电力监控系统网络安全编排与响应（SOAR）技术应用探究

徐　润

（遵义供电局，贵州 遵义 563000）

摘　要　为实现对监控系统网络安全态势的实时感知与网络异常的精准预警，相关人员需开展电力监控系统网络安全编排与响应（SOAR）技术应用研究。计算监控系统网络中的节点关联性、权重，建立电力监控系统网络态势感知框架，实时感知网络安全状态；量化电力监控系统网络态势感知数值，划分网络安全保障场景，设计电力监控系统网络安全保障等级；引进 SOAR 技术，将 SOAR 技术在网络数据中台，根据网络常态化运行条件，设计安全预警界限，根据前端反馈程序与执行逻辑，驱动响应预警不同场景下的电力监控系统网络异常。本研究以遵义供电局电力为试点单位，设计实例应用实验，实验结果证明：提出的方法可以实现对网络安全态势的精准感知与预警。

关键词　电力监控系统　（SOAR）技术　编排　网络安全　态势感知

中图分类号：TM76；TP393.08　　**文献标识码**：A　　**文章编号**：1007-0745（2022）10-0022-03

公司数字化转型带来的业务多元化、电力监控系统的“烟囱式”建设，使之形成相对独立的安全保障模式，为打造高效、灵活和强大的电力监控系统指挥作战体系带来了巨大挑战。在深入遵义供电局电力监控系统安全防护的建设工作中，提出现阶段相关电力监控系统网络安全管理存在下述四个方面的问题 [1]。

一是电力监控系统主站网络安全防御设备、检测设备、分析设备品牌众多，版本繁杂，功能不同，数据模型较为复杂，实时计算指标较多的难题。

二是电力监控系统的安防设备网络拓扑结构不一，不同设备的安全策略配置变化多样。电网网络安全专业起步较晚，网络安全知识储备低下，运维人员专业知识欠缺，跟不上网络攻击技术的发展。

三是《网络安全法》颁布以前建设的业务支持系统基本没有考虑网络安全防护，防御设备具有防御功能不全、网络威胁检测手段单一、改造难度大的特点。

四是电力监控系统网络边界安全设备配置及维护工作主要依靠“人工分析”“案例”“经验分析”，缺少切实依据 [2]。

为解决上述问题，针对现阶段公司电力监控系统网络安全管理工作的难点、痛点，开展电力监控系统网络安全编排与响应（SOAR）技术应用研究，旨在减轻现场运维人员工作量，提高现场运维人员工作效率，节约人力、物力，降低运维成本。

1 电力监控系统网络态势感知

为实现对网络的安全编排与响应，根据电力系统网络节点分布，建立如下图 1 所示的框架，实时感知系统网络安全。

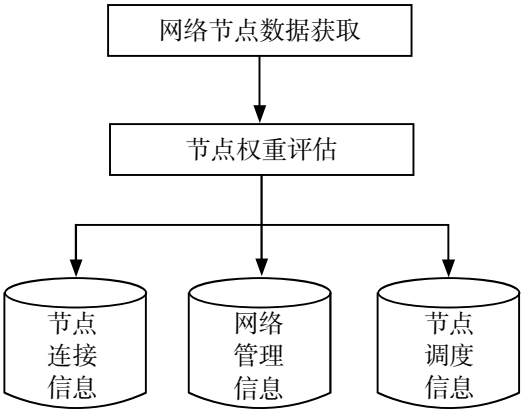

图 1　电力监控系统网络态势感知框架

随机选择电力监控系统网络中两个节点，将其表示为 A 与 B，计算节点 A 与节点 B 的空间关联性 [3]。此过程如下计算公式所示：

$$P(AB)=\frac{S}{N}+\frac{F}{N}i+\frac{Q}{N}j \tag{1}$$

公式（1）中：$P(AB)$ 表示节点 A 与节点 B 的空间关联性；S 表示网络节点集合中共性数量；N 表示网络节点集合中特征点数量；F 表示网络节点集合中差异点

表 1 网络安全保障场景与等级划分

序号	安全态势值（H）	安全保障等级	网络安全保障场景
（1）	0~0.2	四级	日常供电安全保障、居民生活运维安全保障等
（2）	0.2~0.4	三级	电力监控网络安全周活动保障、其他电力活动安全保障等
（3）	0.4~0.8	二级	重要国际活动安全保障、重要节假日活动安全保障等
（4）	0.8~1.0	一级	大型电力事故演习活动保障等

表 2 电力监控系统网络终端测试环境参数

序号	项目	参数
（1）	前置机 IP 地址	192.168.1.21
（2）	前置机端口号	15003
（3）	配置软件	数据库（Oracle、SqlServer）、Python、Php、Redis 等
（4）	操作系统	Linux 系统 /Unix 系统
（5）	Web 应用服务器	Tomcat
（6）	配置环境变量	jdk

数量；i 表示统一度；Q 表示网络节点集合中对立点数量；j 表示差异度。考虑到节点之间的 i 与 j 存在相互转化关系，因此，在分析电力监控系统网络安全态势时，可以根据节点权重分析其态势。其中节点权重的计算公式如下：

$$W=\sum_{k>1}^{k}\overline{e}_{ik} \tag{2}$$

公式（2）中：W 表示电力监控系统网络节点权重；$\overline{e}$ 表示随机一致性指标；k 表示权向量系数。在上述计算内容的基础上，根据主观权向量，评估节点在当前状态下的态势[4]。计算节点网络态势值，计算公式如下：

$$H_N=c_N/a_N \tag{3}$$

公式（3）中：H 表示电力监控系统网络节点态势值；c 表示节点连接信息当前状态；a 表示节点日志信息当前状态。按照上述方式，掌握电力监控系统网络态势值，以此种方式，实现对节点安全状态的感知。

2 网络安全保障场景与等级划分

在上述设计内容的基础上，量化电力监控系统网络态势感知数值，定义 H 的取值在 0~1 之间，定义 H 在不同取值下的网络安全状态。当 H 取值 >0，且 <0.2 时，定义其安全等级为五级，此时对应的网络安全保障场景为基础场景。按照此种方式，划分其他网络安全保障场景，划分电力监控系统网络安全保障等级[5]。具体内容如表 1 所示。

按照表 1 所述方式，划分电力监控系统网络安全保障场景，在具体工作中，匹配电力企业的活动场景与安全保障等级，为网络安全编排与响应打下基础。

3 基于 SOAR 技术的网络异常响应与预警

完成上述设计后，引进 SOAR 技术，设计电力监控系统网络异常响应与预警。可将 SOAR 技术的驱动响应过程作为网络功能封装过程，将 SOAR 技术应用在网络数据中台上，根据网络常态化运行条件，设计安全预警界限。当前端反馈的数据中携带隐患因子或异常信息超出预警界限后，SOAR 技术将立刻定位并访问前端传递信息对应的 IP 地址，确认信息存在危险性后，执行并驱动全局响应程序，以此种方式封锁账号。此过程计算公式如下：

$$K(o)=\frac{s_j}{\sum_{j>1}^{n}s_j} \tag{4}$$

公式（4）中：$K(o)$ 表示对电力监控系统网络节点 o 的驱动响应；s 表示安全指标客观权向量；n 表示危险因子。在此基础上，集成在终端的威胁情报查询器将主动扫描系统网络漏洞，并将漏洞信息反馈给数据中台，数据中台将在接收到信息后，识别并判断网络标签，根据标签识别结果，评估网络安全预警等级。

按照上述设计，在电力监控系统网络安全编排与

表 3 电力监控系统网络安全预警响应效果

时段（s）	本文方法预警次数（次）	期望预警次数（次）
0~2	0	0
2~4	2	2
4~6	1	1
6~8	1	1
8~10	0	0

响应时，技术人员需要根据当前状态下电力系统的实际状态，预先录入多种类型的网络安全策略数据，并对策略数据划分等级。在此种条件下，终端将根据前端反馈程序与执行逻辑，驱动并响应不同场景下的电力监控系统网络安全预警。以此种方式，实现对网络异常的响应与预警，完成电力监控系统网络安全编排与响应（SOAR）技术的应用研究。

4 实例应用分析

完成上述设计后，为实现对电力监控系统网络安全编排与响应技术在实际应用中效果的检验，下述将以遵义供电局电力为试点单位，按照本文设计的技术应用流程，设计如下所示的实验。

为满足实验需求，在开展相关研究前，在电力监控系统网络终端部署测试环境，环境参数如表 2 所示。

完成对测试环境的配置后，使用本文设计的 SOAR 技术，对电力监控系统网络的安全编排与响应展开测试。测试前，设计网络公开 CIC 数据集合作为此次实验的测试样本数据，在对样本的分析与评估中发现，现有数据样本集合中存在 4 个安全隐患。将数据随机录入电力监控系统网络节点，通过设计数据采样时序、数据最大训练次数、节点权重等方式，实时感知电力监控系统网络态势。同时，根据电力监控系统的应用场景，划分网络安全保障等级，并匹配安全保障场景与对应的安全等级。在此基础上，引进安全编排与响应（SOAR）技术，结合前端实时反馈的网络数据，响应并预警监控系统网络异常。

调用监控系统网络终端 PC 机后台数据，统计在 1s~10s 时段内，终端对网络异常的响应情况，其结果如表 3 所示。

根据表 3 所示的实验结果可知，本文方法对电力监控系统网络安全的预警响应次数与期望预警次数完全一致。说明本文设计的方法在实际应用中的效果良好。综合上述实验，得到如下结论：此次设计的网络安全编排与响应（SOAR）技术，可以实现对网络安全态势的精准感知与预警，通过此种方式，为遵义供电局电力监控系统网络安全、运营提供全面的保障。

5 结语

根据遵义供电局电力监控系统网络安全管理、运维特点及痛点，本文通过电力监控系统网络态势感知、网络安全保障场景与等级划分、网络异常响应与预警，完成了电力监控系统网络安全编排与响应（SOAR）技术应用研究。此次研究将业界优秀的“安全中台”管理模型在建设中进行了实践和结合，形成具有地区调度机构鲜明特点的网络安全“统一安全中台”模型，该模型将“安全能力”“安全大脑”“安全数据”“业务场景”有效整合，实现遵义供电局电力监控系统网络安全管理效能提升、数据化运营服务提升、业务连续性保障能力提升、业务场景定制化能力提升，有效实现了遵义供电局电力监控系统自身安全能力与业务需求的持续对接，是管好“发展和安全两个关键问题”的最佳实践。

参考文献：

[1] 许暖，韩志峰，郑瑞刚．基于分级分类的安全编排技术在网络安全应急响应中的应用探索 [J]. 网络空间安全，2021,12(Z1):45-53.
[2] 商宗义．多措并举 精准发力——华北能源监管局扎实开展电力监控系统网络安全监管工作 [J]. 中国电业，2021(10):36-37.
[3] 谢秋华，杨廷勇，杨云，等．主动免疫的水电站电力监控系统网络安全防护方案设计 [J]. 水电站机电技术，2021,44(08):13-16,120.
[4] 张亮，屈刚，李慧星，等．智能电网电力监控系统网络安全态势感知平台关键技术研究及应用 [J]. 上海交通大学学报，2021,55(S2):103-109.
[5] 苏生平，赵金朝．基于多维反向渗透的电力监控系统网络安全管理模式探索 [J]. 青海电力，2021,40(04):16-20.