电子信息工程领域中危险因素的识别与网络安全技术的应用

苏志强

北京知存科技有限公司，北京市，100083；

摘要：围绕电子信息工程中的危险因素识别与网络安全技术应用构建理论框架，强调对象边界清晰与机制协同统一。文本以资产通道行为三维要素为骨架，提出分类判据与图谱化表达，阐明由边缘自治吸收快变扰动、由中心协调修正慢变偏差的组织方式。方法侧重分区分级与最小权限，配合多要素认证细粒度审计与策略编排，实现识别决策执行闭环，提升系统韧性与可恢复能力。体系强调统一术语一致口径与证据留痕，使识别结果能够直接映射到控制动作，评估体系与治理流程共同作用，促成长期稳定改进与可验证成效。方法不依赖具体案例与现场数值，以原理与约束推导可执行路径，强调边缘自治与中心协调的分工配合，使体系具备自我校准与渐进演化能力。

关键词：电子信息工程；危险因素识别；网络安全技术；纵深防护；治理体系

DOI：10.69979/3060-8767.25.06.067

引言

电子信息工程系统跨越硬件平台基础软件通信网络与业务应用，接口众多、耦合紧密、状态快速变化，危险因素具有跨域传导与隐蔽滋生的特点。工程实践常见口径不一与边界模糊，导致识别与处置脱节，窗口被动压缩。为形成可迁移的方法体系，本文在纯理论范围内重构对象与约束，给出分类判据与识别流程，并将安全技术与治理规则对齐，使风险信号能够被稳定转化为可执行动作，进而以滚动评估和度量驱动实现长期优化与能力提升。研究围绕三条主线展开，即理论框架与图谱表达，安全技术体系与协同策略，评估度量与治理落地，目标是以最小复杂度换取更高韧性与更短恢复时间，适配不同规模与阶段的工程实践。在术语与结构上使用统一表达，所有对象以资产通道行为三类名词刻画，所有动作以监测隔离修复三类动词表述，通过这种简化抽象，跨团队沟通成本显著降低，规则与工具得以共用并渐进升级。

1 理论框架与风险图谱

1.1 危险因素分类与边界刻画

电子信息工程的危险因素可分为环境扰动设备缺陷人员失误流程偏差供应链隐患与网络对抗六类，前四类主导物理侧风险，后两类经由通道进入网络侧并可能回流物理侧[1]。分类判据以触发条件传播路径检测难度修复代价与时间敏感性为核心，辅以可观测性与可控性双轴对齐优先级。为避免维度膨胀，应将同源事件合并为等价类，对跨域耦合加注显著标记，提示协同处置。风险图谱以资产为节点、以通道为边，将状态量行为量与约束量统一编码，形成事件层状态层与结构层三层表征，使定位能回溯到具体对象与接口。生命周期存在阶段差异，规划建设运行退役各含特有风险，运行期重在配置漂移与疲劳积累，退役期重在数据遗留与凭证泄漏。为降低识别主观性，可设置观测点与阈值，如接口数量变更频度报警密度与越权请求强度，并以颜色与权重呈现压力分布与传导方向。图谱需定期校准，增量更新与版本留痕并行，统一术语与编号规则贯穿设计建设与运维，跨团队共享时以发布节拍与生效时间约束口径，避免不同版本同时在线触发误判。图谱应支持分层折叠与区域聚合，能够在高层显示压力热点，在低层展开到设备端口与账户角色，查询结果可映射到控制清单与处置剧本。为保证长期可用，还需定义度量量纲与继承规则，明确由局部状态向区域视图的聚合方式，并规定由历史片段向预测窗口的外推口径。图谱与控制之间建立映射表，风险标签直接触发相应门槛与动作优先级，必要时进入降级运行或关停隔离。通过结构化表达与统一语义，识别与治理可以在同一底座内协同，转换损耗得以降低，处置链条得以缩短。

1.2 多源感知与识别机制

识别流程由感知抽取推断三步组成。感知侧汇聚日志告警配置工况与人工记录，在边缘完成预过滤与去噪，减少抖动进入中心。抽取侧将原始记录映射为结构关系时序片段与行为基线三类特征，并以增量更新保持时效[2]。推断侧以规则推理保证可解释，以统计学习弥补未知，在弱标注与少样本情形引入自监督表征与迁移蒸馏以提升泛化。为兼顾误报与漏报，设置分层阈值与回滞窗口，并将处置结果回写知识库形成闭环校准。跨域复

杂事件可借助因果图约束推断方向，避免将相关性误判为因果。识别输出采用任务化封装，携带对象边界与建议动作，编排模块可直接接管并下发处置单。为保证记录可信，应对关键来源进行对时与签名校验，重要链路启用双通道比对与异常告警。数据治理需覆盖采集传输存储与使用全流程，字段含义与计量口径以数据字典固定，任何变更都附带来源与责任。模型老化通过滑动窗口再训练缓解，参数更新遵循小幅渐进与可回退原则，评估集保留代表性片段以稳定对比。呈现方式采用四色等级绑定处置建议，一线可据此判断节奏与资源需求，管理侧可据此估算风险库存并调整优先级。为减少跨系统语义鸿沟，应建立术语映射与事件字典，将不同来源的同类现象统一到共同概念之下，降低判读分歧。识别链路持续监测延时与丢包，当链路进入紧张区间时自动降采样并切换到必要字段，保证核心信号不断流。在闭环中引入人工校核与复核队列，争议样本由专家审核并沉淀为高质量规则与模板，新规则通过灰度发布进入生产，效果不佳可快速回滚。识别到的高风险对象同时触发画像更新与控制强度提升，使知识与控制同步演进。

2 安全技术体系与协同策略

2.1 分区分级与最小权限架构

纵深防护以资产清单与拓扑基线为入口，先完成分区分级，再落地最小权限。边缘负责接口收敛与本地隔离，区域负责横向访问路径裁剪与流量整形，中心负责策略意图与统一审计。身份认证采用多要素校验与风险自适应组合，低风险动作走简化流程，高风险动作触发二次校验并强制留痕[3]。访问控制以角色为主属性为辅，常态保持策略稳定，事件窗口允许临时授权并自动失效。数据保护遵循分级分类，对核心数据启用加密脱敏与最少留存，对一般数据执行周期清理与到期销毁。为抑制配置漂移，建立基线对比与差异阻断，重大变化在变更窗口集中处理并记录证据。权限与设备状态绑定，终端未达标进入隔离区完成修复后再放行。跨区访问经由跳板点统一审计并限制命令集，横向移动空间随之收缩。关键服务设置冗余与切换路径，计划内定期演练以保证真实故障可控切换。为减少误操作，将危险指令与敏感资源绑定双确认，并设置冷却时间与最小观察期，避免频繁震荡。网络结构引入微隔离单元，单元之间以白名单通信，默认拒绝未声明路径，跨单元访问需携带身份与设备健康证明。边缘节点部署轻量策略引擎，在高延时或断链情形下仍能执行最小集处置，中心只下发意图与边界参数，由本地根据环境自适应展开。策略发布分层分批，先在低风险域演练，再扩展至核心域，发布过程保留回滚按钮与对比报告，保证变更可解释可复现。为兼顾效率与安全，可将零信任思想落到身份设备网络三条线，身份线聚焦可信标识与行为基线，设备线聚焦完整性度量与加固基线，网络线聚焦最短路径与拓扑可视。三条线在策略中心对齐口径，在区域侧按本地特征微调权重。由此在不增加过多复杂度的前提下获得安全收益，并以证据支撑审计与问责。

2.2 关键安全技术的组合应用

入侵检测承担异常发现，规则方法覆盖已知威胁，行为方法刻画未知模式，两者以证据合成给出结论。恶意代码防护以静态分析高效筛查，以动态沙箱验证执行轨迹，结论带证据路径便于复核。漏洞管理强调闭环推进，包含暴露面盘点风险评估修复实施与验证回归，并与停机窗口和业务优先级对齐。流量侧同时应对带宽洪泛与应用欺骗，速率限制挑战应答与异常指纹协同工作，边缘节点可预置限幅模板以压低峰值[4]。终端与嵌入式设备通过完整性度量与白名单控制降低侧门，固件更新采用分批灰度与快速回退。日志审计围绕可追溯与不可抵赖组织，时间同步与签名留痕共同保障可信。策略编排提供跨域联动能力，在发现横向移动迹象时同步触发隔离取证与阻断，并以战术手册约束顺序与超时回收，防止处置过度。密码技术保护机密与完整，密钥管理贯穿生成分发使用与销毁，重要密钥实施分权托管与硬件保护。态势感知汇聚多源线索形成全景视图，以推演工具检验处置方案一致性与复原时间。工控与物联网场景加入时序一致性校验与命令白名单，异常控制指令在本地二次确认并全程留痕，远程通道启用名单制与带宽配额，降低隐蔽外联带来的泄漏风险。为抑制数据外流，在出口侧叠加内容标记与动态水印，结合敏感词典与结构特征实现细粒度判定，对低可信会话触发延迟与抽检复核。欺骗与引诱为高价值目标建立诱饵资产与仿真服务，将对手引入可控环境并记录手段，产出的规则与样本再回灌检测引擎。人机协同同样重要，指挥台以场景化剧本引导处置，全链路保留操作与证据，事后复盘可定位节奏失配与资源瓶颈。面向长期演进，应当以年度与季度两节拍梳理技术组合的有效性，淘汰边际收益低且维护成本高的模块，将高收益模块前移到边缘或代理位置，以降低延时与带宽消耗。

3 评估度量与治理落地

3.1 风险评估模型与指标体系

评估模型服务排序与取舍，目标在于将复杂状态压

缩为可执行信号。指标体系由暴露度脆弱度重要度耦合度可恢复度与合规度构成，前四项决定发生概率与传播规模，后两项决定后果与修复效率。暴露度来源于接口数量对外依赖与可达性，脆弱度反映缺陷密度与老化程度，重要度取决于所在环节与替代成本，耦合度衡量跨域联动强弱，可恢复度体现冗余水平与应急资源可用性，合规度约束底线与边界。评估节拍采用周与月双循环，重大变更触发临时评估。输出以风险清单与建议路线呈现，用于驱动预算分配与窗口安排。模型需自校准，利用处置结果与演练记录修正参数，使判断随体系成熟逐步稳健。方法结合情景构建与随机仿真，对极端而合理的扰动执行压力测试，识别放大点与单点故障。为增强落地性，可设置红黄绿三段阈值与预警区间，对长期处于预警区间的对象触发结构复核与资源倾斜，并在下一周期更新权重。评估结果同时回灌到设计规则与运行边界，形成前后联动的改进闭环。在度量实现上，引入基础计分与修正因子相结合的方式，基础计分反映静态属性，修正因子反映短期变化，二者相乘得到当期权重。为避免指标相互掩盖，需要执行相关性与重要性分析，剔除冗余项并校正偏移项。对跨区域对象执行配额约束，避免单一领域过度占用预算。在报告呈现中，以分层看板展示趋势与阈值命中，管理侧能够直观理解风险库存与缓解成效。对复发频繁而损失较小的事件建立自动处置与延时合并，释放人力到高价值事项。对损失潜力巨大而发生概率较低的事件保留应急资源与替代路径，定期演练以检验可执行性。

3.2 治理流程与持续改进路径

治理体系由制度流程与能力三要素构成。制度明确职责边界与奖惩，流程规定从识别到处置到复盘的闭环，能力通过培训演练与对抗持续提升。供应链纳入统一口径，外部伙伴遵守配置基线与变更流程，关键组件实施来源审核与哈希校验，交付物在入库前完成验收并留存签署记录。研发活动贯彻左移理念，在需求设计与交付阶段设置质量门槛，缺陷不过门不得流向下游。变更管理实行预约与双人复核，高风险动作在夜间与假期收紧窗口并准备回退方案。应急指挥以统一席位为核心，信息线路与权责对应关系清晰，保证决策传达与现场动作同速。持续改进依托度量驱动，围绕发现时间响应时间恢复时间与复发率设定目标，并以看板公开透明，推动团队形成良性竞争。文化建设将安全目标与业务目标并列，鼓励以问题为线索持续修正结构与做法，第三方审计提供独立视角与数据质量校验。外部沟通设置专门窗口，事件期间保持及时回应与事实更新，减少误解与情绪积累。在组织协同上，建立跨域会商机制与例会节拍，重大议题以事实清单驱动讨论，结论对应责任与时限。对外包团队设置准入门槛与试运行期，不达标不得进入核心环境。对人员能力实行分级授权，关键席位引入替补与轮值，避免单点依赖。知识管理以问题清单与模板库为载体，复盘结论进入卡片化条目，供后续检索与培训。对于新引入的控制措施设定观察期与副作用记录，必要时回退或改写，减少次生风险。年度与季度分别进行能力体检与策略审查，识别结构性缺口与投资顺序。对跨项目的数据执行匿名化与范围控制，既满足共享与复核，又保护隐私与合规。

4 结语

电子信息工程的风险跨越物理与网络两侧，只有在对象边界清晰分类判据可执行与技术体系协同的前提下，识别结果才能迅速转化为有效动作。本文以三层框架串联识别技术与治理机制，提出分区分级与最小权限的底座，并以滚动评估与度量驱动推动长期优化。面向未来还需在数据一致性策略编排与演练常态化三个方面深化，使系统在复杂环境中保持稳定运行并具备可靠恢复能力。当规则与工具在同一语义底座中运行时，信息可被快速理解，行动能够彼此协同，组织便能以更小代价获得更高韧性与可恢复水平。

参考文献

[1]冯云婷,李攀,李景景,等.电子信息工程中网络安全技术应用研究[J].软件,2025,46(02):4-6.
[2]郭鹏.电子信息工程中的计算机技术应用及其安全研究[J].电子元器件与信息技术,2021,5(09):9-10.DOI:10.19772/j.cnki.2096-4455.2021.9.005.
[3]尹标迪.基于大数据分析的电子信息工程安全威胁检测[J].网络安全和信息化,2025,(07):157-159.
[4]李娟.电子信息工程潜在的安全隐患与防护技术分析[J].中国新通信,2025,27(06):26-28.