文章编号:1007-5321(2025)05-0121-07　　**DOI**:10.13190/j.jbupt.2024-211

基于主客观分析的电力 5G 虚拟专网安全风险评估方法设计

梅文明[1]，刘智铭[2]，胡柏吉[2]，张大华[2]，刘　新[3]
(1. 国家电网有限公司，北京 100031；2. 中国电力科学研究院有限公司，北京 100192；
3. 国家电网山东省电力公司 电力科学研究院，济南 250002)

摘要：第 5 代移动通信系统(5G)虚拟专网承载电力业务，在提升系统承载量的同时，也带来了新的安全挑战。通过对电力系统进行安全性分析，能够有效辨识安全风险，并指导后续的安全防护策略设计。然而，现有方法一方面缺乏具有针对性的体系构建，另一方面未能给出直观的量化评估。基于电力业务特点提出了基于主客观分析的电力 5G 虚拟专网安全风险评估方法，搭建评估指标体系，并通过层次分析法、熵值法等方法从主客观 2 方面对安全风险进行分析评估。最后，通过实例分析证明了所提安全风险评估方法的有效性和适用性。

关　键　词：电力无线通信系统；第 5 代移动通信系统虚拟专网；安全风险评估；主客观分析法
中图分类号：TP711　　**文献标志码**：A

Design of a Security Risk Assessment Method for Power 5G Virtual Private Network Based on Subjective and Objective Analysis

MEI Wenming[1]，LIU Zhiming[2]，HU Baiji[2]，ZHANG Dahua[2]，LIU Xin[3]
(1. State Grid Corporation of China，Beijing 100031，China；2. China Electric Power Research Institute，Beijing 100192，China；
3. Electric Power Science Research Institute，State Grid Shandong Electric Power Company，Jinan 250002，China)

Abstract：The 5th generation of mobile communications system (5G) virtual private network carrying power business not only increase system capacity，but also bring new security challenges due to the openness. Conducting security analysis on wireless power systems can effectively identify security risks and guide the design of subsequent security protection strategies. However，existing methods lack targeted framework construction and fail to provide intuitive quantitative evaluations. In this paper，a security risk assessment method for power 5G virtual private network is proposed based on the characteristics of power business. On the basis of building the assessment indicators framework，the analysis of security risks is conducted from subjective and objective aspects through analytical hierarchy process and entropy value method. Finally，the effectiveness and applicability of the proposed safety risk assessment method is proved through example analysis.

Key words：wireless power system；the 5th generation of mobile communications system virtual private network；security risk assessment；subjective and objective analysis

收稿日期：2024-10-18
基金项目：国家电网有限公司总部科技项目(5700-202316291A-1-1-ZN)
作者简介：梅文明(1983—)，男，高级工程师。
通信作者：刘智铭(1996—)，男，工程师，邮箱：liuxiaoxiaoming@163.com。

随着全球能源转型的加速推进,电力行业正经历着前所未有的变革,逐步向清洁、高效、智能的新型电力系统转型。在这一转型过程中,电力业务呈现出了场景多样化、终端海量化、需求个性化的发展趋势,各业务融入了物联网、大数据、云计算等现代信息技术以达成深度数字化和智能化[1]。

然而,这一转变也伴随着数据量的爆炸性增长和业务需求的复杂化。有线通信网络受限于建设成本、地理条件、承载能力和灵活性等因素,难以满足电力业务传输需求[2],无线通信网络,尤其是第5代移动通信系统(5G, the 5th generation of mobile communications system)[3]在发、输、变、配、用等用电环节中展现出巨大潜力,不仅提升了传输速率和承载量等关键系统性能,还为实现电网实时控制、精准运维和高效管理提供了强有力的技术支撑。然而,5G在带来诸多优势的同时,也伴随着一系列新的安全挑战和风险[4]。例如,分布式拒绝服务攻击[5]、数据空口传输[6]、核心网数据泄露[7]等信息泄露风险,可能导致电力业务控制指令、隐私数据泄露,甚至业务中断。5G混合组网导致的公网交互[8]、多制式网络切换[9]等风险也导致了潜在的恶意渗透等威胁。上述风险的存在令5G虚拟专网承载电力业务面临着严峻的安全挑战。因此,亟须制定完善、全面的风险评估方法。

当前,已有部分研究聚焦于无线通信网络承载电力业务的安全性分析,通过模拟攻击场景,展示了无线网络在应对各类已知攻击时存在的安全风险和漏洞[10-11]。一方面,现有研究缺乏针对5G网络和电力业务特点设计的具备系统性、全面性的安全风险评估体系;另一方面,多数研究停留在定性分析阶段,未能有效量化不同层面的安全风险数值,导致评估结果难以直观反映实际安全状况。

针对现有存在的量化评估体系缺位、评估指标和信息模糊的问题,设计了一套适用于5G虚拟专网承载电力业务场景、包含完整评估体系的安全风险评估方法,从主客观2个角度对系统内的各类安全风险进行了分析评估,并在评估过程中根据电力业务的实际特点引入了安全风险影响范围和影响程度2个关键指标,实现了对电力5G虚拟专网下安全风险的全面、准确的量化评估。最后,通过实例分析给出了对秒级涉控类电力业务的综合风险评估,在填补现有安全风险量化评估方法空白的同时,为制定安全防护策略提供了有力支持。

1 主客观组合赋权分析法

主客观组合赋权分析法是一种在综合决策过程中,将多种权重分配方法相结合以得出更加全面和合理的权重分配结果的方法。其中,主观赋权法主要通过专家经验和知识反映偏好和意图,而客观赋权法则基于数据本身的信息量和统计特性。

层次分析法是一种根据给定标准评估并选择方案的多准则决策技术[12-13]。通过构建层次结构模型,将复杂的决策问题分解为具有层次结构、分属于若干层次、可以独立分析的若干子问题,并在此基础上通过比较元素对上层层次中元素的影响来对其进行系统地评估,最终得出决策结果。为了避免此方法存在的较大随机性和波动性,存在部分研究利用模糊集合和模糊关系,综合对部分边界模糊、不易定量的因素进行定量评价[14]。

信息熵用于衡量所提供有效信息的丰富程度或价值贡献[15]。基于熵的特性,可以利用其来判断评估结果的离散程度。例如,信息熵可以通过冗余度、不确定性的度量以协助优化数据压缩算法[16]等。与在重要节点识别领域的应用相似,信息熵还用于在信息系统内量化评估各性能指标的重要性,为系统分析和改造提供参考数据[17]。对于信息系统安全性评估而言,信息熵也提供了一种具备可行性和适应性的量化评估机制。

2 安全风险评估方法设计

随着电力业务场景的多样化发展和电力数据海量化增长趋势的浮现,5G成为了承载电力业务的主要无线数据传输方案之一。与此同时,电力业务场景下潜藏的安全风险也持续增加,亟须从系统的角度出发对安全风险进行有效、量化的评估,从而设计对应的安全防护机制和策略,以确保电力业务的安全稳定运行。

2.1 安全风险评估指标体系构建

目前电力业务安全风险评估主要基于定性指标,为提高风险评估方法的针对性和可用性,在本小节中将电力5G虚拟专网安全划分为关键基础设施安全、电力无线网络安全、电力业务数据安全、电力系统应用安全和电力生产管理安全5个方面[18]构建评估指标体系。其中,关键基础设施安全指系统内与各类设备主要相关的安全因素,主要包括外部环境安全、设备硬件安全、软件更新

安全 3 个具体因素；电力无线网络安全指系统内信息在无线通信过程中的相关安全因素，主要包括 5G 协议安全、无线链路安全、设备访问控制 3 个具体因素；电力业务数据安全指电力业务数据在系统内流转过程中的相关安全因素，包括数据存储安全、系统密钥安全、机密合规 3 个具体因素；电力系统应用安全指电力业务服务提供过程中的相关安全因素，主要包括云平台安全、接入安全、业务隔离 3 个具体因素；电力生产管理安全指电力业务场景下与生产、管理等层面相关的安全因素，主要包括生产管理机制、内部人员管理、重要资产管理 3 个具体因素。

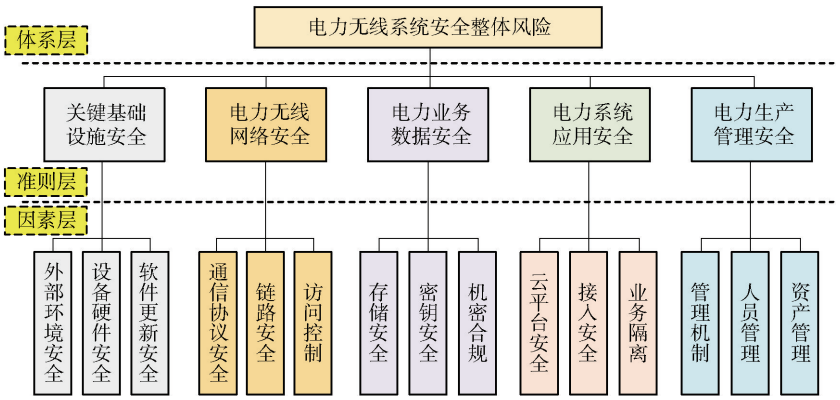

图 1　电力 5G 虚拟专网安全风险评估指标体系

构建科学且系统的安全风险评估指标体系是量化设计风险评估方法的基础先决条件。所提体系旨在清晰划分电力系统各层次、各维度的安全因素，从而提高安全风险评估方法的准确性和实用性，并为后续主、客观指标权重的确定提供可靠体系支撑。

2.2　基于层次分析法的主观权重计算

电力系统贯穿发、输、变、配、用各个环节，环环相扣且相互影响，部分潜在的安全风险隐藏在复杂的电力业务逻辑和特殊工况中，现阶段仍需要经验丰富的专业人员凭借实践经验对安全风险进行评估。同样的，由于电力业务场景的复杂性和评估人员个人知识结构的局限性，在对电力业务场景下潜在安全风险的危害性进行评估时，易遭遇惯性思维问题。为解决这一问题，在层次分析法的基础上引入并应用了模糊综合评判方法，该方法能够有效剔除多方面模糊因素对评判过程的干扰。

基于以上安全风险评估指标体系，本小节结合模糊综合评判和层次分析法计算各指标的主观权重，并基于一致性检验进行可靠性判断，具体步骤如下。

1）判定矩阵构造：基于层次分析法将同一方面的指标进行两两对比，并通过数学语言对比较结果进行描述[19]。

根据专家打分及历史经验，基于标度基准对各层判断指标构造判定矩阵 $\boldsymbol{A}=(a_{ij})_{n\times n}$，具体如下：

$$\boldsymbol{A}=\begin{pmatrix}1 & a_{12} & \cdots & a_{1n}\\ a_{21} & 1 & \cdots & a_{2n}\\ \vdots & \vdots & & \vdots\\ a_{n1} & a_{n2} & \cdots & 1\end{pmatrix} \tag{1}$$

其中：$a_{ij}>0$；当 $i\neq j$ 时，$a_{ij}=1/a_{ji}$；矩阵中的元素 a_{ij} 为该层上第 i 个指标和第 j 个指标的相对重要情况。

2）各层次指标权重确定：对矩阵中的向量按列进行规范化处理，即如下归一化操作：

$$\boldsymbol{A}'=(a'_{ij})_{n\times n}=\left(\frac{a_{ij}}{\sum_{k=1}^{n}a_{kj}}\,\middle|\,i=1,2,\cdots,n\right)_{n\times n} \tag{2}$$

然后，将归一化得到的矩阵 $\boldsymbol{A}'$ 按行求和得到权重向量 $\boldsymbol{W}'=(w'_1,w'_2,\cdots,w'_n)$ 为

$$w'_1=\sum_{k=1}^{n}a'_{kj};\ i=1,2,\cdots,n \tag{3}$$

最后，将以上权重向量再次进行归一化处理以得出最终各层次指标权重 $\boldsymbol{W}=(w_1,w_2,\cdots,w_n)$。

3）指标一致性检验：为评估指标权重是否符合实际情况，需要通过一致性检验的方式保证评估准确性，一致性检验以特征根为基础，判断后续计算得到的一致性比率是否满足一致性条件。最大特征根 $\lambda_{\max}$ 和后续一致性比率 C 的计算如下：

$$\lambda_{\max}=\sum_{i=1}^{n}\frac{(\boldsymbol{AW})_i}{nw_i} \tag{4}$$

$$C=\frac{\lambda_{\max}-n}{R_{\text{ave}}(n-1)} \tag{5}$$

基于现有普遍经验,若 C 值小于0.1,则判定矩阵通过一致性检验,具体所采用的平均随机一致性标度 R_{ave} 值如表1所示。

表1 随机一致性检验指标值

n	1	2	3	4	5	6	7	8
R_{ave}	0.00	0.00	0.58	0.90	1.12	1.24	1.32	1.41

4)模糊关系确定:根据模糊综合评判方法,设指标集为 $\boldsymbol{X}^k=(X_1^k,X_2^k,\cdots,X_m^k,\cdots,X_M^k)$,其中 X_m^k 表示第 k 层的第 m 个评估指标;设判断集 $\boldsymbol{Y}=(Y_1,Y_2,\cdots,Y_m)$ 表示针对不同指标产生威胁的可能性。为了方便实际应用并贴近电力业务场景,同时采用专家调查的方式确定判断集和指标集间的映射关系 $\boldsymbol{R}:\boldsymbol{X}^k\rightarrow\boldsymbol{Y}$。此时,将模糊主观指标权重定义为

$$w_i^f=w_i\left(\sum_{l=1}^{L}c_{i,l}B_l\right) \tag{6}$$

其中:$c_{i,l}$ 是根据专家调查得到的指标风险等级频数,B_l 是该风险等级对应的具体严重程度。得到某层次下各指标的模糊主观指标权重后,对其进行归一化操作即得到最终的各指标主观权重 $\boldsymbol{W}^{\text{sub}}$。

2.3 基于信息熵和扩散范围的客观权重计算

在本小节中,基于信息熵和扩散范围评估电力无线通信系统安全风险指标的客观权重。为了提炼出具有广泛适用性的评估准则,暂时从理论层面评估潜在的共性风险。同时,由于电力无线通信系统的特殊性,需要在定量分析中进一步明确各风险发生后所影响的具体范围。在实际场景中,可以根据风险发生后受影响的具体设备数量确定风险程度值,而在本小节中为了便于后续的综合评估,通过4个等级划分风险的扩散范围,并采用最大隶属度原则确定风险扩散范围,如表2所示。

表2 风险扩散范围数值

风险扩散级别	个体	小范围局部	大范围局部	整体
风险扩散范围值	0.1	0.4	1.0	5.0

其中:单一个体指影响仅限于1个具体的个体或实体,如单一设备或单一个人,此种扩散范围小,直接相关性强,易于观察和评估;小范围局部指影响扩展到了一定数量的个体或实体,但仍然局限于1个较小的区域,例如电力网络内单一网关覆盖的较小区域,此种影响范围相对较大,但仍可控制在一定范围内;大范围局部指影响扩散到了某一单独功能区或厂区,此种影响范围较广;系统整体指可能影响全国电力业务的正常运行。综上,所提信息熵和扩散范围的客观权重计算具体步骤如下。

1)原始矩阵构造:对于有 m 个电力业务和 n 个指标的安全风险评估指标体系,首先根据各评估指标对应的初始值构建矩阵 $\boldsymbol{M}=(x_{ji})_{m\times n}$,其中 x_{ji} 表示第 i 个指标在第 j 个业务中的评估值,具体为1段时间内与该指标相关的风险事故次数。

2)特征权重计算:根据第 j 个业务下各指标的值计算各指标的特征权重为

$$p_{ji}=\frac{x_{ji}}{\sum_{j=1}^{m}x_{ji}} \tag{7}$$

3)信息熵值计算:基于各指标权重计算指标对应的熵值 E_i 为

$$E_i=\frac{-\frac{1}{\ln m}}{\sum_{j=1}^{m}p_{ji}\ln p_{ji}} \tag{8}$$

4)指标权重归一化计算:根据指标 i 在不同业务下的风险扩散范围值 S_{ji} 和信息熵值 E_i 计算各指标客观权重 w_i^o 为

$$w_i^o=\frac{(1-E_i)\sum_{j=1}^{m}S_{ji}}{m\sum_{i=1}^{n}(1-E_i)} \tag{9}$$

从而可以得到基于信息熵和扩散范围的客观指标权重 $\boldsymbol{W}^{\text{obj}}=(w_1^o,w_2^o,\cdots,w_n^o)$。

2.4 基于最优组合赋权法的综合风险评估

为了兼顾以上主观指标权重和客观指标权重,以实现电力5G虚拟专网安全风险的综合评估,在本小节中采用最优组合赋权法,以综合专家意见和客观情况。对于电力业务而言,持续稳定地提供服务是系统的核心能力,而吞吐量是衡量系统能否满足业务需求的关键指标之一。如果系统的吞吐量能够满足业务高峰期的需求,那么就可以有效避免因系统性能问题导致的业务中断,进而保证了系统的安全性。同时,在以上提出的安全风险评估指标体系中,以吞吐量作为各层级指标下的系统性能观测点,能够给出遭遇各类安全风险冲击后的性能波动。

表3 风险影响等级与吞吐量对照表 %

影响等级	1	2	3	4
涉控业务	$t\geqslant85$	$85>t\geqslant75$	$75>t\geqslant60$	$t<60$
非涉控业务	$t\geqslant75$	$75>t\geqslant65$	$65>t\geqslant50$	$t<50$

需要注意的是，涉控业务由于其敏感性和实时性，普遍具备较高的运行标准，具体系统吞吐量对应的风险影响程度如表 3 所示，通过 t 表示实时吞吐量和常态吞吐量的比率。综上，所提出的基于最优组合赋权法的综合风险评估步骤如下。

1）指标组合权重计算：基于最优组合赋权法，可以将在 2.1 和 2.2 小节中得到的主观权重 w_i^f 和客观权重 w_i^o 通过加权求和的方式进行计算，以得到第 j 个业务下的综合评估值为

$$\boldsymbol{M}_j = \sum_{i=1}^{n} w_i x_{ji} = \sum_{i-1}^{n} (k_1 w_i^f + k_2 w_i^o) x_{ji} \quad (10)$$

其中：k_1 和 k_2 分别表示主观权重和客观权重的加权系数，此时可以将问题转换为最优组合系数的求解问题。

2）最优组合系数求解：为尽可能满足多指标评价体系中指标分散、评估对象存在差异的特点，基于赋权计算方法求解最优组合系数为

$$\max F(k_1, k_2) = \max \sum_{j=1}^{m} \boldsymbol{M}_j = \max \sum_{j=1}^{m} \sum_{i=1}^{n} (k_1 w_i^f + k_2 w_i^o) x_{ji} \quad (11)$$

其中：$k_1^2 + k_2^2 = 1$，$k_1 k_2 \geqslant 0$，进一步，根据拉格朗极值原理可得到最优组合系数 k_1^* 和 k_2^* 为

$$k_1' = \frac{\sum_{j=1}^{m} \sum_{i=1}^{n} w_i^f x_{ji}}{\sqrt{\left(\sum_{j=1}^{m} \sum_{i=1}^{n} w_i^f x_{ji}\right)^2 + \left(\sum_{j=1}^{m} \sum_{i=1}^{n} w_i^o x_{ji}\right)^2}} \quad (12)$$

$$k_2' = \frac{\sum_{j=1}^{m} \sum_{i=1}^{n} w_i^o x_{ji}}{\sqrt{\left(\sum_{j=1}^{m} \sum_{i=1}^{n} w_i^f x_{ji}\right)^2 + \left(\sum_{j=1}^{m} \sum_{i=1}^{n} w_i^o x_{ji}\right)^2}} \quad (13)$$

接着，对 k_1' 和 k_2' 进行归一化处理后得到最优组合系数 $k_1^* = k_1'/(k_1' + k_2')$，$k_2^* = k_2'/(k_1' + k_2')$，从而计算得到主客观综合权重 $\boldsymbol{W} = (w_1, w_2, \cdots, w_n)$。

3）综合风险计算：为了从实际情况出发评估综合风险 $\boldsymbol{W}^*$，本小节以系统吞吐量为指标分析各风险因素对系统运行的具体影响程度，并作为综合风险计算的因子之一：

$$w_i^* = \left(\sum_{j=1}^{m} w_i d_{ji}\right) \Big/ m \quad (14)$$

其中：d_{ji} 表示第 i 个指标在第 j 个业务下对系统运行的风险影响等级，从而根据得到的评估值 $\boldsymbol{W}^* = (w_1^*, w_2^*, \cdots, w_n^*)$ 以确定在电力 5G 虚拟专网安全风险评估体系下各相关风险的威胁等级。

3　实例分析

在本节中，基于电力业务实际场景进行实例分析，验证所提评估方法的有效性。为了便于归纳总结，将电力业务按照业务类型分为涉控类业务和非涉控类业务，并根据业务需求将涉控类业务进一步划分为毫秒级业务和秒级业务，将非涉控类业务划分为采集类业务和市场类业务。同时，基于 Python 搭建仿真平台评估所提方法。

3.1　实例计算

以 5G 虚拟专网承载秒级涉控类业务为例，结合系统拓扑结构，按照所提出的安全风险评估指标体系进行模型构建，具体步骤如下：首先为了便于分析和描述，将基础设施安全、网络安全、数据安全、应用安全、管理安全 5 个准则层评估指标分别记为 $B_1^2 \sim B_5^2$，针对基础设施安全 B_1^2 的因素层指标，标记为 $B_1^3 \sim B_3^3$，其余指标同理。在主观评估分析部分，由 20 位专家从实际业务特点的角度出发，对各指标之间的重要性进行对比，并给出每个指标对应的指标风险等级，从而利用层次分析法和模糊综合评判得到安全风险指标主观权重值，表 4 和表 5 分别为准则层和部分因素层指标的判定矩阵，以及对应的主观权重 $\boldsymbol{W}^{\text{sub}}$ 和一致性比率 C。

表 4　准则层指标判断矩阵

B^1	B_1^2	B_2^2	B_3^2	B_4^2	B_4^2	$\boldsymbol{W}^{\text{sub}}$	C
B_1^2	1	5	3	2	5	0.396	0.089 7
B_2^2	1/5	1	2	3	3	0.245	0.089 7
B_3^2	1/3	1/2	1	2	3	0.162	0.089 7
B_4^2	1/2	1/3	1/2	1	3	0.134	0.089 7
B_5^2	1/5	1/3	1/3	1/3	1	0.060	0.089 7

表 5　因素层指标相对于基础设施安全的判断矩阵

B_1^2	B_1^3	B_2^3	B_3^3	$\boldsymbol{W}^{\text{sub}}$	C
B_1^3	1	5	3	0.616	0.090 6
B_2^3	1/5	1	2	0.253	0.090 6
B_3^3	1/3	1/2	1	0.131	0.090 6

同时，根据基于信息熵和扩散范围对安全风险进行客观分析，并计算得到各层评估指标的客观权重。在此实例计算过程中，选定配电自动化（三

遥)、分布式电源调控和变电站巡检机器人3个具体5G虚拟专网秒级涉控类业务,以该业务中与不同安全风险相关的事故发生频数为客观观测数据,经计算得到的准则层各指标客观权重为

$$\boldsymbol{W}_1^{\text{obj}} = (w_{11}^o, w_{12}^o, w_{13}^o, w_{14}^o) = (0.079, 0.217, 0.084, 0.383, 0.237)$$

同时,经计算得到的因素层各指标客观权重为

$$\boldsymbol{W}_2^{\text{obj}} = (w_{21}^o, w_{22}^o, w_{23}^o, w_{24}^o) = (0.323, 0.110, 0.567)$$

$$\boldsymbol{W}_3^{\text{obj}} = (w_{31}^o, w_{32}^o, w_{33}^o, w_{34}^o) = (0.456, 0.271, 0.273)$$

$$\boldsymbol{W}_4^{\text{obj}} = (w_{41}^o, w_{42}^o, w_{43}^o, w_{44}^o) = (0.347, 0.513, 0.140)$$

$$\boldsymbol{W}_5^{\text{obj}} = (w_{51}^o, w_{52}^o, w_{53}^o, w_{54}^o) = (0.539, 0.229, 0.231)$$

$$\boldsymbol{W}_6^{\text{obj}} = (w_{61}^o, w_{62}^o, w_{63}^o, w_{64}^o) = (0.454, 0.429, 0.117)$$

基于以上得到的主客观指标权重,通过2.4小节中方法计算得到的准则层最优组合系数为(0.387,0.613);经计算得到的各因素层最优组合系数分别为(0.413, 0.587),(0.503, 0.497),(0.464,0.536),(0.517,0.483)和(0.505,0.495)。根据各风险因素对系统运行的具体影响程度求解得到的准则层综合风险评估值为(0.403, 0.304, 0.266,0.862,0.283);因素层 $B_1^2 \sim B_5^2$ 的综合风险评估值为(0.740, 0.225, 0.387),(0.779, 0.486, 0.482),(0.908, 0.927, 0.107),(0.979, 0.539, 0.350),(0.801,0.593,0.103)。

3.2 实例分析与比较

在本小节中,给出了具体的安全风险统计结果,如图2所示。

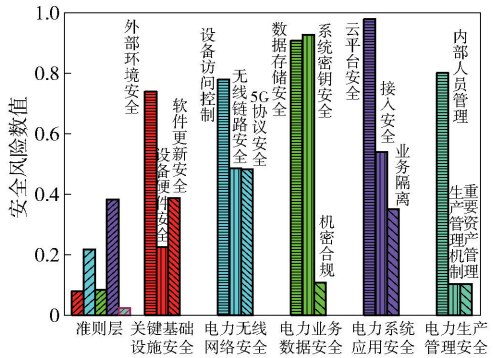

图2 电力5G虚拟专网安全风险统计结果

图2给出了准则层和因素层下各指标的安全风险统计结果。柱形图中各条长度表示该指标下电力5G虚拟专网的具体安全风险值。从图2中可以看出,在准则层中,安全风险数值最高的指标为电力系统应用安全,数值最低的指标为电力生产管理安全,这是由于目前的安全制度建设和安全培训已经较为完善,仅存在个别人员由于自身操作失误等原因导致的少量安全事故,且此类事故由于在生产环境中具备稳定的隔离措施,影响普遍都在可控范围内。而电力系统应用安全作为现有恶意攻击的主要侵入点和目标,承受了大量网络攻击,且在受到攻击后会对系统的运行造成较为严重的不良影响,同时由于各类电力业务在无线网络中的复合化,导致了较大的安全风险,需要给予更多的关注并设计相对应的安全机制和策略。

对于不同准则而言,关键基础设施安全中风险数值平均值为0.451,方差为0.046,各因素层指标风险数值较为离散,各因素层指标间相对独立,相关性较小,其中最高的指标为外部环境安全,这主要是由于极端天气等具备不可抗力的突发情况难以预测和有效预防,对物理基础设施构成了直接威胁;电力无线网络安全中风险数值平均值为0.582,方差为0.019,各因素层指标风险数值较为平均,各因素层指标间由于共同的网络底座而相关性较大,其中风险数值最高的指标是设备访问控制,恶意攻击者通过伪造或冒用身份接入系统,不仅可能导致数据泄露,还可能对系统造成更严重的破坏;电力业务数据安全中风险数值平均值为0.647,方差为0.146,各因素层指标风险数值十分离散,各因素层指标间相对独立,相关性很小,其中风险数值最高的指标是系统密钥安全,密钥是数据加密和解密的核心,一旦泄露或被盗用,将直接威胁到数据的机密性和完整性;电力系统应用安全中风险数值平均值为0.623,方差为0.069,各因素层指标风险数值较为离散,各因素层指标间相对独立,相关性较小,其中风险数值最高的指标是云平台安全,当承载各类应用和服务的云平台受到攻击而失能后,系统将大概率整体崩溃;电力生产管理安全中风险数值平均值为0.499,方差为0.086,各因素层指标风险数值较为离散,各因素层指标间相对独立,相关性较小,其中风险数值最高的指标是内部人员管理,这反映了人员在安全管理中的主体地位。

4 结束语

为了量化评估安全风险,面向电力业务场景提出了一种电力5G虚拟专网安全风险评估方法。所提方法首先基于电力场景特点构建了评估指标体系,将安全风险进行了层次化划分,其次从主客观2个维度出发,分别基于层次分析法、模糊综合评判

和熵值法评估了各风险指标权重。同时，在对综合风险值的计算中也加入了影响范围和影响程度 2 个实际场景中需要着重考虑的关键因素。实例分析展示了所提方法与电力业务的适配性，表明所提方法能够有效评估 5G 虚拟专网承载不同电力业务的安全风险数值，为安全防护策略的设计提供指导。

参考文献：

[1] BEDI G, VENAYAGAMOORTHY G K, SINGH R, et al. Review of Internet of things (IoT) in electric power and energy systems[J]. IEEE Internet of Things Journal, 2018, 5(2): 847-870.

[2] DIB L D M B A, FERNANDES V, FILOMENO M L, et al. Hybrid PLC/wireless communication for smart grids and Internet of things applications[J]. IEEE Internet of Things Journal, 2017, 5(2): 655-667.

[3] CHETTRI L, BERA R. A comprehensive survey on Internet of things (IoT) toward 5G wireless systems[J]. IEEE Internet of Things Journal, 2019, 7(1): 16-32.

[4] YAN Y, QIAN Y, SHARIF H, et al. A survey on cyber security for smart grid communications[J]. IEEE Communications Surveys and Tutorials, 2012, 14(4): 998-1010.

[5] OLIMID R F, NENCIONI G. 5G network slicing: A security overview[J]. IEEE Access, 2020, 8: 99999-100009.

[6] ALWIS C, PORAMBAGE P, DEV K, et al. A survey on network slicing security: Attacks, challenges, solutions and research directions[J]. IEEE Communications Surveys and Tutorials, 2024, 26(1): 534-570.

[7] 冯登国, 徐静, 兰晓. 5G 移动通信网络安全研究[J]. 软件学报, 2018, 29(6): 1813-1825.
FENG D G, XU J, LAN X. Study on 5G mobile communication network security[J]. Journal of Software, 2018, 29(6): 1813-1825.

[8] 苏俊浩, 刘晗, 王玉东, 等. 电力业务与公网 5G 匹配模式及合作建设[J]. 邮电设计技术, 2023(6): 51-57.
SU J H, LIU H, WANG Y D, et al. Matching mode and cooperative construction of power service with public 5G network[J]. Designing Techniques of Posts and Telecommunications, 2023(6): 51-57.

[9] 杨建, 张若文. 基于 5G 共建共享场景的典型网络切换优化问题分析[J]. 通信与信息技术, 2022(2): 36-37.
YANG J, ZHANG R W. Analysis of typical network handover optimization issues in 5G co-construction and sharing scenarios[J]. Commnication and Information Technology, 2022(2): 36-37.

[10] LIU J N, WENG J, YANG A, et al. Enabling efficient and privacy-preserving aggregation communication and function query for fog computing-based smart grid[J]. IEEE Transactions on Smart Grid, 2019, 11(1): 247-257.

[11] ISLAM S N, BAIG Z, ZEADALLY S. Physical layer security for the smart grid: Vulnerabilities, threats, and countermeasures[J]. IEEE Transactions on Industrial Informatics, 2019, 15(12): 6522-6530.

[12] SAATY T L. How to make a decision: The analytic hierarchy process[J]. European Journal of Operational Research, 1990, 48(1): 9-26.

[13] TIAN G, ZHANG H, ZHOU M C, et al. AHP, gray correlation, and TOPSIS combined approach to green performance evaluation of design alternatives[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2017, 48(7): 1093-1105.

[14] 付国庆, 龚军, 吕小毅. 基于 AHP 与模糊数学的信息安全风险评估模型[J]. 信息安全与通信保密, 2014(10): 100-103.
FU G Q, GONG J, LV X Y. Information security risk assessment model based on AHP and fuzzy[J]. Information Security and Communications Privacy, 2014(10): 100-103.

[15] STRAATHOF S M. Shannon's entropy as an index of product variety[J]. Economics Letters, 2007, 94(1): 297-303.

[16] BALAKRISHNAN K J, TOUBA N A. Relationship between entropy and test data compression[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2007, 26(2): 386-395.

[17] HUANG L, SHEN Y, ZHANG G, et al. Information system security risk assessment based on multidimensional cloud model and the entropy theory[C]//2015 IEEE 5th International Conference on Electronics Information and Emergency Communication, IEEE, 2015: 11-15.

[18] WILLIAMS P, DUTTA I, DAOUD H, et al. Security aspects of Internet of things-a survey[C]//2020 IEEE 6th World Forum on Internet of Things (WF-IoT), IEEE, 2020: 1-6.

[19] LIAO H, MI X, XU Z, et al. Intuitionistic fuzzy analytic network process[J]. IEEE Transactions on Fuzzy Systems, 2018, 26(5): 2578-2590.