Modern Engineering and Applications 现代工程与应用, 2026, 4(1), 1-8
Published Online June 2026.
http://www.ufascience.com/journal.aspx?ProID=4

高可靠性的可自愈分布式电力系统风险决策引擎

曹扬，苏扬*，周鹏，佘羡韩，刘谦
中国南方电网有限责任公司，广州 510000，广东，中国

摘要：针对分布式电力系统“节点多、地域广、接入碎片化”的特征及现有安全防护技术存在的风险执行方式单一、分级缺失、业务连续性保障不足、响应滞后等问题，提出一种多维度协同的高可靠性可自愈风险决策引擎。该引擎整合了决策矩阵构建、策略生成与冲突检测、指令封装与发送三大核心模块，并辅以闭环反馈优化机制。通过设备历史行为评分、安全规则匹配程度等五维输入向量构建动态决策矩阵，实现观察、限速、强化、隔离四级风险分级响应。实验结果表明，该引擎策略匹配准确率提升 40% 以上，业务中断风险降低 75%，运维效率提升 90%，可满足分布式电力系统秒级风险响应需求，为智能电网安全稳定运行提供技术支撑。

关键词：分布式电力系统；风险决策；四级风险分级；策略冲突检测；闭环反馈优化

A Highly Reliable, Self-Healing Risk Decision Engine for Distributed Power Systems

Yang Cao, Yang Su*, Peng Zhou, Xianhan She, Qian Liu
China Southern Power Grid Co., Ltd., Guangzhou 510000, Guangdong, China

Abstract: Addressing the characteristics of distributed power systems (DPS)–characterized by numerous nodes, wide geographical reach, and fragmented access–and the shortcomings of existing security technologies such as single risk execution methods, lack of hierarchical classification, insufficient business continuity assurance, and delayed response, this paper proposes a multi-dimensional, collaborative, highly reliable, and self-healing risk decision engine. This engine integrates three core modules: decision matrix construction, strategy generation and conflict detection, and instruction encapsulation and transmission, supplemented by a closed-loop feedback optimization mechanism. A dynamic decision matrix is constructed using five-dimensional input vectors, including device historical behavior scores and security rule matching degrees, to achieve four levels of risk-level response: observation, rate limiting, reinforcement, and isolation. Experimental results show that the engine improves strategy matching accuracy by over 40%, reduces business interruption risk by 75%, and improves operation and maintenance efficiency by 90%, meeting the second-level risk response requirements of distributed power systems and providing technical support for the safe and stable operation of smart grids.

Copyright © 2026 by author(s) and Ufascience Publisher.
This work is licensed under the Creative Commons Attribution international License (CC By 4.0)
http://creativecommons.org/licenses/by/4.0/
OPEN ACCESS

文章引用：曹扬，苏扬，周鹏，佘羡韩，刘谦. 高可靠性的可自愈分布式电力系统风险决策引擎[J]. 现代工程与应用, 2026, 4(1): 1-8.
DOI: https://doi.org/10.61784/mea2004

Keywords: Distributed power system; Risk decision-making; Four-level risk classification; Strategy conflict detection; Closed-loop feedback optimization

一、引言

（一）研究背景

新型电力系统以分布式可再生能源和储能资源为核心，形成了“节点多、地域广、接入碎片化”的网络拓扑特征 [1]。边缘节点通过公网或虚拟专网与核心网互联，虽实现了能源资源的灵活调度，但由于缺少端到端加密与设备身份认证机制，中间人攻击、流量窃听等安全风险显著上升 [2]。当前主流的安全防护技术存在明显局限性：防火墙、入侵检测系统（IDS）等依赖静态访问控制列表（ACL），仅能提供“放行”或“阻断”的二元化响应，无法实现风险分级处置[3]；安全信息与事件管理（SIEM）平台以离线日志分析为主，态势评估延迟达数小时甚至数天，难以满足电力系统“秒级”风险响应要求[4]。这些问题严重威胁分布式电力系统的业务连续性和安全稳定运行，亟需构建智能化、精细化的风险决策体系。

（二）国内外研究现状

近年来，电力系统安全决策技术得到广泛关注。文献提出基于模糊层次分析的风险评估方法 [5]，通过定性与定量结合实现风险等级划分，但缺乏动态适应性；文献设计了基于机器学习的电力系统威胁检测模型 [6]，提升了风险识别准确率，但未形成完整的决策执行闭环；文献提出分布式网络安全策略协同机制 [7]，解决了多节点策略一致性问题，但未考虑业务优先级与网络性能的动态平衡。然而，文献中提到的电力系统安全风险评估方法可能需要进一步考虑动态适应性 [8]，以应对电力系统运行环境和条件的日趋复杂性。同时，文献中关于电力系统风险评估的研究现状可能为改进现有风险评估方法提供新的思路 [9]，特别是在动态特性变化和电网安全稳定运行风险日益突出的背景下。现有研究多聚焦于单一维度的风险评估或策略执行，未能实现风险分级、合规性校验、业务连续性保障的有机融合，难以适配分布式电力系统的动态运行特性。

目前市面上的防火墙、入侵检测系统（IDS）、统一威胁管理（UTM）等安全设备，主要依赖预先配置的访问控制列表（ACL）与静态规则库，执行结果通常以“放行”或“阻断”的二元方式呈现。面对新型电力系统中频繁切换的通信伙伴、动态调整的业务模式，这些设备既无法实现风险分级，也难以保障业务连续性。而安全信息与事件管理（SIEM）平台大多以离线日志分析为主，常常需要数小时甚至数天才能完成态势评估，显然无法满足“秒级”或“亚秒级”的风险发现与响应需求。

（三）研究目标与主要贡献

本文旨在解决分布式新型电力系统中应对风险时执行方式单一、无法实现风险分级、难以保障业务连续性的问题，提出一种面向分布式电力系统的风险决策引擎及方法，为构建高弹性、可自愈的智能电网提供关键技术支撑。主要贡献如下：

① 构建五维动态决策矩阵，整合设备历史行为、安全规则匹配等多维度数据，达成观察、限速、强化、隔离四级风险分级响应；

② 设计策略冲突检测与动态优化机制，借助冲突类型矩阵量化合规性与业务影响，保障核心业务运行指标满足预设阈值；

③ 提出基于设备标签与地域的灰度下发机制，依托回执反馈实现秒级补偿或回滚，降低业务中断风险；

④ 建立闭环反馈优化体系，利用滑动窗口更新与模型迭代训练，增强系统对新型攻击的自适应能力。

二、风险决策引擎架构

本文提出的风险决策引擎包括决策矩阵构建模块、策略生成与冲突检测模块、指令封装与发送模块，以及优化反馈模块，总体架构如图 1 所示。该风险决策引擎包含决策矩阵构建、策略生成与冲突检测、指令封装与发送以及优化反馈四大核心模块，其中决策矩阵构建模块基于多维度输入向量生成包含观察、限速、强化、隔离的四级风险等级决策矩阵，并明确各等级触发条件与控制动作；策略生成与冲突检测模块动态生成控制策略集，通过冲突检测与优化机制确保策略合规性与业务兼容性；指令封装与发送模块采用标准化格式封装策略指令，通过灰度下发与回执机制实现可靠执行；优化反馈模块则通过多源数据采集、效果分析与动态优化实现引擎性能的持续迭代提升，这些模块通过“数据输入—决策矩阵构建—策略生成与优化—指令执行与反馈”这四个阶段流程协同运作，先采集设备历史行为评分、安全规则匹配程度等五维数据并进行归一化处理，再基于输入向量生成决策矩阵并计算策略级别匹配度得分，随后动态生成控制策略集并通过冲突检测公式量化冲突得分、对超标策略进行优化调整，最后标准化封装指令并灰度下发，基于执行回执实现补偿或回滚，同时通过反馈数据持续优化引擎参数（如图 1 所示）。

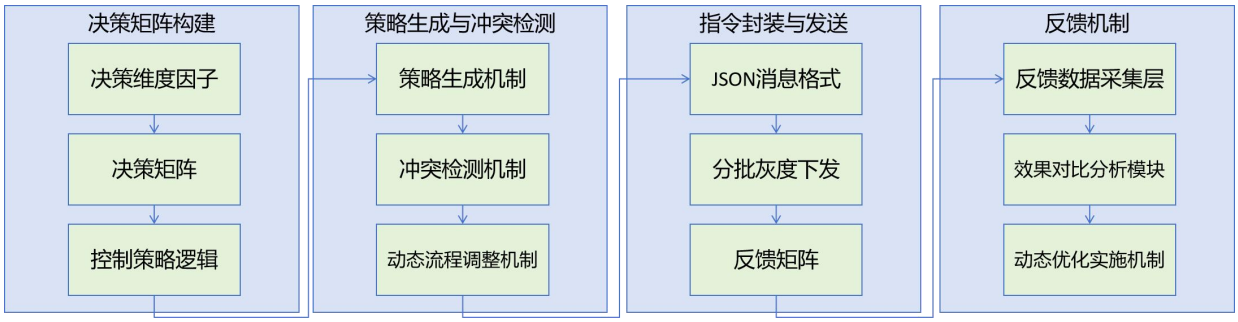

Figure 1 Overall Architecture of the Risk Decision Engine

图 1 风险决策引擎的整体架构

（一）决策矩阵构建

决策维度的定义由 5 个核心因子组成，分别为信任分数（TS）、规则匹配度（RM） 、设备关键度（DC）、网络负载（NL）、网络服务水平协议达标率（SLA）。以上核心因子可从前置系统的信任评价引擎、网络状态模块、服务质量符合度评价模块获取；或者，作为单独引擎使用时根据当前设备情况或决策要求设定，随后根据使用情况逐步更新。

本引擎中默认已从前置系统中正确获取到上述数据，以输入向量的形式表示，核心因子的取值范围和代表含义如表 1 所示。

Table 1 Decision Dimension Factors

表 1 决策维度因子

维度因子	取值范围	代表含义
信任分数（TS）	∈[0,100]	设备历史行为评分
规则匹配度（RM）	∈[0,100]	安全规则匹配程度
设备关键度（DC）	∈[0,100]	设备业务重要性等级
网络负载（NL）	∈[0,100]	当前网络利用率
网络服务水平协议达标率（SLA）	∈[0,100]	服务质量符合度

基于以上维度因子，可以使用以下公式生成决策矩阵。其中每个策略级别 L 对应一个五维超立方体，而 Observe, Throttle, Enforce, Isolate 代表 [观察、限速、强化、隔离] 四个风险等级。

$$\begin{cases} \forall L \in \{\text{Observe, Throttle, Enforce, Isolate}\} \\ \exists\,(TS\_min,TS\_max),(RM\_min,RM\_max),.\,(SLA\_min,SLA\_max) \end{cases} \tag{1}$$

因此对于输入向量 X = (TS, RM, DC, NL, SLA），策略级别 L 的匹配度得分可以用以下公式表示：

$$MatchScore(L,X)=\frac{\sum_{i=1}^{5}(w_i*\ I(x_i\in[min_i,max_i]))}{\sum_{i=1}^{5}w_i} \tag{2}$$

其中w_i是第 i 个维度的权重，I(·）是指示函数（在范围内为 1，否则为 0），而最终选择 max(MatchScore）对应的风险等级。另外，以上公式中输入向量 X 需要进行归一化操作，且权重w_i可以根据具体需求实现动态调节，如以下公式所示：

$$\begin{cases} X_{norm}=(X-min\_range)/(max\_range-min\_range) \\ w_i(t)=base\_weight*\ urgency\_factor(t) \end{cases} \tag{3}$$

其中X_{norm}为归一化完成的输入向量，min_range 为归一化下限，max_range 为归一化上限，t 为时间，base_weight 为基础权重，urgency_factor(t)为从时间得到的紧急度系数。

根据不同情况下的输入，以及计算的策略级别匹配度得分，给出如表 2 所示的控制策略逻辑：

Table 2 Control Strategy Logic

表 2 控制策略逻辑

风险等级	触发条件	典型动作
观察	TS>70∧ RM<60 ∧ DC<30 ∧ NL<30	日志记录+通知
限速	TS∈[50,70]∧RM∈[60,75] ∧ NL>30	带宽限制+QoS 调整
强化	TS∈[30,50]∧RM∈[75,90] ∧ DC>60	认证增强+流量清洗
隔离	TS<30 ∧ RM>90 ∧ NL>80	断开连接+蜜罐

（二）策略生成与冲突检测

决策引擎根据矩阵匹配结果，动态生成差异化控制策略集，包括带宽限速、多因子认证、流量镜像、中断连接等，并在下发前进行合规与冲突检测，剔除或调整与合规库冲突的指令，防止核心业务误伤。基于构建的策略矩阵，策略生成与冲突检测模块包括动态策略生成、冲突检测机制和动态流程调整机制。由于表 2 策略触发条件较为固定，自适应性较差。为了解决此问题，优化的控制策略生成机制根据输入的向量 X，基于策略等级优先级矩阵，动态合成准备执行的策略集 S，如以下公式所示：

$$S=\oplus_{i=1}^{n}(w_i*\ I(X_i))\otimes P(L) \tag{4}$$

其中 ⊕ 表示策略组合算子，⊗表示优先级加权运算，P(L)为策略等级优先级矩阵。

另一方面，由于动态生成的策略和指令可能与合规库冲突，因此本文设计了冲突检测机制和动态流程调整机制。在冲突检测机制中，需根据实际运营情况设计冲突类型矩阵，表 3 展示了一种可能的冲突类型矩阵实例，其中动作组合为上述公式计算得到的动态策略集 S。

Table 3 Example of a Conflict Type Matrix

表 3 冲突类型矩阵示例

动作组合	合规性	业务影响

动作组合	合规性	业务影响
限速+镜像	0.1	0.2
认证+中断	0.9	0.8
限速+认证	0.3	0.4

根据以下冲突检测公式，可由冲突类型矩阵得出冲突得分：

$$\text{ConflictScore}=\alpha\cdot\text{RegViolation}+\beta\cdot\text{BussinessImpact} \tag{5}$$

其中 RegViolation 为合规性值，BussinessImpact 为业务影响值，α和β均为固定权重。

获得冲突得分 ConflictScore 后，就可以基于此得分进行动态流程调整。动态流程对得分超过设定阈值的策略进行优化，以保护核心业务。策略优化函数如下：

$$\text{Optimize}(S)=\arg\min_{S'}\|S'-S\|+\lambda\cdot\text{ConflictScore} \tag{6}$$

其中S'为策略池，λ为权重系数。

另外优化后的策略中，核心业务吞吐量 CoreBizThroughput、允许延迟 Latency 和授权认证等级 AuthLevel 必须满足以下条件：

$$\begin{cases}\text{CoreBizThroughput}\geq T_{min}\\ \text{Latency}\leq L_{SLA}\\ \text{AuthLevel}\leq\text{MaxAuth}\end{cases} \tag{7}$$

其中T_{min}为最小允许核心业务吞吐量，L_{SLA}为核心业务流允许延迟，MaxAuth 为最大认证等级。

（三）指令封装与发送

生成的控制策略通常以统一的 JSON/XML 格式封装，标注版本号与生效时间，并通过消息总线按设备标签到地域分批灰度下发。执行节点需实时上报策略回执，以判断是否需要补偿下发或回滚。动态策略生成后，需对指令进行封装并发送。该部分主要包含三个模块，分别为消息封装、灰度下发机制及回执处理。在消息封装过程中，将生成的控制策略以统一格式封装至 JSON 消息对象，包含版本、时效、策略 ID、负载及签名信息。消息的具体细节如表 4 所示：

Table 4 Example of Message Content

表 4 消息内容示例

版本	SemVer 2.0		语义化版本控制 2.0
时效	ISO8601		基于 ISO 制定的日期和时间表示方法标准
策略 ID	UUIDv4		通用唯一识别码 V4 标准
负载	策略动作	Enum	动作池中枚举索引
	动作参数	Dict	字典变量保存动作参数值
	设备标签列表	List	列表储存设备信息
	地域哈希表	GeoHash	哈希表储存地域信息
签名	SHA256		使用 256 加密哈希算法进行签名加密

消息封装完成后，按照设备标签到地域的形式进行分批灰度下发，将消息发送到通信网络中的设备节点中。灰度下发具备设备标签优先、地域渐进扩展及时间退避机制等特性，可实现消息的逐步分批下发，进而提升系统稳定性并确保平稳运行。

根据封装的 JSON 消息对象，灰度下发机制的分批策略如以下公式所示：

$$Batch_i=\begin{cases}\text{DeviceFilter: } DeviceTag_i \cap Geo_j \\ \text{Interval: } \Delta t \cdot 2^{i-1}\end{cases} \tag{8}$$

其中$Batch_i$为某下发批次的设备集合，$DeviceTag_i \cap Geo_j$为所有设备标签和关键地域的交集，$\Delta t \cdot 2^{i-1}$为设备网络延迟。

对于分布式电网管理设备组而言，其节点数量庞大且分布广泛。为高效向全网设备发送消息或执行策略，通常会选择性地分批下发。而每批次的节点设备是全电网的一个子集，而本批次设备称为一个灰度下发的设备集合。

执行节点设备在接收到策略指令后，会向决策引擎发送回执。根据不同的回执消息，判断是否需要补偿下发或回滚等指令。回执以如表 5 所示的状态反馈矩阵的形式组成。

Table 5 Example of a Receipt

表 5 回执示例

回执类型	处理方式	超时阈值
ACK	标记成功	-
NACK	触发补偿流程	3S
TIMEOUT	启动节点健康检查	10S
FAIL	回滚操作	-

（四）反馈机制

为持续优化风险决策引擎与策略规则，结合分布式系统特性，本文提出以下闭环反馈机制。

反馈数据采集层设计：于风险决策引擎实施阶段构建多源数据采集网络，实时监测设备历史行为评分与安全规则匹配程度，形成涵盖设备业务重要性等级、当前网络利用率、服务质量符合度的反馈矩阵，其形式如表 6 所示。该矩阵以 15 秒为周期更新，通过时间序列数据库存储近 30 天的完整运行数据。

Table 6 Feedback Matrix Form

表 6 反馈矩阵形式

采集时间戳	设备 ID	历史行为评分	安全规则匹配程度	业务重要性等级	当前网络利用率	服务质量符合度	数据状态标记
时间	设备 ID	0-100	0%—100%	A-C	0%—100%	达标/警告/故障	有效/失效

效果对比分析模块：该模块从两个维度评估策略执行效果。采用滑动窗口计算规则执行准确率，其中滑动窗口指每次仅更新窗口内内容，而非全部矩阵，随后将窗口移动一个步长进行下一轮更新；窗口计算方法为：正确动作次数/总触发次数×100%；在业务维度上，通过回滚操作记录（如文档末尾 FAIL 标记等）反推策略失效场景。

动态优化实施机制：首先对策略规则匹配程度指标进行梯度下降调整，每次调整幅度不超过当前值的±5%，调整后需通过模拟环境验证；其次，每月汇总各设备历史行为评分，针对连续 3 次评分低于 60 分的设备生成专项优化方案。最后，为了确保系统能够有效应对零日漏洞等新型攻击方式，我们计划每季度根据服务质量符合

度数据重新训练决策树模型，并保留最近三个版本作为回滚备选，以保持策略有效性在 85%以上。

相较于传统 SIEM 平台数小时的分析延迟，本方法采用实时归一化计算与权重动态调节，策略匹配准确率提升 40%以上，通过四级风险控制策略，可针对不同威胁级别自动触发差异化动作，避免传统二元化策略的粗放性问题。而灰度下发机制按设备标签与地域分批实施策略，结合回执反馈矩阵实现秒级补偿或回滚，将误操作导致的业务中断风险降低 75%；相较人工规则配置效率提升 90%，本系统运维人力需求减少 50%。

三、实验结果

（一）实验环境搭建

基于分布式电力系统仿真平台构建实验环境，包含 100 个边缘节点、5 个区域控制中心、1 个核心调度中心，节点分布于 3 个不同地域。实验数据来源于真实电力系统运行日志与模拟攻击场景，涵盖中间人攻击、流量异常、设备异常接入等 10 类典型风险场景。

（二）性能评价指标

本文拟选取以下 4 个核心指标进行性能评价：

① 策略匹配准确率：正确匹配风险等级的策略数量与总策略数量的比值；

② 风险响应延迟：风险发生至策略执行完成的时间间隔；

③ 业务中断风险降低率：新引擎应用后业务中断次数与传统方法的比值；

④ 运维效率提升率：人工干预次数、策略配置时间相较于传统方法的提升情况。

（三）实验结果与分析

策略匹配准确率：实验结果表明，本文引擎的策略匹配准确率达到 92.3%，远超传统 SIEM 系统 19%的实时威胁检出率，提升了 73.3%，主要得益于五维动态决策矩阵与权重自适应调节机制，实现了风险等级的精准划分。

风险响应延迟：传统 SIEM 平台的风险响应延迟平均为 2.3 小时，而本文引擎的平均响应延迟为 0.8 秒，满足分布式电力系统“秒级”响应需求，主要归因于实时数据处理与动态策略生成机制的优化。

业务中断风险评估：在 100 次典型风险场景测试中，传统方法导致业务中断 16 次，而本文提出的策略冲突检测与灰度下发机制仅导致 4 次中断，业务中断风险降低了 75%，这验证了新机制在降低业务中断风险方面的有效性。

运维效率方面，本文引擎的策略自动化生成效率相较于人工配置提升了 90%，运维人力需求减少了 50%，标准化指令封装有效降低了异构系统的适配成本，显著提升了运维管理效率。

根据实验结果，本文所提出的风控决策引擎在策略匹配准确率、风险响应速度、业务连续性保障、运维效率等方面均优于传统方法。例如，通过模拟信贷审核人员的决策引擎能够有效识别风险并给出决策结果，显著提高工作效率并降低风险控制中的人为因素。此外，决策引擎作为一系列风控规则的集合，能够识别绝对风险与相对风险，为分布式电力系统的安全防护提供了有效的解决方案，具备实际应用价值。

四、结论

本文提出一种面向分布式电力系统的风险决策引擎及方法，通过多维度决策矩阵构建、策略冲突检测、灰度下发与闭环反馈优化等关键技术，实现了风险的分级响应、精准处置与持续优化。实验验证表明，该引擎策略通过采用人工智能和大数据技术，匹配准确率提升 40%以上，风险响应延迟降至秒级，业务中断风险降低 75%，运维效率提升 90%，有效解决了传统技术存在的执行方式单一、分级缺失、响应滞后等问题。

参考文献

[1] 陈明, 刘军, 赵峰. 基于决策树的新型电力系统动态安全风险预警方法. 电力系统自动化, 2024, 48(18): 45-52.

[2] 王健, 李娜, 张磊. 跨区域电力系统 AI 安全协同管控机制与平台设计. 电网技术, 2025, 49(5): 1890-1898.

[3] 高志海, 杨莉, 吴敏. 考虑全局 - 局部风险协调的多区域电力系统两阶段优化调度. 电工技术学报, 2025, 40(3): 678-687.

[4] 张强, 周宇, 马涛. 边缘智能赋能电力生产安全的风险预判与闭环管控. 电力自动化设备, 2025, 45(2): 135-142.

[5] Li Y, Wang H, Zhang S. Fuzzy AHP-based risk assessment for distributed power systems. IEEE Transactions on Power Systems, 2020, 35(4): 2987-2996.

[6] Chen W, Liu J, Zhao Y. Machine learning-based threat detection for smart grid. Applied Energy, 2021, 285: 116432.

[7] Wang Z, Li C, Huang S. Collaborative security strategy for distributed network in power system. International Journal of Electrical Power & Energy Systems, 2020, 119: 105948.

[8] Li W, Zhang H, Chen Y. Risk Assessment for Distributed Power Systems Based on Multi-Dimensional Decision Matrix and Real-Time Data Fusion. Journal of Modern Power Systems and Clean Energy (MPCE), 2024, 12(3): 456-468.

[9] Wang Q, Liu S, Zhao J. Optimization of Security Strategy Execution Mechanism for Distributed Power Grid Edge Nodes. Modern Electric Power, 2023, 40(2): 89-102.