DOI:10.20033/j.1003-7241.(2025)06-0090-05

配电网便携式运维管控平台集群信息安全性评估模型设计

杭海燕[1]，史俊霞[1]，黄志华[1]，徐轶兵[2]
（1.国网浙江省电力有限公司湖州供电公司，浙江 湖州 313000；
2.上海物盾信息科技有限公司，上海 201100）

摘 要：针对目前使用的基于德尔菲-层次分析法（delphi-analytic hierarchy process，D-AHP）与灰色理论、基于二维结构熵的信息安全风险评估方法无法识别全部脆弱点，导致评估结果不精准的问题，构建配电网便携式运维管控平台集群信息安全性评估模型。通过对平台集群信息安全性评估模块化分析，能够对多个模块的节点信息进行统一安全风险评估。通过分析攻击图来识别脆弱点，并对运维管控平台n层节点进行了量化处理。计算节点脆弱度，获取有效攻击路径。构建基于层次结构的平台集群信息安全性评估指标体系，计算目标层权重，并对计算结果进行模糊评价。使用相乘法进行信息处理，定义一个二元函数，通过对信息交换的损失计算，得到相应安全风险值。结合矩阵法来构建安全性评估数学模型，并划分信息安全性风险评估等级。由实验结果可知，该模型能够精准识别脆弱点，且安全性评估结果精准度最高为0.99，具有精准评估效果。

关键词：配电网；便携式运维管控平台；集群信息；安全性评估模型
中图分类号：TP18；TP309 文献标识码：A 文章编号：1003-7241(2025)06-0090-05

Design of Cluster Information Security Assessment Model for Portable Operation and Maintenance Management Platform of Distribution Network

HANG Hai-yan[1], SHI Jun-xia[1], HUANG Zhi-hua[1], XU Yi-bing[2]
(1. State Grid Zhejiang Electric Power Co., Ltd., Huzhou Power Supply Company, Huzhou 313000, China;
2. Shanghai Wudun Info Tech Co., Ltd., Shanghai 201100, China)

Abstract: Aiming at the problem that the current information security risk assessment methods based on delphi-analytic hierarchy process (D-AHP) and grey theory、two-dimensional structural entropy can not identify all vulnerable points, leading to inaccurate assessment results, a cluster information security assessment model for portable operation and maintenance management platform of distribution network is constructed. Through modular analysis of platform cluster information security assessment, unified security risk assessment can be carried out for node information of multiple modules. The vulnerable points are identified by analyzing the attack graph, and the n-layer nodes of the o&m and control platform are quantified. It calculates the vulnerability of nodes and obtains effective attack paths. A hierarchical platform cluster information security evaluation index system is constructed, the weight of target layer is calculated, and the results are evaluated fuzzy. A binary function is defined for information processing by using phase multiplication, and the corresponding safety risk value is obtained by calculating the loss of information exchange. Combined with matrix method, the mathematical model of security assessment is constructed and the risk assessment grade of information security is divided. According to the experimental results, the model can accurately identify vulnerable points, and the highest accuracy of safety evaluation results is 0.99, which has accurate evaluation effect.

Keywords: distribution network; portable operation and maintenance control platform; cluster information; security assessment model

0 引言

当前，配电网运维管控平台设计得越来越简洁，方便携带，用户对平台集群信息的依赖性越来越强。但是，一方面，由于其本身的特殊性和局限性，以及其本身存在的缺陷，使得其在为人类的工作带来方便和高效的同时，也面临着病毒、蠕虫、木马等各种攻击。因此，如何有效地预防各类安全威胁，降低对信息系统的伤害，已经越来越引起人们的重视。为此，需对信息安全性评价。有的学者提出了基于D-AHP与灰色理论的信息安全评估方法，通过构建评估指标体系，建立D层次化模型，结合灰色理论求解指标权重，以此评估信息是否安全[1]；还有的学者提出了基于二维结构熵的评估方法，分析平台正常和故障前后运行的差异数据，构建基于二维结构熵的评

收稿日期：2023-12-27

估模型，以此分析信息安全性[2]。然而，上述这两种方法的研究都是针对脆弱节点进行统一识别的，不能准确高效将所有配电网中的各个等级节点进行完整识别，导致评估结果不具有全面性。为此，构建了一种配电网便携式运维管控平台集群信息安全性评估模型。

1 平台集群信息安全性评估模块化分析

模块化是指从配电网便携式运维管控平台角度对集群信息进行分析，将其分解、合并，形成一个模块化的分析体系，然后通过模块化的方式将其信息集成到一个模块中[3]。为此，在安全性评估领域中，应用模块化分析方法能够进行统一安全风险评估。由此，设计的平台集群信息安全性评估模块化分析示意图，如图1所示。

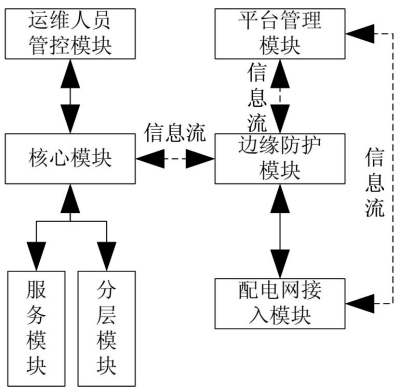


图1 平台集群信息安全性评估模块化分析示意图

由图1可知，该模块化分析主要是通过运维人员管控模块进行内部和外部信息流的风险评估，这样可以保证评估工作更加全面。

1.1 平台管理模块

该模块整合了各项技术指标，不断改进，加强管理，确保了配电网便携式运维管控平台的安全。安全的管理是系统安全的根本[4]。由于其动态特性，其危险性也很大。平台管理内容包括安全策略管理、组织安全管理、信息资产管理、非授权访问管理。通过对非授权访问管理，能够防止对平台集群信息的干扰，及时中断非正常访问行为[5]。

1.2 核心模块

该模块负责将信息流快速地从一个平台交换至另一个平台，为平台集群信息安全性评估提供数据库支持。通过构建保障交换架构，避免信息全部交换到一个平台现象的出现，为此，建立和维护评价系统和数据库是该模块研究的重点。

1.3 分层模块

该模块主要为路由、网络服务质量、访问控制服务等提供信息流，该信息流首先通过各个分层后再传送到核心模块，以此控制对信息的安全访问，防止未授权用户对平台的不安全访问。

1.4 服务模块

该模块包含了所有向用户提供的应用服务任务，主要负责评估用户访问的安全性。通过对平台脆弱性评估，能够及时发现平台本地漏洞，以此检查本地服务的可靠性。

1.5 边缘防护模块

该模块是配电网便携式运维管控平台的第一道防线，也是从信息接收到交换的最后一道防线，它可以保证数据的安全性，避免在交换过程中丢失和修改。

1.6 配电网接入模块

该模块是对集群信息进行全面分析的关键模块，可以对配电网的主动和被动安全进行审核，防止与不安全的外部网络进行直接的连接。

2 平台集群信息安全性评估模型构建

2.1 脆弱点识别与脆弱度计算

在配电网便携式运维管控平台中，易受攻击的节点对集群的信息造成了严重的破坏。攻击图是一种用于对网络缺陷进行评价的方法，对连接节点的薄弱环节进行了详细的分析[6-7]。攻击者可以从最小的节点出发，在多个弱点上进行多级的进攻。通过分析攻击图来评估节点的脆弱性，来设计有效攻击路径，步骤为：首先，分析了攻击模式。然后通过对各个节点进行分层，确定每个节点的最有效攻击路径，得出各个节点的脆弱部位，最后将其与其他节点的脆弱部位进行对比，进而确定脆弱节点数量和位置[8]。脆弱点识别的详细内容为：

配电网便携式运维管控平台中节点共分为n层，分别是L_1、L_2、…、L_n。从最后一层开始生成的攻击路径中，每条路径都存在一个最大深度。使用攻击图在每层攻击路径中确定一个覆盖节点，直到所有层的覆盖节点都被确定后，开始识别脆弱点。使用$\xi_n(i)$来表示节点被攻击后为上一层节点被攻击提供的有利条件，当$\xi_n(i)$为0时，则表示无法为上一层节点提供有利条件，该节点不是脆弱点，反之，则是。

节点的脆弱性由节点的规模决定，节点所拥有的论据节点数量就是节点的度[9]。由于各信息节点的数据交互能力以及网络的控制能力，仅依靠网络规模是远远不够的。所以，每一层都需具备一个拓扑矩阵，利用n个有向权的拓扑矩阵来描述节点的脆弱度，并给出n个有向权的拓扑矩阵[10]。对各层的节点进行了量化，并给出了不同节点之间的关系。将每一层节点中的度定义为与其直接联系所有节点与相邻节点总数目的比值，该值越大，说明

节点度就越大[11]。

基于此，第n层中第i个节点的脆弱度，可表示为：

$$\alpha(n)_i=\frac{m(n)_i}{r_i^2} \tag{1}$$

式中，$m(n)_i$表示邻居节点总数量；r_i表示所有节点与其相邻节点的总数量。

当配电网便携式运维管控平台中第一个节点的漏洞被利用后，下一个节点的攻击将会在下一个节点上进行有效的攻击，从而达到下一个节点的弱点，即完成了脆弱度的计算[12]。

2.2 基于层次结构的平台集群信息安全性评估指标确定

层次结构模型的建立实质上是对集群信息的分析、重构和评估。首先，将待解决的问题进行分解，根据相关程度进行聚类重组，构造出一种多层次的层次结构模式。其目的在于对各类安全事件进行分析，并针对其成因，采取相应的防范对策。最高级别的层级模式是专注于研究目标，鉴于平台中主要针对的是信息安全问题，所以把信息安全作为评估对象[13]。

由脆弱点识别与脆弱度计算结果可知，不同的信息安全风险评价取决于不同的威胁。为此，确定了基于层次结构的平台集群信息安全性评估指标体系，如图2所示。

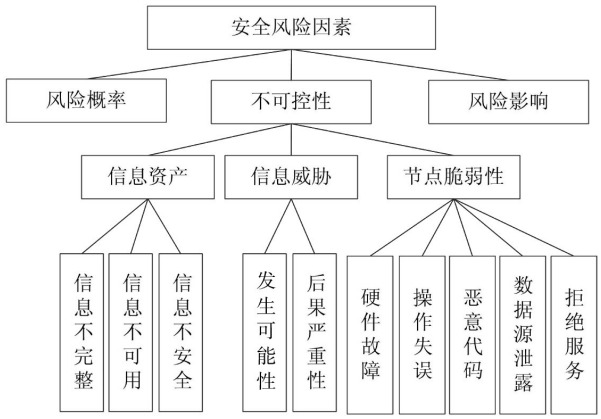


图2 基于层次结构的信息安全性评估指标体系

由图2可知，在充分考虑各风险因子的可控性的基础上，将风险概率、风险影响和不可控性作为评价指标，并将风险评价分为三级，即基于对集群信息的脆弱性进行分析。

2.2.1 目标层权重计算

在配电网便携式运维管控平台实际运行情况下，层次结构模型中的各个不安全元素比较客观清晰，因此，目标层权重计算依然采用层次分析法来进行[14]。以目标层的安全事件为基准，给出1−9标度的评价尺度，并构建判断矩阵，公式为：

$$E=\begin{bmatrix}\lambda_{11} & \lambda_{22} & \cdots & \lambda_{1n}\\ \lambda_{21} & \lambda_{22} & \cdots & \lambda_{2n}\\ \vdots & \vdots & \vdots & \vdots\\ \lambda_{n1} & \lambda_{n2} & \cdots & \lambda_{nm}\end{bmatrix} \tag{2}$$

式中，λ_{nm}表示该元素的重要程度，其取值是1−9之间的自然数。

通过式(2)，可以采用和积方法求出各单元的相对权值，然后经过标准化处理后，进行矩阵的一致性验证。当该值小于0.1时，判定矩阵的一致性可以被接受，反之，则需要修正[15]。

2.2.2 计算模糊评价结果

计算评价结果，公式为：

$$T=\omega^3\times E \tag{3}$$

式中，ω^{T}表示风险概率、风险影响和不可控性这三个二级指标的总权重值。

2.3 安全性评估数学模型构建

在确定的基于层次结构的平台集群信息安全性评估指标中，首先通过识别节点脆弱性及面临的威胁，了解目标安全因素，根据该因素评估集群信息的安全性。

平台集群信息安全性评估，可描述为：

$$O=f\left(x,y,z\right) \tag{4}$$

式中，x表示信息资产；y表示威胁；z表示脆弱性。

在集群的信息安全性评估过程中，一般采用矩阵和相乘法进行信息处理。集群信息安全性评估的风险取决于安全事件的发生概率，而节点的脆弱性则是造成网络安全事故的重要原因。

安全事件风险值的图形，如图3所示。

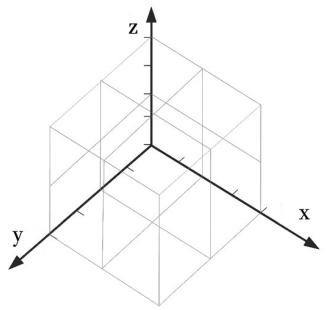


图3 安全事件风险值的图形

使用相乘法进行信息处理时，即图3安全事件风险值图形中的y轴和z轴，分别代表威胁出现的概率和节点脆弱程度。基于此，定义一个二元函数，可表示为：

$$\beta=y\otimes z \tag{5}$$

在配电网便携式运维管控平台中，使用相乘法获取的评估结果存在一定误差，为此，可将二元函数进行柔化处理，可表示为：

$$\beta=\sqrt{y\times z} \tag{6}$$

在信息交换过程中，出现的损失可表示为：

$$\gamma = \sqrt{x \times z} \tag{7}$$

基于此，得到的安全风险值为：

$$g = [\sqrt{y \times z} \times \sqrt{x \times z}] \tag{8}$$

为此，结合矩阵法来构建安全性评估数学模型，如下所示：

$$P = \sum_{i=1}^{n} \omega_i g = \sum_{i=1}^{n} \omega_i [\sqrt{y \times z} \times \sqrt{x \times z}] \tag{9}$$

根据式(9)的数学模型，划分信息安全性风险评估等级，如下所示：

(1) 当$P<2$时，风险等级非常低，平台集群信息是十分安全的；

(2) 当$2 \leqslant P<4$时，风险等级较低，平台集群信息较安全；

(3) 当$4 \leqslant P<6$时，风险等级适中，平台集群信息存在一定危险性；

(4) 当$6 \leqslant P<9$时，风险等级较高，平台集群信息不安全。

(5) 当$P>9$时，风险等级十分高，平台集群信息极不安全。

3 实验

3.1 实验环境

配电网便携式运维管控平台是配电自动化的核心，通过采集配电数据，实现对配电网周围运行环境的监视。该平台主要是由配电主站、终端、子站和通道组成的，如图4所示。

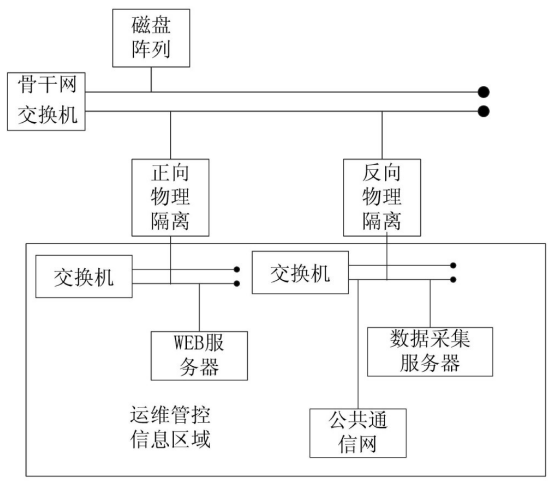


图4 实验平台结构示意图

由图4可知，通过采集相关实验参数，能够实现配电网数据的实时采集与监控，为实验结果分析提供数据支持。

3.2 实验结果与分析

3.2.1 脆弱点识别

对配电网便携式运维管控平台中脆弱点进行识别时，主要是对比不同地区不同用电时期的信息量对脆弱点识别的影响，将节点脆弱所造成的信息损失量作为脆弱点识别的评价指标。

分别使用基于D-AHP与灰色理论的信息安全风险评估方法(方法1)、基于二维结构熵的信息安全风险评估方法(方法2)和平台集群信息安全性评估模型，对比分析信息损失量，对比结果如图5所示。

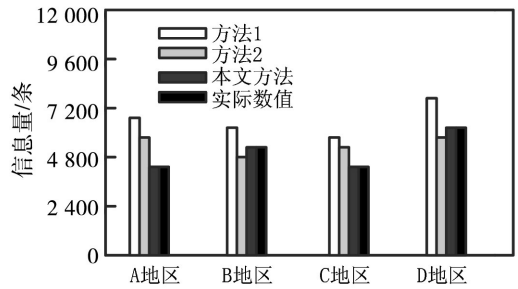


图5 三种方法信息损失量对比

由图5可知，使用方法1的信息安全风险评估方法，与实际数值相差最大，其中最大误差出现在A地区，数值为2 800条；使用方法2的信息安全风险评估方法，与实际数值相差较小，其中最大误差也出现在A地区，数值为1 700条；使用平台集群信息安全性评估模型，与实际数值无误差，基本一致。

由此可知，使用构建的平台集群信息安全性评估模型，统计的信息损失量与实际数值一致，说明脆弱点识别结果精准。

3.2.2 安全性评估

以数据缺乏保护被窃取、配置漏洞、系统漏洞、设备有意损坏、设备无意损坏指标，分别使用方法1的信息安全风险评估、方法2的信息安全风险评估方法和平台集群信息安全性评估模型，对比分析安全性评估结果，如图6所示。

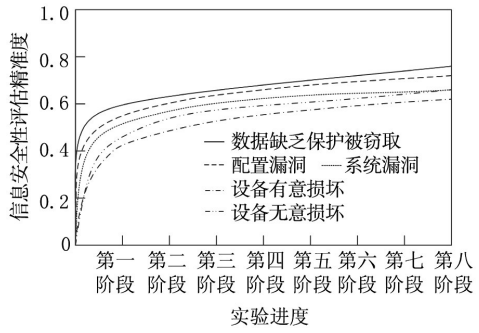
由图6(a)可知，使用该方法的5个指标评估精准度，随着实验进度的进行，始终低于0.8。其中设备有意损坏指标的安全性评估结果精准度最低为0.59，数据缺乏保护被窃取指标的安全性评估结果精准度最高为0.78。

由图6(b)可知，使用该方法对数据缺乏保护被窃取指标的安全性评估结果精准度最高，精准度数值为0.82；对设备有意损坏指标的安全性评估结果精准度最低，精准度数值为0.74。

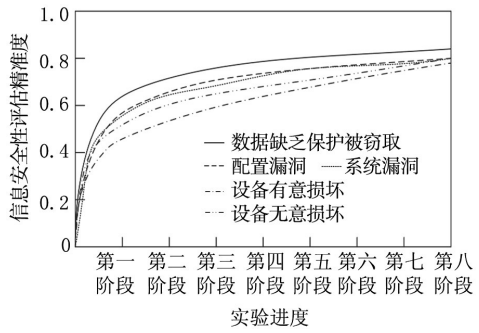
由图6(c)可知，使用该方法的5个指标评估精准度，随着实验进度的进行，均高于0.8，其中设备有意损坏指标的安全性评估结果精准度最高为0.99，设备有意损坏指标的安全性评估结果精准度最低为0.91。

通过上述对比结果可知，使用构建的平台集群信息

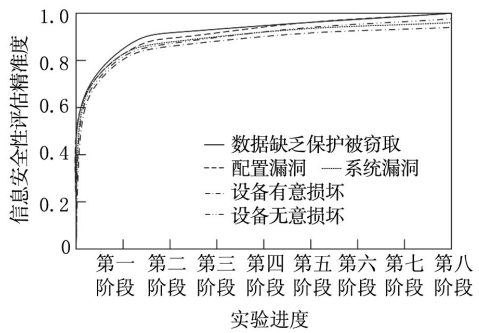
安全性评估模型，能够得到精准评估结果。



(a) 方法 1 的信息安全风险评估



(b) 方法 2 的信息安全风险评估方法



(c) 平台集群信息安全性评估模型

图 6 三种方法安全性评估结果对比

4 结束语

通过对平台集群信息安全性评估模块化分析，能够实现多个模块的同时评估，同时量化不同模块之间的关系。结合矩阵和相乘法构建的数学评估模型，能够保证评估结果的可靠性和准确性。设计的配电网便携式运维管控平台集群信息安全性评估模型，充分结合实际配电网环境进行了实验分析。但仍存在不足：在实际评估过程中，由于配电网环境的复杂性，仅靠技术评估容易造成疏忽。为此，需开发相应的评估软件，提高评估效率，增强评估过程的客观性。

参考文献：

[1] 许硕，唐作其，王鑫．基于 D-AHP 与灰色理论的信息安全风险评估[J]．计算机工程，2019，45(7)：194-202．

[2] 董慧宇，唐涛，王洪伟．基于二维结构熵的 CBTC 系统信息安全风险评估方法[J]．自动化学报，2019，45(1)：153-162．

[3] 罗新宇，段斌，吴俊锋，等．基于证据推理的风电场 SCADA 系统安全脆弱性定量评估方法[J]．电力系统自动化，2020，44(11)：25-31．

[4] 熊文泽，靳江红，唐军梅．SCADA 系统信息安全定量风险评估方法[J]．中国安全科学学报，2019，29(8)：157-163．

[5] 张帆，步兵，赵骏逸．列车运行控制系统信息安全风险评估方法[J]．中国安全科学学报，2020，30(S1)：172-178．

[6] 刘道远，孙科达，周君良，等．模糊综合评判法在电力企业网络信息安全评估中的应用[J]．电信科学，2020，36(3)：34-41．

[7] 段旭晨，彭道刚，姚峻，等．基于 SA-PSO-AHP 的火电厂控制系统信息安全威胁评估[J]．中国电力，2019，52(5)：29-35．

[8] 许钦百，王彩芬．基于密码学理论的私密信息安全风险评估方法[J]．科学技术与工程，2019，19(7)：172-176．

[9] 摆世彬，严明辉，徐伟，等．含大规模风电集群电网的在线计算数据生成技术[J]．电力系统保护与控制，2021，49(3)：66-73．

[10] 廖元媛，王剑，田开元，等．基于贝叶斯推理的铁路信号安全数据网信息安全动态风险评估[J]．铁道学报，2020，42(11)：84-93．

[11] 毛子骏，梅宏，肖一鸣，等．基于贝叶斯网络的智慧城市信息安全风险评估研究[J]．现代情报，2020，40(5)：19-26，40．

[12] 董坤祥，谢宗晓，甄杰，等．基于数据泄露类型的网络信息安全风险度量与可保性研究[J]．保险研究，2019(11)：25-41．

[13] 赵晓敏，赵影，李斯特，等．基于 MMC 的交直流混合配电网交流系统协调控制策略分析[J]．内蒙古电力技术，2021，39(5)：7．

[14] 王鑫，唐作其，许硕．基于模糊理论和 BRBPNN 的信息安全风险评估[J]．计算机仿真，2019，36(11)：184-189．

[15] 许钦百，王彩芬．基于密码学理论的私密信息安全风险评估方法[J]．科学技术与工程，2019，19(7)：172-176．

作者简介：杭海燕(1981—)，男，本科，工程师，研究方向：电力系统及其自动化。