云南腾电科技有限公司

曲靖供电局110kV变电站电力监控系统网络安全态势感知系统建设-项目实施方案

（YNTD-ITSS-0902）

编制人：谢广胜　　编制时间：2025.08.01

审核人：赵建中　　编制时间：2025.08.01

批准人：陆涛　　审批时间：2025.08.01

文件编制和变更履历

版本	编制/更改		发布		实施		更改记录
	作者	日期	审核	日期	批准	日期	
V1.0	谢广胜	2025.8.1	赵建中	2025.8.1	陆涛	2025.8.1	首次发布

目录

1. 项目总览

1.1. 项目背景与依据

为全面落实国家《网络安全法》、《关键信息基础设施安全保护条例》及能源行业网络安全防护系列规范要求，强化曲靖供电局所属110kV变电站电力监控系统的网络安全主动防御与态势感知能力，特规划并实施本网络安全态势感知系统（NSAP）项目。本项目旨在构建一套覆盖“采集、分析、预警、响应”全流程的网络安全纵深防护体系，实现从“被动防护”到“主动预警、智能感知”的转变，保障电网监控系统的安全稳定运行。

1.2. 建设目标

本项目计划于2025年8月正式启动，力争在2026年第一季度完成整体建设与试运行。核心建设目标如下：

全面监测： 实现对110kV变电站电力监控系统网络流量、安全设备日志、主机行为、应用访问等安全数据的全面采集与标准化处理。

智能分析： 建立基于规则和机器学习的威胁检测模型，精准识别网络攻击、异常行为、违规操作等安全事件，降低误报率。

实时预警与可视： 构建统一的网络安全态势可视化平台，实现安全风险的实时告警、全局态势的动态呈现与风险量化评估。

协同响应： 建立初步的安全事件应急响应流程，实现告警事件与运维工单的联动，提升事件处置效率。

合规达标： 建设成果需满足电力监控系统安全防护“安全分区、网络专用、横向隔离、纵向认证”的总体原则，并通过相关安全测评。

1.3. 建设范围

本项目覆盖曲靖供电局指定范围内110kV变电站的电力监控系统，主要包括：

系统范围：站控层、间隔层相关监控主机、服务器、网络设备、安全设备及关键应用系统。

功能范围： 网络安全态势感知平台软件的建设，以及必要的探针（软件/

硬件）部署、安全数据中台构建、展示中心建设等。

服务范围：包含系统规划设计、软硬件集成部署、策略配置调优、联调测试、等保定级备案协助、人员培训及初期运维支持。

2. 项目组织与管理

2.1. 项目组织架构

成立三级项目组织，确保项目高效推进：

项目领导小组： 由曲靖供电局、云南中恒及云南腾电高层领导组成，负责项目重大决策、资源协调与最终审批。

项目管理办公室（PMO）： 由三方项目经理及核心骨干组成，负责日常计划、执行、监控、沟通与风险管理。

项目实施小组：

业务协调组（甲方主导）： 负责业务需求确认、现场协调、业务数据提供及最终用户测试。

技术实施组（乙方主导）： 负责系统设计、部署、开发、测试、培训等全部技术工作。

质量与安全组（双方参与）： 负责项目质量审查、安全规范符合性检查及文档管理。

2.2. 各方职责

角色方 核心职责

曲靖供电局　　提出总体安全需求，审批建设方案，提供必要现场环境与业务接入，组织最终验收。

云南中恒　作为总集成与服务方，负责项目整体管理、资源协调、与甲方的需求对接及部分现场配合工作。

云南腾电　作为技术实施方，负责态势感知系统的详细设计、产品提供、系统集成、部署实施、技术培训及文档交付。

3. 总体技术架构与设计

本项目采用“一个中心、三层体系”的总体架构：

数据采集层： 在网络关键节点、核心服务器部署轻量级探针，通过流量镜像、Syslog、SNMP、API接口等多种方式，采集网络、安全、主机、应用日志。

数据分析层： 构建安全大数据平台，对采集的异构数据进行标准化、范式化处理，并利用关联分析引擎、威胁情报库、行为分析模型进行深度挖掘与智能分析。

态势展示与响应层： 通过统一可视化平台，实现全局安全态势概览、实时威胁告警、攻击路径溯源、资产风险画像、合规报表生成，并提供事件工单流转接口。

4. 项目实施路线图

项目分为五个阶段，循序渐进，确保建设质量。

4.1. 第一阶段：项目启动与详细设计

计划时间：2025.08 - 2025.09

目标： 完成项目蓝图设计，达成技术共识。

关键任务： 项目启动会、现场调研、需求深度分析、编制《详细设计说明书》及《实施方案》。

交付物： 《项目章程》、《详细需求规格说明书》、《系统详细设计文档》。

4.2. 第二阶段：平台搭建与数据接入

计划时间：2025.10 - 2025.12

目标： 完成核心平台部署，实现首批数据接入与分析。

关键任务： 软硬件环境准备、平台软件安装部署、采集探针部署与调试、基础数据接入、平台基本功能联调。

交付物： 部署完成的软硬件系统、《系统部署报告》、《数据接入规范》。

4.3. 第三阶段：功能实现与策略优化

计划时间：2026.01 - 2026.02

目标： 完成核心检测能力建设，实现有效预警。

关键任务： 威胁检测规则与模型配置、场景化分析仪表板开发、告警策略调优、与现有运维流程初步集成。

交付物： 《威胁检测规则集》、《态势可视化大屏》、《系统配置手册》。

4.4. 第四阶段：系统联调与试运行

计划时间：2026.03

目标： 全面验证系统功能与性能，进入实用化考核。

关键任务： 全网联调测试、模拟攻防演练、性能压力测试、系统试运行（不少于1个月）。

交付物： 《系统联调测试报告》、《试运行报告》、《应急预案》。

4.5. 第五阶段：验收交付与培训 (2026.04)

目标： 完成项目验收，移交运维能力。

关键任务： 编制竣工文档、组织全面培训、进行项目最终验收评审。

交付物： 《项目竣工报告》、《用户操作手册》、《运维手册》、《最终验收报告》。

5. 质量管理与风险控制

质量管理：

遵循ISO9001质量管理体系，设立质量检查点（如设计评审、代码审查、测试用例评审）。

所有交付物均需经过内部评审和客户确认。

试运行期间记录系统缺陷并限期整改。

风险控制：

技术风险： 采用成熟、经过电力行业验证的技术和产品；进行充分的概念验证（PoC）测试。

进度风险： 制定详尽的WBS和进度计划，使用项目管理工具跟踪，定期审视关键路径。

安全风险： 实施方案必须通过甲方安全评审；实施过程严格遵守现场安全生产规定；部署操作在业务低峰期进行。

沟通风险： 建立定期会议制度（周报、月报）和即时沟通渠道，确保信息透明对称。

6. 培训与知识转移计划

为确保系统建成后能用、好用，制定三级培训计划：

管理层培训： 介绍系统价值、呈现的宏观态势及管理报表。

运维人员培训： 重点培训平台日常监控、告警处置、报表生成、系统基础配置与维护。

分析人员培训： 深度培训威胁狩猎、事件溯源分析、检测规则自定义、情报利用等高级技能。

7. 验收标准

项目验收将分为阶段验收和最终验收。最终验收需满足以下基本条件：

系统功能符合《详细设计说明书》要求，并通过所有合同约定的测试。

系统性能指标（如数据处理延迟、页面响应时间、并发用户数）达到设计标准。

完成所有合同约定的交付物提交，且文档齐全、准确。

完成对所有相关用户的培训，且通过考核。

系统稳定试运行期满，无重大缺陷。