端口少的 RTU 系统 B 网交换机无法接入问题,将RTU系统B网交换机接入I区网安、调试，出具整改报告及佐证材料。	按要求将 RTU 系统 B 网交换机接入 I 区网络安全监测装置、调试，满足调度要求。	项	1

五、投标要求

5.1 投标方必须具有河南电力认可的风险评估资质，即中国网络安全审查技术与认证中心颁发的信息安全风险评估服务资质（CCRC）或 中国信息安全测评中心颁发的信息安全服务资质证书（风险评估类）。

5.2 具备 ISO27001 信息安全管理体系认证证书。

5.3 相关报告需通过河南省调的审核。

5.4 投标方需具备电力监控系统网络安全监测装置调试专业知识和技能，熟悉电力监控系统的安全防护方案及规定，提供自 2019 年 1 月 1 日起至报价截止日，单机容量 600MW 以上河南省调统调电厂的相关业绩证明文件。

六、其他要求

6.1 投标方中标后需要与招标方签订保密协议。

6.2 投标方应在省调规定的期限内完成有关工作。

6.3 本次采购安装调试完毕后，免费 1 年的维护。

6.4 乙方应提供合格的产品和施工服务，若施工材料及施工工艺不合格，不符合要求，可视该工程为不合格。

6.5 乙方必须组织足够的人力，保质保量按期完成施工任务，若施工过程中发生工作范围偏差或其它未尽事宜，乙方应先确保工作继续开展，随后双方协商解决。

6.6 本年度电力监控网络评估工作开展期间发现设备异常，乙方需提供此问题解决方法，随后双方协商解决。