人工智能与 IT 服务事件管理深度融合的设计框架研究

甄理

昆仑数智科技有限责任公司，北京，100000；

摘要：本文围绕人工智能（AI）与 IT 服务事件管理的深度融合展开研究，提出了一种创新的设计框架。在传统 IT 服务管理体系中，事件管理（IM）作为核心流程，承担着快速响应服务异常、缩短故障生命周期的关键职责。然而，随着企业 IT 环境日益复杂，传统以人工为主导的事件处理模式逐渐暴露出效率瓶颈。本文构建了 AI 驱动的事件管理设计框架。该框架覆盖事件从记录、分类、分析到解决的完整生命周期。

关键词：人工智能；IT 服务事件管理；深度融合；智能日志分析；根因分析；自动化修复

DOI：10.69979/3041-0673.25.11.023

前言

事件管理（Incident Management，简称 IM）作为 IT 服务管理体系的核心流程，旨在通过快速响应和规范化处理机制，最大限度降低服务中断对业务的影响。根据 ISO20000 标准，事件管理聚焦于检测、记录、分类和优先级排序服务异常状态，通过触发预定义的响应策略实现服务恢复。[1]其本质是通过标准化流程缩短故障生命周期，需在最小化业务干扰的前提下恢复至约定服务级别。[6]现代实践进一步强调主动监控的价值，通过实时状态采集与预警机制，能够提前识别潜在风险。[2]

在实施框架上，事件管理呈现多维度的协同特征。基于 ITIL 框架的流程设计，包含事件受理、根因分析、处置决策等环节，同时需整合服务台、技术团队等多方资源。[4]其流程贯穿服务全生命周期，既为事后分析提供数据支撑（如服务成本核算），亦能通过闭环反馈优化资源配置。[5]此外，量化指标体系的引入为过程改进提供了科学依据，通过阈值分析识别低效环节，推动管理体系的持续优化。[3]

从学科演进视角看，事件管理已从单纯的技术操作发展为融合管理学与信息技术的交叉领域。[7]其理论内涵不断扩展，既包含紧急响应的战术层面，也涉及服务战略的规划维度。当前研究趋势聚焦于智能化升级，使人工智能与事件管理深度融合，以便应对复杂 IT 环境的挑战。

1 以人工为主导的事件处理模式存在的效率瓶颈及引入人工智能的必要性

其核心问题在于流程高度依赖人工经验与手动操作，导致响应速度缓慢且容错率低。传统模式下，事件从发现到分派需经历多级人工确认与工单流转，流程繁琐且易受人为因素干扰，例如复杂故障的根因分析往往因技术人员的经验差异而延误，而简单重复性任务（如密码重置）又占据大量人力资源。此外，人工处理难以实现 7×24 小时持续响应，夜间或节假日的服务中断往往因人员不足导致解决周期延长。更为关键的是，知识传承机制的缺失使得事件处理经验难以沉淀为可复用的标准化流程，同类问题的反复发生暴露出系统性效率缺陷。同时，人工判断易受主观认知偏差影响，在面对复合型故障或海量告警时，难以快速关联根因并制定有效处置策略，最终形成“响应迟滞—资源挤兑—服务恢复延迟”的恶性循环。这种依赖个体经验、缺乏自动化技术支撑的被动管理模式，已难以适配数字化转型下对服务连续性及资源优化配置的更高要求。

2 人工智能与事件管理深度融合的设计框架

事件管理流程是 IT 服务管理中的一个核心流程，注重服务为导向、处理时效、服务质量，通过切实有效的 IT 服务管理为企业创造价值。

事件管理流程大概如下:当一个事件输入的时候，首先要对事件进行检查、定位。检查事件的时候要明确事件的影响范围和紧急程度，还要进行初步的归类评估。服务台是事件的入口，它接收事件后，操作人员通过查阅配置管理数据库（Configuration Management Database,CMDB）进行处理。

2.1 事件的查明和记录

当用户在使用系统过程中遇到问题时，整个处理流程会从信息收集开始。用户或工作人员发现异常后，会立即向服务台反馈，工作人员会记录用户的联系方式、所在位置等基本信息，同时在系统中详细登记事件发生的具体时间、涉及的设备或服务等情况。例如，用户反馈"系统突然无法登录"，工作人员除了记录用户姓名和电话，还会备注事件发生时间和具体操作场景。所有事

件都会先提交给服务台统一处理，技术支持团队不能直接接收事件报告。

服务台工作人员会为每个事件分配一个专属编号，就像给每个事件贴上"身份证"。接下来会根据现有记录快速核查：如果发现类似的历史事件，比如之前出现过相同系统的登录故障，就会在原有记录基础上补充新情况，必要时还会调整事件等级；如果是全新事件，则会创建独立档案。例如，若发现当前登录事件与服务器维护有关，就会关联到最近的系统升级记录。

在确认事件详情后，工作人员会立即评估事件影响范围。如果遇到大面积系统瘫痪等重大故障，会第一时间上报管理层并同步告知用户当前处理进展；普通事件则直接进入标准处理流程。整个过程中，系统会持续更新事件状态，就像快递追踪一样让用户体验透明化管理。所有沟通记录、处理方案和用户反馈都会完整保存，既方便后续查询，也为未来遇到同类事件提供参考依据。这种闭环管理机制确保每个环节都有据可查，既提升处理效率，也保障了用户知情权。

此阶段可以利用人工智能实现智能日志分析与自动分类。利用自然语言处理（NLP）和机器学习（ML）技术，人工智能可实时分析来自系统日志、监控工具和用户报告的数据，自动识别异常模式并生成事件记录。例如，通过语义分析将非结构化的错误描述转化为结构化数据（如故障类型、影响范围），减少人工录入错误和时间消耗；还可以利用人工智能实现多源数据关联。人工智能可整合配置管理数据库（CMDB）、监控系统、网络设备等多源数据，自动关联事件与受影响的 IT 组件（如服务器、应用模块），快速定位事件根源，避免人工排查的延迟。

2.2 初步归类和初步支持

经过第一步的事件查明和记录，可从用户处获取的事件信息基本上已得到，事件管理数据库已经根据这些信息进行更新，接下来就是事件的初步归类和初步支持。这个环节的核心目标是尽快帮用户恢复正常使用，最大程度降低事件带来的不便。对于常见事件，系统会自动比对历史记录和解决方案库，若发现相似案例，可直接调用已有方法处理，无需重复分析。例如遇到网络连接故障或软件操作疑问等常见情况，工作人员能立即提供标准解决方案。若事件属于新型或复杂情况，系统无法自动匹配解决方案时，工作人员会立即将事件升级至更专业的技术团队。在这个过程中，工作人员会持续记录事件进展，并与各技术部门保持协作，确保用户随时了解处理进度。对于特别复杂或从未出现过的事件，技术团队会启动深度调查程序，通过分析日志、测试验证等方式找出根本原因，最终形成可复用的解决方案存入知识库，方便后续同类事件的快速处理。整个流程始终以用户满意度为核心，既保障了常规事件的高效解决，也为特殊事件建立了持续优化的处理机制。

此阶段人工智能可以实现智能事件分类与优先级排序。基于历史事件库和机器学习模型，人工智能可自动为新事件分配类别（如硬件故障、软件错误）并评估优先级（如高、中、低）。例如，通过分析事件关键词（如“宕机”“延迟”）和历史解决时间，基于机器学习模型动态调整优先级规则；人工智能可以实现知识库驱动的自愈建议。人工智能结合知识库中的解决方案和案例库，为常见事件提供自动化处理建议。例如，当检测到某应用版本存在已知漏洞时，自动推送补丁安装指南或触发预定义的修复脚本，缩短解决时间（MTTR）。人工智能可以实现智能分派与升级机制。人工智能可根据事件类型、影响范围和服务级别协议（SLA）自动分派任务至二线/三线支持团队，并在超时或复杂事件时触发升级流程，确保响应时效性。

2.3 事件调查和分析

当事件经过前两个环节仍未解决时，专业支援团队会立即接手处理。工作人员会第一时间确认受理事件，并明确后续沟通的时间节点，确保能及时向用户反馈进展。此时用户会收到事件处理进度的通知，包括当前所处的解决阶段。支援团队会优先提供临时解决方案，帮助用户缓解事件带来的困扰，例如通过系统重置或功能调整等应急措施。在处理过程中，团队会结合过往类似事件的处理经验，调取已有的解决方案库和历史案例进行比对分析。如果发现需要调整事件等级或处理优先级，会根据事先约定的服务标准重新评估，并及时与用户沟通变更后的处理计划。所有操作细节都会被完整记录，包括尝试过的解决方法、新增的事件分类等关键信息。当事件最终解决后，团队会将完整处理过程、耗时情况以及最终方案同步给用户，并确认事件已完全关闭。整个过程中，用户始终能通过服务渠道了解最新动态，既保障了事件处理的透明度，也确保了不同团队间的高效协作。

此阶段人工智能可以实现根因分析（RCA）自动化。利用人工智能算法（如决策树、随机森林）分析事件关联数据（如系统日志、性能指标），快速识别根本原因。例如，通过模式匹配发现多次“数据库连接超时”事件均与特定服务器内存不足相关，直接定位硬件资源瓶颈；人工智能可以实现实时异常检测与预测。基于时间序列

分析和预测模型（如 LSTM 神经网络），人工智能可预测潜在故障（如磁盘空间不足、服务响应缓慢），提前触发告警或自动扩容，将被动响应转为主动预防；人工智能可以实现跨团队协作支持。人工智能聊天机器人可协助专家团队共享实时事件信息，同步知识库更新，并通过语义分析提炼讨论要点，提升协同效率。

2.4 解决事件和恢复服务

当事件经过深入分析后，技术团队会根据最新掌握的情况制定具体解决步骤。他们会先采用已验证有效的临时解决方案快速缓解事件影响，例如通过系统重置或功能调整等方式。若发现需要调整原有方案，会及时向用户说明变更内容并获得认可。在实施最终解决方案过程中，工作人员会同步更新处理进度，通过电话、邮件或系统通知等方式告知用户当前进展。事件彻底解决后，团队会将完整的处理流程、采取的具体措施以及最终结果详细记录在案，这些经验会成为未来处理同类事件的参考依据。整个过程既确保了服务及时恢复正常，又让后续的事件处理更加高效精准，用户不仅能清楚了解每个环节的进展，还能感受到事件解决的透明度和专业性。

此阶段人工智能可以实现自动化修复执行。对于标准化事件（如密码重置、服务重启），人工智能可通过自动化工具链直接执行修复操作，无需人工干预。例如，人工智能检测到某服务进程崩溃后，自动触发重启脚本并验证服务恢复状态；人工智能可以实现动态调整解决方案。在复杂事件处理中，人工智能 AI 可根据实时反馈（如部分修复失败）动态推荐替代方案，并通过 A/B 测试评估不同措施的有效性，优化解决路径。

2.5 事件终止

当事件彻底解决后，服务流程会进入最后的确认环节。此时工作人员会与用户共同核实事件是否彻底解决，例如确认系统功能已恢复正常、相关操作不再出现异常等。这个阶段需要更新完整的处理记录，包括最终采取的解决措施和事件根源分析。服务团队会确保所有操作信息清晰易懂，例如用通俗语言说明事件原因和处理方案，并根据事件根源正确归类事件类型。用户需要确认解决方案的有效性，包括对处理结果的认可和对服务过程的满意度评价。整个处理过程会详细记录关键节点，例如事件解决耗时、最终完成时间、用户对服务的评价等。这些记录不仅作为服务闭环的证明，还会被存入共享知识库，为后续同类事件提供参考依据。通过这种闭环管理，既保障了用户权益，也持续优化了事件处理机制，确保每次服务都能让用户清楚了解进展和结果。

3 结论

在数字化转型背景下，IT 服务管理的效能已成为企业保障业务连续性与构建竞争优势的核心要素。针对传统事件管理流程中响应迟滞、过度依赖人工经验等痛点，本文创新性地提出了一种以人工智能为核心驱动的深度融合设计框架，通过分层技术架构重构事件管理的全生命周期。该框架首先运用自然语言处理（NLP）技术对用户工单和系统日志进行语义解析，结合随机森林等机器学习模型实现事件类型的智能分类与优先级动态调整，例如可精准区分“网络延迟”与“服务器宕机”等异构故障场景。在根因定位阶段，通过 LSTM 神经网络对时间序列数据进行异常检测，并借助决策树算法关联配置管理数据库（CMDB）配置信息与多源日志，将某电商平台支付故障的排查时效从小时级缩短至分钟级。进入自动化处置环节后，系统基于强化学习模型动态生成修复策略。最后，框架通过人工智能技术构建故障模式库，自动沉淀某制造业设备报警事件的解决方案。未来研究将聚焦多模态数据融合（如 IoT 设备与日志的协同分析）及联邦学习在跨组织协作中的应用，以应对分布式 IT 环境带来的复杂性挑战，推动事件管理从被动响应向预测性维护的范式升级。

参考文献

[1]齐元.论 ISO20000 事件管理与问题管理的流程及区别[J].电子质量,2021,(12):105-108.
[2]陈峻.监控与事件管理[J].网络安全和信息化,2019,(12):42-44.
[3]郝姝琪.论 ISO20000 体系量化指标梳理[J].商场现代化,2016,(22):94-96.
[4]刘宇杰,杨吉春.基于 ITIL 理念的事件管理流程在南车株洲所的设计[J].计算机光盘软件与应用,2014,17(10):253-254.
[5]葛泓,朱斌,赵建三.IT 服务管理体系实践之事件管理[J].中国教育信息化,2011,(17):33-36.
[6]Janvan Bon,章斌.详解事件管理[J].中国计算机用户,2008,(35):35-37.
[7]刘列励,尤舒.事件管理学科辨析[J].北京理工大学学报(社会科学版),2004,(01):72-75+79.