

基于系统安全工程理论的某电力建设集团企业 双重预防机制研究

丛志明

中国电力工程顾问集团有限公司安质环部/安全管理处, 北京

收稿日期: 2026年8月10日; 录用日期: 2026年9月1日; 发布日期: 2026年9月11日

摘 要

本研究结合系统安全工程理论, 为电力建设集团构建了适配的双重预防机制, 明确跨层级、全专业、国内外的系统边界, 基于危险三要素辨识危险源, 运用LEC法完成风险量化评价与分级管控, 界定隐患为风险控制措施失效, 搭建“辨识-评价-管控-排查治理”全流程体系, 并通过信息化建设实现机制数字化落地。该机制破解了传统安全管理的痛点, 实现传统与新型风险一体化管控, 提升了电力建设安全管理的科学性与有效性, 为新能源电力产业安全发展、助力“双碳”目标落地筑牢安全屏障, 后续需结合行业发展持续动态优化机制。

关键词

系统安全工程, 电力建设, 风险分级管控, 隐患排查治理

Research on the Dual-Prevention Mechanism of a Power Construction Group Enterprise Based on System Safety Engineering Theory

Zhiming Cong

Department of Safety, Quality, Environment and Health/Safety Management Office, China Power Engineering Consulting Group Co., Ltd., Beijing

Received: August 10, 2026; accepted: September 1, 2026; published: September 11, 2026

Abstract

Combined with system safety engineering theory, this study constructs a tailored dual-prevention

文章引用: 丛志明. 基于系统安全工程理论的某电力建设集团企业双重预防机制研究[J]. 管理科学与工程, 2026, 15(5): 1013-1021. DOI: 10.12677/mse.2026.155098

mechanism for power construction groups. It defines the system boundaries covering multi-level organizations, full-range specialties, and domestic-overseas business scope. Hazard identification is carried out based on the three-element hazard theory, and the LEC method is adopted for quantitative risk assessment and hierarchical risk control. This study defines hidden dangers as failures of risk-control measures, and establishes a full-process system of “identification-assessment-control-investigation and rectification”. Digital implementation of the mechanism is realized via information-based construction. The proposed mechanism addresses pain points of conventional safety management, enables integrated management of traditional and emerging risks, and improves the scientificity and effectiveness of safety management for power construction. It builds a solid safety barrier for the safe development of the new-energy power industry and supports the achievement of the “Dual-Carbon” goals. Continuous dynamic optimization of the mechanism shall be performed in accordance with industrial development in follow-up work.

Keywords

System Safety Engineering, Power Construction, Hierarchical Risk Control, Hazard Investigation and Rectification

Copyright © 2026 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 引言

我国明确提出“2030 年前碳达峰、2060 年前碳中和”的发展目标，该目标已成为引领能源结构转型、推动生态文明建设的核心导向¹。在此指引下，新能源电力建设领域迎来爆发式发展机遇，业务扩张的同时也使得安全管理的复杂性与管控压力同步激增，2025 年，电力建设领域事故呈现事故起数、死亡人数双增长趋势，安全管理水平已成为制约新能源电力产业持续健康发展的关键瓶颈。

对于大型集团化电力企业而言，其自身管理体系具有层级多元、业务覆盖面广、项目地域分布分散等典型特征，传统安全管理模式以“事后被动处置、粗放式监管”为主，缺乏对全流程、全要素的系统性管控，难以全面、精准识别新能源电力建设及运营过程中的各类危险有害因素，无法实现风险的事前预防与事中管控，更难以适应新技术、新业务、新领域拓展带来的新型安全风险挑战，进一步加剧了安全管理的难度，因此急需构建科学、系统、高效的安全管控机制，建立健全适配产业发展特点、契合集团化管理模式的安全管控体系，实现对各类风险的精准识别、分级管控与动态预警，为“双碳”目标的如期实现筑牢安全保障。

2. 系统安全工程

2.1. 系统安全工程内涵与发展

系统安全工程是以工程设计理论、安全科学原理及系统分析方法为核心基础，通过系统性的分析、预测与评价，识别系统潜在风险、优化安全设计，进而保障系统全生命周期安全性的综合性工程技术[1]。该技术体系的形成源于实际工业生产中的安全需求，早在 20 世纪 60 年代，美国航空航天领域因导弹武器研发过程中连续发生重大安全事故，相关部门逐步出台一系列系统安全相关标准与规范，标志着系统安全工程正式形成并应用于实践。随着技术的不断成熟，系统安全工程的应用范围逐步拓展至核工业、化学工业、机械制造等多个高危及复杂工业领域，成为保障工业系统安全稳定运行的核心技术支撑。

¹https://www.gov.cn/gongbao/content/2021/content_5649728.htm

系统安全主要包括系统安全工程和系统安全管理两个方面。系统安全工程的核心在于运用理学和工程的原理、标准、及技术，对危险进行辨识与风险评价，并通过采取相应的措施消除危险，或在危险无法完全消除的情况下，有效降低这些危险引发的风险。系统安全管理是指系统、子系统、设备和基础设施的设计、开发、测试、采购、使用和报废过程中，为识别风险、评估和缓解相关风险，以及跟踪、控制、接受和记录所涉及的风险而采取的所有计划和行动[2]。系统安全工作流程如图 1 所示。

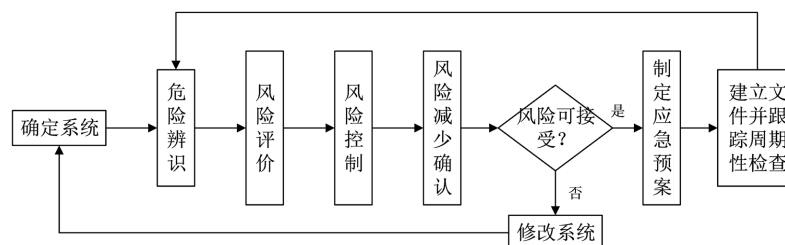


Figure 1. Flow chart of system safety
图 1. 系统安全流程图

我国对系统安全工程的研究与应用始于 20 世纪 70 年代，此后众多学者围绕系统安全分析与评价技术开展了大量基础性与应用性研究[3]。由于生产系统的工艺特性、作业环境的复杂程度及研究对象的差异化，学者们在实践探索中逐步提出了数十种针对性的系统安全分析与评价技术方法，如系统安全检查表(SCL)、故障危险分析法(FHA)等[4]。这些分析方法的评价对象全面覆盖人员素质、安全管理状况、生产设施可靠性、作业环境安全性等系统安全核心要素，能够实现对各类潜在危险有害因素的全面识别与科学评价[3]。大量工程实践表明，系统安全分析与评价技术作为系统安全工程的核心组成部分，是实现系统全生命周期安全管控、降低安全事故发生率的重要手段，为各类工业系统的安全稳定运行提供了有力保障。

2.2. 其他安全管理理论

当前主流安全管理理论体系中，韧性工程(Resilience Engineering)与 Safety-II理论在复杂系统安全领域受到广泛关注。韧性工程以复杂系统视角为核心，认为安全并非系统的静态属性，而是系统在面对预期内扰动与非预期冲击时，通过动态调整自身功能、结构与运行模式，持续维持核心目标的能力[5]。该理论突破了传统“故障导向”的安全管理局限，但缺乏标准化的危险辨识工具、量化评价方法与分级管控流程，难以直接支撑多层次集团企业的标准化、可复制安全管控体系构建。Safety-II理论由安全学者霍尔奈格尔提出，将传统聚焦“事故为何发生、如何消除失效”的安全管理范式定义为 Safety-I，而 Safety-II则转向关注“工作为何成功、如何提升正向绩效”[6]，该理论拓展了安全管理的研究边界，但对于电力建设这类高风险、强监管、事故后果不可逆的行业，失效防控仍是安全管理的底线核心，仅依靠正向绩效提升无法满足合规性管控与风险精准防控的刚性要求。

因此，对于层级多元、业务广泛、合规要求严苛的电力建设大型集团而言，构建双重预防机制的核心需求是建立一套可落地、可量化、可追溯的标准化管控体系。系统安全工程理论既能够精准匹配这一核心需求，也为后续融合前沿安全管理理念预留了升级空间，因此是本研究构建双重预防机制的最优理论基础。

3. 双重预防机制

双重预防机制全称为“安全风险分级管控和隐患排查治理双重预防机制”，是植根于风险预控理论与系统安全工程思想的现代化安全管理体系，其核心要义在于通过“风险分级管控”与“隐患排查治理”两个相互关联、层层递进的关键环节，构建安全风险的全流程闭环管控体系。该机制以风险管控为

前端防线，以隐患治理为后端兜底，通过两大环节的协同联动，实现对安全风险从源头预判到末端治理的全链条管控，体现了系统安全工程“事前预控、事中管控、事后闭环”的核心思想。

我国双重预防机制的政策体系经历了“战略提出 - 配套完善 - 法律固化”的渐进式构建过程。2016年，《中共中央 国务院关于推进安全生产领域改革发展的意见》首次从国家战略层面明确提出“构建安全风险分级管控和隐患排查治理双重预防机制”的要求[7]，标志着该机制正式成为我国安全生产治理的核心制度导向；此后，应急管理部相继印发《关于实施遏制重特事故工作指南构建双重预防机制的意见》等配套文件[8]，从制度设计、技术标准、实施路径、责任划分等维度进行细化，为双重预防机制在企业层面的落地提供了可操作的指导框架；2021年新修订的《中华人民共和国安全生产法》²正式将双重预防机制构建纳入法律规范，明确要求生产经营单位建立并落实该机制，完成了双重预防机制从政策要求到法律义务的制度升级。

在电力建设领域，双重预防机制的适配性与扩展性进一步凸显[2]。针对风电、光伏、储能等新能源项目地域分布分散、施工环境复杂、新技术应用密集、新型风险突出的特点，双重预防机制通过整合传统风险管控经验与新型风险识别技术，构建“传统风险与新型风险一体化管控”的安全管理模式，为电力产业在快速扩张过程中筑牢安全屏障。

4. 构建电力建设集团企业双重预防机制

4.1. 系统确定

双重预防机制旨在对系统内的全要素、全范围、全生命周期的危险进行辨识与控制，以保证系统安全。组织机构方面，电力建设集团实施多层级管理，系统包括一级企业、二级企业、三级企业，以及部分企业派生的独立法人的日常生产经营活动，还包括企业开展电力建设活动的项目管理组织机构。专业方面，系统涵盖投资、设计、施工、监理、运维等过程。地域范围方面，系统包括国内、国外所有涉及地区。系统各要素详见表 1。

Table 1. Table of system elements
表 1. 系统要素表

序号	方面	系统要素
1	组织机构	一级企业、二级企业、三级企业、派生独立法人、项目部
2	专业	投资、设计、施工、监理、运维
3	地域	国内、国外

4.2. 危险辨识

危险辨识的目的是为了对其进行控制，以防止事故发生，危险理论认为危险是由导致事故的充分、必要要素组成的实体，通常包括危险源、触发机理和威胁目标和结果三个要素[9]。樊运晓等认为只有基于危险三要素的辨识才能准确描述危险场景或情景，继而提出实用可靠的危险控制措施[10]。因此，在危险辨识过程中除了要识别出具有一定能量的危险源，还要结合具体工作场景，以及监管背景，对危险触发机理和威胁目标进行描述。危险辨识清单如表 2 所示。为便于管理，可对危险源进行分类，《生产过程危险和有害因素分类》³从人、物、环、管四个方面进行分类，结合生产实际，也可按照作业活动单元、

²<https://flk.npc.gov.cn/detail?id=ff8081817a66b816017a7956b7db0ad4&fileId=&type=&title=%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E5%AE%89%E5%85%A8%E7%94%9F%E4%BA%A7%E6%B3%95>

³<https://openstd.samr.gov.cn/bzgk/std/newGbInfo?hcno=BCBA1F97621C11B4B5A6C10783C93DB1>

系统生命周期、专业类型、组织机构等进行划分。

Table 2. Hazard identification list

表 2. 危险辨识清单

序号	危险源	触发机理	威胁目标
1			
2			
⋮			

4.3. 风险评价与控制

风险评价是对危险程度进行定性、定量或半定性半定量描述的过程，即当危险辨识出来无法消除时，需要对危险程度进行评价，判定对人员、社会、环境、财产等是否在可接受范围。基于风险概念，风险评价一般是通过判定系统中危险演变为事故的后果等级和发生概率(可能性)等级并采用风险矩阵的方法确定风险的等级，其中发生概率(可能性)往往还包括威胁目标暴露危险环境的频率。Graham 和 Kinney 在开展系统安全危险性分析时，基于统计的研究方法得出半量化评价方法，后演化为 LEC 法^{[11] [12]}。LEC 法先进在于得出风险的量化指标，并提出风险分级标准，为风险分级管理提供了理论依据。对危险进行风险评价得出表 3。

Table 3. Risk assessment table

表 3. 风险评价表

危险源辨识				风险评价				
序号	危险源	触发机理	威胁目标	L(可能性)	E(暴露频率)	C(严重度)	风险值	风险等级
1								
2								
⋮								

Table 4. Risk control table

表 4. 风险控制表

序号	危险源辨识			风险评价			风险控制		风险值
	危险源	触发机理	威胁目标	L(可能性)	E(暴露频率)	C(严重度)			
1									
2									
⋮									

当风险值高于可接受程度时，往往需要对风险进行控制，进而降低风险值至可接受范围内(安全)。采取控制措施对风险值进行降低的过程叫做风险控制，基于危险理论和能量流 - 屏障分析方法，风险控制可从三要素之间设置屏障，进而阻止伤害的发生，以降低风险值。风险控制并非无限度降低风险值为好，还需考虑措施的有效性、适用性、投入成本，同时，还需再一次进行风险评级，以确认风险值是否降低或增加新的危险。风险控制详见表 4。

4.4. 隐患排查与治理

在《安全生产事故隐患排查治理暂行规定》⁴中明确隐患是指违反安全生产法律、法规、规章、标准、

⁴https://www.mem.gov.cn/gk/zfxzgkpt/fdzdgknr/gz11/200712/t20071228_405675.shtml

规程和安全生产管理制度的规定，或者因其他因素在生产经营活动中存在可能导致事故发生的物的危险状态、人的不安全行为和管理上的缺陷，当前征求意见稿中删除了“违反安全生产法律、法规、规章、标准、规程和安全生产管理制度的规定”。按照系统安全工程理论，隐患是指危险控制措施的失效，或为识别危险、评估和缓解相关风险，以及跟踪、控制、接受和记录所涉及风险而采取的所有计划和行动出现了一个或多个缺陷。简言之，隐患就是危险失去了控制，意外能量可以作用于威胁目标，事故可能会发生。

借鉴危险检查表法，可参考形成隐患排查表(表 5)，对系统安全工程整个流程进行隐患排查。排查出的隐患一般可根据整改难易程度分为一般隐患和重大隐患，当前各行业主管部门已发布重大事故隐患判定标准。

Table 5. Hidden danger investigation table
表 5. 隐患排查表

阶段	规定动作	是否存在隐患	隐患描述	隐患等级	整改要求
危险源辨识					
风险评价					
风险控制					
档案管理					
⋮					

4.5. 信息化建设

综上所述，基于系统安全工程理论的双重预防机制建设，从危险辨识出发，利用风险评价，判定危险性程度，结合危险三要素制定针对性控制措施，对风险进行控制，从而实现整个系统安全。可利用信息化手段，建立双重预防机制信息化流程。

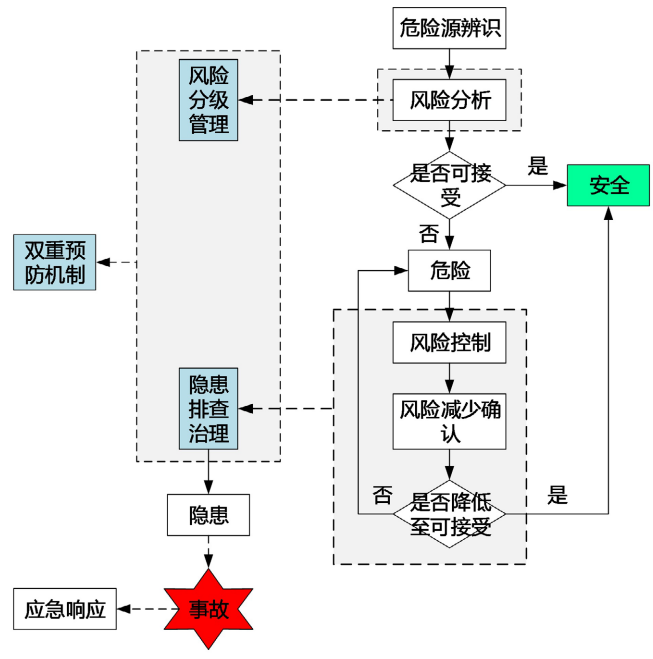


Figure 2. Flow chart for informatization construction of the dual-prevention mechanism
图 2. 双重预防机制信息化建设流程图

主要分为几个模块：危险源辨识模块，充分全面辨识整个系统全生命周期可能存在的危险源，并从危险三要素进行描述；风险评价模块，针对危险源从可能性、严重度、暴露频率三个维度开展风险评价，结合企业实际情况划定风险阈值，实现风险分级管控；隐患排查治理模块，由于整个流程环节是在系统中进行，不存在规定动作未执行，因此隐患排查治理仅需对风险控制措施的有效性进行核实即可。信息化建设流程图见图2。

5. 实践应用

基于上述双重预防机制建设路径，对某大型电力集团公司建立了双重预防机制，开展风险分级管控和隐患排查治理工作(见图3和图4)。

安全风险分级管控方面，全层级梳理火电、风电、光伏、输变电、市政、房建、电力运行等行业领域，起重吊装安装、脚手架(高支模)、深基坑、高处作业、吊篮作业、动火作业、受限空间、爆破作业、运维检修等作业类型，一级、二级、三级等风险等级开展全流程风险辨识与管控，全年辨识各类管控风险9394项，其中火电类风险占比49%，起重吊装安装类风险占比24%。综合行业领域与作业类型的风险分布，安全风险呈现两大核心特征：业务集中性：一是火电业务为风险核心，占比接近总风险的一半，新能源及输变电业务风险次之，与集团业务结构及火电行业固有风险特征高度相关；二是作业环节集中性：起重吊装、脚手架、深基坑、高处作业等施工类高风险作业占比合计达65%，是施工阶段安全管控的关键环节。

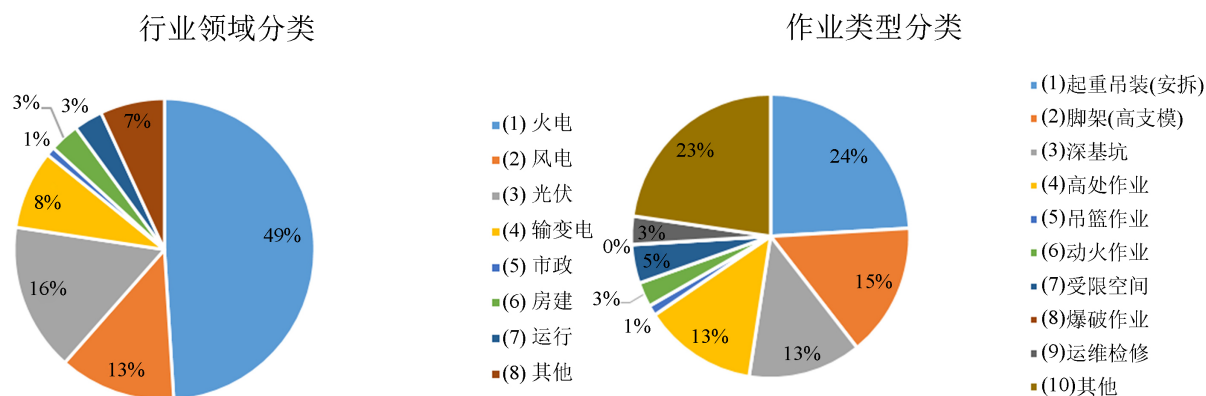


Figure 3. Statistical analysis chart of risks

图3. 风险统计分析图

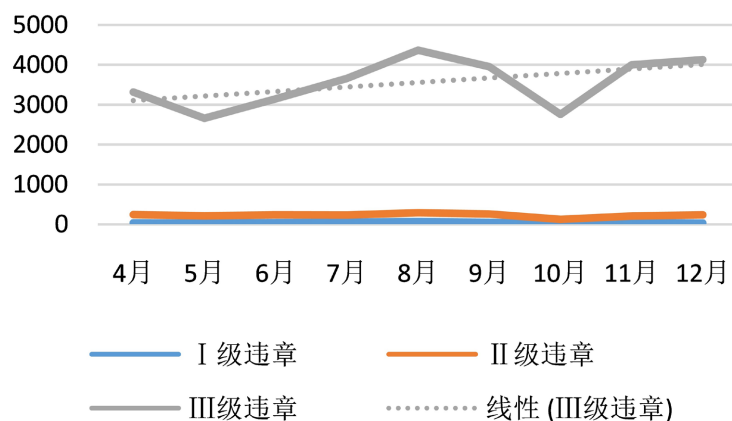


Figure 4. Statistical analysis chart of hidden dangers

图4. 隐患统计分析图

隐患排查治理方面,依据《重大事故隐患判定标准》及相关标准规范,构建了以隐患严重性为核心的三级违章分级体系,并配套建立了“排查-上报-整改-验收-销号”的闭环治理流程,共发现问题隐患 34,453 项。从隐患等级的数量分布来看,三类隐患的构成差异显著,呈现出“金字塔型”结构,三级违章占比超 90%,月均数量约 3500 项,反映出基层作业环节的合规性管理仍存在薄弱环节;从隐患数量的时间分布来看,呈现出“阶段性波动、整体趋稳、长期微增”的特征,隐患分布与业务节奏高度耦合,一般隐患数量的季节性波动与施工进度、作业量直接相关,施工旺季(7~9 月)为隐患管控的关键时段。

6. 讨论分析

基于上述实践结果,从风险行业分布来看,火电业务风险占比达 49%,核心驱动因素有三点:一是火力发电“三个 8000 万”国家政策背景下,火电业务增速较快,风险随之增加。而新能源项目受 136 号文影响,业务量迅速缩减,风险相对减少;二是固有风险属性差异,火电建设涉及锅炉、汽机、电气等复杂工艺系统,包含大量高温高压作业、重型设备吊装、多工序交叉作业场景,单项目风险密度显著高于风电、光伏等新能源项目;三是管理耦合复杂度差异,火电项目参建单位多、专业分工细、工序衔接紧密,多主体协同带来的管理交叉风险进一步推高了风险总量。新能源项目虽地域分散、野外作业环境复杂,但单体项目工序相对单一、设备集成度高,风险总量仍低于火电业务。从隐患分布特征来看,“金字塔型”的违章等级结构完全契合海因里希事故法则的规律,大量轻微违章是事故发生的基础,反映出基层作业行为合规性、现场日常管理精细化仍是安全管理的薄弱基本面。而隐患数量的季节性波动特征,则印证了安全管理与生产节奏的强耦合关系:7~9 月施工旺季作业量饱和、人员劳动强度提升,叠加夏季高温、多雨等恶劣作业环境,既增加了违章行为的发生概率,也稀释了现场安全管理资源,导致隐患数量显著上升,这一规律为企业动态调配安全资源提供了明确的数据依据。

本研究将隐患界定为“风险控制措施的失效”,并非简单的概念定义调整,而是打通了风险分级管控与隐患排查治理的内在逻辑,构建了“危险源→风险评价→设置控制屏障→屏障失效→形成隐患→诱发事故”的完整逻辑链条,其理论意义与管理价值集中体现在责任界定与资源分配两个核心维度。

在安全责任界定层面,传统隐患治理常出现“权责模糊、追责泛化”的问题,根源在于隐患与风险管控环节脱节,无法追溯隐患产生的源头。以“控制措施失效”为核心判定标准,能够实现隐患责任的精准追溯:风险控制措施的设计、制定责任归属业务管理部门,若因措施设计不合理、针对性不足导致失效,责任主体为措施制定部门;控制措施的执行、落地责任归属执行一线,若因作业不规范、管理不到位导致措施未有效执行,责任主体为现场执行单元;控制措施有效性的监督、核查责任归属安全监管部门,若因监督缺位未及时发现失效状态,责任主体为监管部门。这一界定逻辑为企业全员安全生产责任制的落地提供了可追溯的判定依据,有效避免了隐患治理中的责任推诿与泛化问责问题。

在安全资源分配层面,传统模式常采用“平均用力、全面排查”的资源投放方式,资源投入与风险等级不匹配,边际效益偏低。基于控制措施失效的逻辑,企业可以通过统计不同控制措施的失效频率、失效后果,精准识别高失效风险的管控环节,将资源优先投向高风险、高频失效的控制措施优化上,实现“风险等级越高、措施失效后果越重,资源投入强度越大”的差异化配置。同时,通过分析控制措施的系统性失效规律,能够识别出管理体系中的共性短板,从制度完善、技术升级、培训优化层面进行根源性治理,而非单纯增加现场排查频次,从本质上提升安全资源的投入产出效率。

7. 结论

本研究以系统安全工程理论为核心支撑,构建了适配集团化管理特点的双重预防机制,有效解决了传统安全管理模式被动、粗放的问题。研究明确了机制构建的系统边界,覆盖集团多级组织机构、全专

业流程与国内外全域地域；基于危险三要素完成危险源精准辨识，结合 LEC 法实现风险的量化评价与分级管控，界定了隐患为风险控制措施失效的核心内涵，形成“危险辨识 - 风险评价与控制 - 隐患排查治理”的全流程管控逻辑。并以某电力集团为例，通过信息化建设搭建专属模块，建立了双重预防机制，对风险开展分级管控，隐患持续排查治理，提高双重预防机制效能。

未来，需结合电力建设领域的技术迭代与业务拓展，持续完善危险辨识清单和风险评价标准，优化信息化系统的动态预警与数据迭代能力，推动双重预防机制与新技术、新场景深度适配，实现机制的常态化、动态化升级，让系统安全工程理论在电力建设安全管理领域的应用持续深化。

参考文献

- [1] 白勤虎, 吴子稳. 系统安全·系统安全工程·系统安全分析及评价[J]. 华东经济管理, 1994, 8(6): 32-34.
- [2] 国家能源局关于加强电力安全治理 以高水平安全保障新型电力系统高质量发展的意见[EB/OL]. https://www.gov.cn/zhengce/zhengceku/202411/content_6990253.htm, 2024-11-20.
- [3] 许绛垣, 罗云, 樊运晓. 系统安全分析评价技术方法对比研究[J]. 劳动保护科学技术, 1998(4): 25-29.
- [4] Joshi, A., Miller, S.P., Whalen, M., et al. (2005) A Proposal for Model-Based Safety Analysis. *24th Digital Avionics Systems Conference*, Washington, 30 October 2005-3 November 2005, 13.
- [5] Ham, D.H. (2021) Safety-II and Resilience Engineering in a Nutshell: An Introductory Guide to Their Concepts and Methods. *Safety and Health at Work*, **12**, 10-19. <https://doi.org/10.1016/j.shaw.2020.11.004>
- [6] Hollnagel, E. (2014) Safety-I and Safety-II: The Past and Future of Safety Management. Ashgate Publishing.
- [7] 中共中央 国务院关于推进安全生产领域改革发展的意见[EB/OL]. https://www.gov.cn/gongbao/content/2017/content_5156728.htm, 2016-12-09.
- [8] 应急管理部. 国务院安委会办公室关于实施遏制重特大事故工作指南构建双重预防机制的意见[Z]. https://www.mem.gov.cn/awhsy_3512/awhbgswj/201610/t20161011_247664.shtml, 2016-10-11.
- [9] 樊运晓, 罗云. 系统安全工程[M]. 第2版. 北京: 化学工业出版社, 2026.
- [10] 樊运晓, 韩丹丹, 牛毅, 李元龙. 基于溯源视角的 Hazard 和隐患关系探讨[J]. 安全, 2021, 42(7): 5-9+97.
- [11] Kinney, G.F. and Graham, K.J. (1980) A Practical Safety Analysis System for Hazards Control: BG0003.
- [12] Fine, W. (1971) Mathematical Evaluations for System Safety Engineering.