Service Science and Management 服务科学和管理, 2026, 15(5), 968-974
Published Online September 2026 in Hans. https://www.hanspub.org/journal/ssem
https://doi.org/10.12677/ssem.2026.155112

Hans汉斯

基于灾害脆弱性分析(HVA)的公立医院信息系统突发故障应急响应机制构建研究

——以J省S医院为例

磨云鲜

上海理工大学管理学院，上海

收稿日期：2026年8月2日；录用日期：2026年8月26日；发布日期：2026年9月2日

摘　要

公立医院业务连续性越来越依赖信息系统即HIS的稳定运行，但是随着医疗信息化的发展，HIS面临的软硬件故障、网络攻击等突发风险日益剧增。本文以J省S医院为例，运用灾害脆弱性分析模型，识别评估HIS面临的潜在故障类型及其脆弱性指数。通过实证分析，本文剖析该院在应急准备与响应能力上的薄弱环节，并据此设计一套HIS故障应急响应机制，以指导医院优化资源配置，提升信息系统的医疗韧性，为同类医疗机构的应急管理提供实践参考。

关键词

灾害脆弱性分析(HVA)，医院信息系统(HIS)，应急响应机制，风险评估

Research on the Construction of Emergency Response Mechanism for Sudden Failure of Public Hospital Information System Based on Disaster Vulnerability Analysis (HVA)

—Taking S Hospital in J Province as an Example

Yunxian Mo

Business School, University of Shanghai for Science and Technology, Shanghai

Received: August 2, 2026; accepted: August 26, 2026; published: September 2, 2026

文章引用: 磨云鲜. 基于灾害脆弱性分析(HVA)的公立医院信息系统突发故障应急响应机制构建研究[J]. 服务科学和管理, 2026, 15(5): 968-974. DOI: 10.12677/ssem.2026.155112

Abstract

The business continuity of public hospitals is increasingly dependent on the stable operation of information system, namely HIS. However, with the development of medical informatization, the sudden risks such as software and hardware failures and network attacks faced by HIS are increasing dramatically. Taking S hospital in J province as an example, this paper uses the disaster vulnerability analysis model to identify and evaluate the potential fault types and vulnerability indexes faced by HIS. Through empirical analysis, this paper analyzes the weak links in the emergency preparedness and response ability of the hospital, and designs a set of HIS fault emergency response mechanism to guide the hospital to optimize the allocation of resources, improve the medical resilience of the information system, and provide practical reference for the emergency management of similar medical institutions.

Keywords

Disaster Vulnerability Analysis, Hospital Information System, Emergency Response Mechanism, Risk Assessment

1. 研究背景

医院信息系统(Hospital Information System, HIS)主要指在医疗系统中，通过信息化技术设施和手段将来访患者的相关信息进行采集、加工、传递和管理，同时也赋予来访患者特定信息筛选和传输权限的功能平台[1]。医院的正常运转、患者安全和医疗服务质量都和 HIS 的稳定运行紧密相关[2]。如今大数据、物联网及云计算技术在医疗领域都有广泛的应用，医院业务连续性也越来越依赖信息系统稳定运行。然而，HIS 面临着日益增长的突发故障风险，如网络瘫痪、病毒感染、硬件故障、软件崩溃等，这些故障可能导致数据泄露、服务中断、经济损失甚至患者不良事件[3]。当前，许多医院在信息系统应急管理方面缺乏完善的安全事件应急预案，安全事件发生时难以快速响应和处置[4]。

灾害脆弱性分析是对灾害事件进行风险分层，度量潜在的灾害事件发生概率，并指导备灾、防灾工作[5]。将灾害脆弱性分析引入 HIS 故障应急响应机制的构建，可以科学地、系统性地识别 HIS 潜在故障类型，评估其发生可能性、影响程度及医院现有应对能力的不足，从而有针对性地制定和优化应急响应策略，提升医院信息系统的韧性。

本研究以 J 省 S 医院为例，探讨如何基于 HVA 构建公立医院信息系统突发故障应急响应机制，以期为提升医疗机构信息系统安全性和应急管理水平提供实践参考。

2. 理论基础

2.1. 灾害脆弱性分析理论(HVA)

灾害脆弱性分析是用来分析系统在灾害发生时所面临的风险程度和应对能力，并进行资源优化配置以减少脆弱性和增强韧性的一种综合性方法。灾害脆弱性分析可对灾害事件进行风险分层，度量潜在的灾害事件发生概率，并指导备灾、防灾工作[6]。将其运用于医院信息系统灾害脆弱性评估，可以揭示脆

弱性来源，并提供依据来改善医院的抗灾能力和减少灾害风险[7]。

2.2. KAISER 模型

KAISER 模型是由美国 Kaiser Permanente 医疗集团研制开发，对灾害脆弱性进行分析和评价，其结果是科学、可靠的[8]。该模型采用 EXCEL 录入数据、建立矩阵进行计算，具有简便实用的特点。KAISER 模型包括灾害事件发生的可能性和严重性共计 7 个维度，每个维度均分为 0~3 级，0 代表无或不适用，1 代表低，2 代表中，3 代表高。

3. 基于 HVA 的系统突发故障风险评估实证——以 J 省 S 医院为例

为精准识别公立医院信息系统突发故障的高危风险事件，明确应急管理的薄弱环节，本文以 J 省 S 医院为研究对象，运用 HVA 工具中的 Kaiser 模型开展实证调研。该医院为大型三甲医院，开放床位 3794 张，年门诊量 470 万人次，年住院量 19 万人次，已实现信息系统全覆盖，涵盖 HIS、EMR、LIS、PACS 等核心系统，其信息系统运行状况具有较强的代表性。

3.1. 成立 HVA 小组

邀请来自医院信息科、医务科、临床科室、护理部、后勤保障部、医学工程部、院感科、门诊办公室的专家及相关技术骨干组成 HVA 评估团队，一共 20 人。

3.2. 评估指标构建

结合该医院信息系统运行实际，参考相关文献和行业标准，通过头脑风暴、专家访谈、讨论等方式，构建了包含 4 个一级指标、10 个二级指标的信息系统突发故障风险评估指标体系。一级指标包括软硬件设施风险、网络安全风险、外部环境风险、人为操作风险；二级指标包括服务器故障、存储设备故障、软件系统崩溃、网络瘫痪、病毒感染、电力中断、自然灾害、操作失误、数据泄露、核心机房故障，全面覆盖信息系统运行过程中可能面临的各类风险，确保风险评估的全面性与针对性。每个二级指标均明确了具体的评估标准，为后续打分评估提供了统一依据。

3.3. 设计风险评估问卷

以 Kaiser 模型作为评价基础来设计风险评估问卷，每个指标从风险发生的可能性和严重性两大维度来进行评价，而严重性又分为人员伤亡、财产损失、服务影响、应急准备、内部反应和外部反应五个小维度进行评价。评价标准见表 1。

3.4. 专家评分机制与风险判定

面向 HVA 评估团队发放问卷，并根据实际情况，结合既往工作和灾害脆弱性理论进行填写，最终回收有效问卷 20 份。

为确保评分的客观性与严谨性，本研究在评分过程中采用了三轮匿名的德尔菲法来达成专家共识。第一轮统一发放标准化 Kaiser 风险评估问卷，同步发放指标释义、评分标准、医院近 3 年信息系统故障历史台账作为参考资料，20 位专家独立匿名填写各风险事件维度评分，全程不开展现场讨论，规避群体从众偏差，回收全部有效问卷。对 10 项故障风险各维度评分进行统计，计算每组评分均值、标准差，将单项维度标准差 ≥ 0.8 判定为专家意见分歧较大指标，整理分歧指标、高低分典型专家打分结果，形成匿名反馈汇总表，不标注专家个人信息。第二轮将分歧数据汇总表同步反馈全部专家，专家参考群体整体打分分布，重新调整自身评分，再次回收问卷，重复统计均值、标准差；若仍存在标准差 ≥ 0.8 的分歧项，

Table 1. Risk event scoring criteria
表 1. 风险事件评分标准

评估指标	细分维度	评分标准(0~3 分制)
可能性	发生的可能性	0 = 无或者不适用 1 = 发生概率低，属于极端意外情况 2 = 有可能发生或曾发生过 1 次以上 3 = 很可能发生或曾频繁发生
严重性	人力与安全影响	0 = 无或者不适用 1 = 仅增加少数医护工作量，无患者伤害 2 = 导致门诊/病房业务明显积压，可能引发医患纠纷，但无重伤 3 = 严重扰乱诊疗秩序，导致患者延误急救、重伤或死亡
	资产与数据影响	0 = 无或者不适用 1 = 局部硬件故障/直接经济损失 1 万元以下 2 = 非核心数据部分丢失/经济损失 1 万~3 万元 3 = 核心数据不可逆损毁/经济损失 3 万元以上
	运营与服务影响	0 = 无或者不适用 1 = 仅影响 1 个临床或行政科室的系统运行 2 = 影响 2 个及以上临床或行政科室的系统运行 3 = 导致全院性核心业务(如挂号、开医嘱、收费等)大面积瘫痪
	应急准备	0 = 无或者不适用 1 = 有系统故障应急预案，且定期开展演练 2 = 有系统故障应急预案，但从未开展实操演练 3 = 完全无应急预案
	内部反应	0 = 无或者不适用 1 = 信息科与临床、后勤等科室沟通顺畅，协作良好 2 = 院内有一定沟通协作，但流程不够通畅、存在信息差 3 = 突发故障时无沟通、无协作，各科室各自为战
	外部反应	0 = 无或者不适用 1 = 与 HIS 软件供应商、网络运营商及上级卫健委有顺畅的协调联动 2 = 与外部有协调联动，但响应迟缓或不顺畅 3 = 完全没有外部协调联动与技术支持保障

启动第三轮评分。经两轮修正后仍存在显著分歧的指标，组织专家组线上专题研讨会，逐一梳理分歧根源：若分歧源于专家对业务场景理解偏差，则统一明确故障场景界定标准；若分歧源于对现有应急资源认知差异，则现场公示机房灾备、应急预案、供应商服务协议等佐证材料。讨论完成后开展第三轮终评，最终采用全部专家评分算术平均值作为各维度最终得分，消除个体主观偏差，保证评估结果客观性。标准差用于反映专家意见离散程度，全部指标标准差区间 0.16~0.41，无指标标准差超过 0.8，三轮德尔菲法后专家打分离散程度低，意见一致性较强，评估结果可信度高。

Kaiser 模型的计分公式原理在于将风险发生的“可能性”与防范失效后的“严重性”进行量化乘积，并进行归一化处理。采用 Kaiser 模型公式计算相对风险值(相对风险值 = 发生可能性分数/3 × (人力影响

+ 资产影响 + 运营影响 + 准备工作 + 内部响应 + 外部响应)/18 × 100%)，该公式以百分比的形式直观呈现了各类风险事件在当前医院防范条件下的综合脆弱程度，数值越高，表明系统的脆弱性越强，越应优先采取干预措施。最终得出各风险事件的脆弱性指数排序。评估结果见表 2。

Table 2. Disaster vulnerability analysis
表 2. 灾害脆弱性分析

风险事件类型	发生可能性(均值 ± 标准差)	人力影响(均值 ± 标准差)	财产影响(均值 ± 标准差)	服务影响(均值 ± 标准差)	应急准备(均值 ± 标准差)	内部反应(均值 ± 标准差)	外部反应(均值 ± 标准差)	相对风险(均值 ± 标准差)	脆弱性指数排序
网络瘫痪	2.5 ± 0.32	2.5 ± 0.28	2.0 ± 0.35	3.0 ± 0.16	2.0 ± 0.31	2.0 ± 0.29	2.0 ± 0.33	62.5%	1
软件系统崩溃	2.6 ± 0.27	2.0 ± 0.30	1.5 ± 0.38	2.8 ± 0.22	2.0 ± 0.34	2.0 ± 0.30	1.5 ± 0.36	56.81%	2
病毒感染	2.4 ± 0.35	1.5 ± 0.33	2.0 ± 0.29	2.5 ± 0.26	2.0 ± 0.32	2.0 ± 0.31	2.0 ± 0.34	53.33%	3
数据泄露	1.8 ± 0.41	1.5 ± 0.37	3.0 ± 0.18	2.5 ± 0.29	2.5 ± 0.35	2.5 ± 0.33	2.8 ± 0.24	49.33%	4
核心机房故障	1.5 ± 0.38	2.8 ± 0.25	3.0 ± 0.17	3.0 ± 0.19	2.5 ± 0.35	2.5 ± 0.33	2.5 ± 0.31	45.28%	5
服务器故障	2.2 ± 0.33	1.5 ± 0.36	2.0 ± 0.32	2.2 ± 0.30	1.5 ± 0.37	1.5 ± 0.34	1.5 ± 0.35	41.56%	6
存储设备故障	1.6 ± 0.39	1.5 ± 0.35	2.5 ± 0.28	2.5 ± 0.27	2.0 ± 0.33	2.0 ± 0.31	2.0 ± 0.32	37.04%	7
操作失误	2.8 ± 0.26	1.0 ± 0.31	1.0 ± 0.33	1.5 ± 0.34	1.5 ± 0.36	1.0 ± 0.32	1.0 ± 0.35	36.3%	8
电力中断	2.0 ± 0.34	1.5 ± 0.37	1.5 ± 0.35	2.0 ± 0.32	1.5 ± 0.38	1.5 ± 0.36	1.5 ± 0.34	35.19%	9
自然灾害	1.0 ± 0.29	2.8 ± 0.24	3.0 ± 0.16	3.0 ± 0.18	2.5 ± 0.33	2.5 ± 0.31	2.8 ± 0.23	30.74%	10

3.5. 核心薄弱环节识别

结合 HVA 评估数据，识别出该医院信息系统突发故障应急管理的核心薄弱环节：一是核心业务容灾能力不足，表 2 数据显示，“网络瘫痪”与“软件系统崩溃”的相对风险值分别高达 62.5%和 56.81%，位居前两名，且其在“服务影响”维度上的得分(3.0 和 2.8)极高。这一数据特征直接映射出系统底层技术架构的冗余度不够。目前核心数据库的恢复时间较长，且缺乏能实现秒级接管的异地灾备方案。一旦主交换机或服务器发生故障，核心业务将直接面临停滞风险；二是实操转化与执行能力较弱，从表 2 各维度的横向评估来看，排名靠前的风险事件在“应急准备”维度的得分普遍偏高(均在 2.0 分及以上，即“有预案但未演练”)。高频高危事件伴随偏高的应急准备得分，证明现有应急管理多停留在制度层面，缺乏常态化的全员实战演练。在突发故障时，医护人员对断网后的手工处理替代流程操作生疏，难以实现从系统平稳切换至手工应急模式；三是信息通报与外部响应滞后，数据显示，“内部反应”与“外部反应”指标在数据泄露、核心机房故障等事件中的得分达到 2.5 至 2.8 的高位(接近各自为战或无外部技术支持的状态)。这反映出应急处置中的协同壁垒：内部缺乏自动化的故障通报机制，信息传递成本高；外部与供应商的应急服务协议落实不够严格，遇到复杂技术灾难时，外部技术支援往往存在严重滞后性。四是边界管控与内部隔离不足，“病毒感染”与“数据泄露”分列风险值第三、四位，尤其数据泄露的“财产影响”得分达到满分 3.0。高发生可能性与高财产损失风险映射了内网安全防线的漏洞。随着互联网医院和医疗物联网设备的广泛接入，医院网络边界日趋复杂。由于机房内部缺乏有效的微隔离手段，且终端设备管控不够严格，极易导致病毒在内网横向扩散，威胁核心数据资产安全。

4. HIS 故障应急响应机制设计

针对 HVA 评估识别出的核心薄弱环节，从响应架构、技术底座、演练机制和多方协同四个维度，设

计了一套系统化的 HIS 突发故障应急响应机制。

4.1. 构建“三级分层”的应急响应架构

针对协同联动机制不畅的问题，打破信息系统故障仅由信息科负责的传统观念，建立覆盖全院的三级响应体系：I 级响应，针对单一工作站死机、打印机故障等科室级局部故障。由临床科室网管员快速识别，立即执行初步隔离，并无缝切换至备用设备或手工替代流程，避免影响整体诊疗；II 级响应，针对 HIS 核心模块卡顿、部分存储设备故障等院级核心业务受损。由信息科主导，启动院级技术抢修与数据恢复，同时医务科、门诊办介入，协调各业务科室启动临时业务流程，如手工开单、挂号分流，确保核心医疗业务的连续性；III 级响应，针对全院网络瘫痪、勒索病毒大面积感染等灾难性全院瘫痪事件。由主管院领导成立应急指挥部，启动最高级别响应。除了内部全力抢修，立即启动与上级卫健部门、公安网监及第三方网络安全专家的协同联动，寻求外部资源紧急援助。

4.2. 强化底层技术冗余与网络安全防线

针对基础设施冗余不足与边界管控薄弱的技术痛点，进行针对性的架构升级：一是提升容灾与高可用级别，根据核心业务的恢复时间目标和恢复点目标，推进同城双活数据中心或异地灾备建设。在核心交换机、防火墙等关键网络节点全面部署双机热备，确保在单点硬件故障时系统能实现“秒级接管”；二是实施微隔离与动态边界管控，面对勒索病毒等外部攻击，在核心机房内部署“微隔离”技术，限制不同业务群组间的非必要访问。同时，加强医生工作站、自助机等终端设备的安全准入认证，切断病毒在内网横向扩散的路径。

4.3. 完善预案细节与常态化实战演练

针对应急预案实操转化能力弱的问题，强化实战演练：一是完善应急预案，结合医院实际业务流程和 HVA 识别的高危风险事件，制定针对性强、可操作性高的应急预案，细化完善手工替代流程，明确各环节的操作规范、责任人和时间节点，例如，制定手工挂号、收费、病历书写、医嘱执行等详细流程，发放至各科室，确保医护人员、行政管理人员在故障发生后能够快速上手；同时，针对 HIS 系统崩溃、网络瘫痪等高危风险事件，制定专项应急处置方案，提升应急处置的靶向性。二是固化常态化实战演练机制，联合医务处、护理部定期开展部门内部演练，每季度开展 1 次多部门联合演练，模拟不同类型的系统故障场景，组织信息科、临床、财务、后勤等相关部门全员参与，检验应急预案的可行性，提升跨部门协同处置能力；演练结束后，组织召开总结评估会，分析存在的问题，及时修正应急预案漏洞。

4.4. 建立自动化通报与 SLA 外部联动机制

针对信息通报滞后与外部响应不力的管理短板，优化沟通渠道：一是部署智能监控与自动化告警：引入 APM (应用性能管理)和 ITSM (IT 服务管理)工具，实现对网络流量、服务器 CPU 及数据库状态的秒级监控。设定合理的告警阈值，一旦发生异常，系统自动通过短信、内部协作平台向技术人员和相关科室主任推送告警，打破信息孤岛。二是刚性约束供应商 SLA 协议：在与 HIS 软件供应商、网络运营商续签合同时，明确细化应急响应服务等级协议(SLA)。例如，规定一般故障的响应时间、核心系统崩溃时的到场时限及数据恢复责任，确保在面临复杂技术灾难时，外部技术支援能够迅速、高效地切入。

5. 结论与局限性

5.1. 研究贡献与适用范围

本研究通过对 J 省 S 医院的 HIS 突发故障进行灾害脆弱性分析，科学量化了信息系统应急体系的脆

弱点，并基于数据结果设计了一套包含“响应架构、技术底座、演练机制、多方协同”四维一体的应急响应机制。本研究的贡献在于将 HVA 模型深度应用至公立医院数字基建的安全管理中，实现了从经验驱动向数据驱动的应急管理转变。本研究所构建的机制框架，不仅为 S 医院优化 IT 资源配置提供了实践路径，其指标体系和管理范式也适用于具有同等信息化建设规模与业务复杂度的其他大型公立综合类医院，为其应对突发 IT 灾难提供参考。

5.2. 研究局限性

尽管本研究取得了一定成果，但仍存在以下局限性：

首先，单案例研究的局限性。本文仅以 J 省 S 医院单一机构为研究样本，其得出脆弱性排序和制定的响应机制受限于该院特定的软硬件架构与资金投入水平，向基层医疗机构或专科医院推广时的普适性有待进一步验证。

其次，专家主观判断的潜在偏误。尽管本研究采用了多轮德尔菲法以求共识，但 Kaiser 模型的打分依然高度依赖于评估团队的认知边界、主观经验和风险偏好，存在不可避免的主观偏差。

最后，HVA 方法本身的工具局限性。灾害脆弱性分析擅长在宏观管理层面进行风险分层与资源优先级排序，但其无法进行微观层面的技术根因分析(如无法精准定位系统底层代码的缺陷或特定网络协议的漏洞)。未来研究需结合专业的技术测试手段(如渗透测试、源代码安全审计等)，以构建更全面的信息系统安全防护与响应闭环。

参考文献

[1] 林仁回, 赵雨, 伊永菊. 医院信息系统应急管理体系的建设[J]. 中国卫生标准管理, 2024, 15(13): 11-14.

[2] 邱梅钗. 基于集团化医院的分院 HIS 应急系统建设探讨附视频[J]. 福建电脑, 2016, 32(9): 101-102.

[3] 马向阳. 医院计算机信息系统(HIS)常见故障与策略附视频[J]. 数字技术与应用, 2022, 40(7): 69-72.

[4] 刘峰, 郑津津, 赵洪伟, 等. 基于多层防护的医院信息安全管理体系优化[J]. 中国卫生产业, 2025, 22(17): 101-104.

[5] 张雅琳, 王莹, 薛辉, 等. 基于 Kaiser 模型的医院后勤应急管理灾害性脆弱分析与应对策略附视频[J]. 中国卫生质量管理, 2019, 26(2): 99-102.

[6] 李双凤. 基于 Kaiser 模型的医院后勤灾害脆弱性分析[J]. 现代医院, 2021, 21(10): 1551-1553.

[7] 杨晔, 王洁, 赵善斌, 等. 基于 Kaiser 模型的山西省肿瘤医院灾害脆弱性分析附视频[J]. 中国肿瘤, 2025, 34(7): 557-563.

[8] 赵大仁, 刘志会, 何思长, 等. 医院灾害脆弱性概念及评价方法初探[J]. 中华灾害救援医学, 2016, 4(9): 520-523.